The Mathematics Student ISSN: 0025-5742
Vol. 86, Nos. 1-2, January-June (2017), xx-yy

EVALUATION OF THE QUADRATIC GAUSS SUM

M. RAM MURTY[1] **AND SIDDHI PATHAK**

(Received : 06 - 05 - 2017 ; Revised : 17 - 05 - 2017)

ABSTRACT. For any natural number n and $(m,n)=1$, we analyse the eigenvalues and their multiplicities of the matrix $\mathcal{A}(n,m) := (\zeta_n^{mrs})$ for $0 \leq r,s \leq n-1$. As a consequence, we evaluate the quadratic Gauss sum and derive the law of quadratic reciprocity using only elementary methods.

1. INTRODUCTION

For natural numbers n and k, a general Gauss sum is defined as

$$\mathcal{G}(k) := \sum_{j=0}^{n-1} e^{2\pi i j^k/n}. \tag{1.1}$$

When $k=1$, (1.1) reduces to the sum of all n-th roots of unity, which is a geometric sum and can be easily evaluated to be zero. The case $k=2$ turns out to be more difficult, and it took Gauss several years to determine (1.1) when n is an odd prime in order to prove the law of quadratic reciprocity. For further reading on Gauss sums, we refer the reader to [2] and [3].

In this article, we focus on the quadratic Gauss sum, namely,

$$\mathcal{G}(2) = \sum_{j=0}^{n-1} e^{2\pi i j^2/n}. \tag{1.2}$$

It can be shown that

Theorem 1.1. *For a natural number n,*

$$\mathcal{G}(2) = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \bmod 4, \\ 0 & \text{if } n \equiv 2 \bmod 4, \\ i\sqrt{n} & \text{if } n \equiv 3 \bmod 4, \\ (1+i)\sqrt{n} & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

There are many proofs of Theorem 1.1 in the literature. But most of the proofs use advanced tools. For example, [4] uses the theory of Fourier series, while [7] proves it using the truncated Poisson summation formula. The novelty of this article is that it utilizes only elementary methods, thus making the proof of Theorem 1.1 accessible to high school students. This linear algebra approach to

2010 Mathematics Subject Classification: 11L05, 11A15.

Key words and phrases : Gauss sum, quadratic reciprocity law.

[1] Research of the first author was partially supported by an NSERC Discovery grant.

evaluating (1.2) was initiated by Schur [9] in 1921 and simplified by Waterhouse [10] in 1970, to prove Theorem 1.1 when n is an odd prime. It was later expanded upon by the first author [8] to prove Theorem 1.1 for all n odd. The case n even was left open. In this note, we use a slight generalization of the method in these earlier works to prove Theorem 1.1 for even natural numbers n, hence determining (1.2) for all natural numbers n using only linear algebra and elementary number theory.

For clarity and continuity of exposition, we include the proof of Theorem 1.1 for n odd and the law of quadratic reciprocity in the earlier sections. We then use these results to prove Theorem 1.1 for n even.

2. Preliminary Results

Let n be a natural number and $\zeta_n := e^{2\pi i/n}$. For $(m,n) = 1$, we define the $n \times n$ matrix, $\mathcal{A}(n,m) = (\zeta_n^{mrs})$ for $0 \leq r, s \leq n-1$.

The motivation behind defining this matrix is the observation that

$$\operatorname{Tr} \mathcal{A}(n,1) = \sum_{j=0}^{n-1} \zeta_n^{j^2} = \mathcal{G}(2).$$

Let $\mathcal{A}(n,m)_{r,s}$ denote the (r,s)-th entry of $\mathcal{A}(n,m)$. Since the trace of a matrix is the sum of its eigenvalues counted with multiplicities, it suffices to find the eigenvalues of $\mathcal{A}(n,m)$ and their multiplicities. In order to compute the eigenvalues, observe that for $0 \leq k, l \leq n-1$,

$$\big(\mathcal{A}(n,m)\big)^2_{k,l} = \sum_{j=0}^{n-1} \zeta_n^{mkj} \zeta_n^{mjl} = \sum_{j=0}^{n-1} \zeta_n^{mj(k+l)}, \tag{2.1}$$

which is zero unless $m(k+l) \equiv 0 \pmod{n}$. Since $(m,n) = 1$, this is equivalent to the condition that $(k+l) \equiv 0 \pmod{n}$, in which case the sum is n because it is a geometric sum. In other words,

$$\mathcal{A}(n,m)^2 = \begin{bmatrix} n & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & n \\ 0 & 0 & 0 & \dots & n & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \\ 0 & 0 & n & \dots & 0 & 0 \\ 0 & n & 0 & \dots & 0 & 0 \end{bmatrix}. \tag{2.2}$$

Therefore,

$$\big(\mathcal{A}(n,m)\big)^4_{r,s} = \sum_{k=0}^{n-1} \big(\mathcal{A}(n,m)\big)^2_{r,k} \big(\mathcal{A}(n,m)\big)^2_{k,s},$$

and the summand is n^2 if $r + k \equiv 0 \pmod{n}$ and $s + k \equiv 0 \pmod{n}$ and zero otherwise. Thus, the summand is non-zero only when $r = s$ in which case it is n^2. This shows that

$$\big(\mathcal{A}(n,m)\big)^4 = n^2 I.$$

Hence, the eigenvalue of $\big(\mathcal{A}(n,m)\big)^4$ is n^2. By elementary linear algebra, we get that the eigenvalues of $\big(\mathcal{A}(n,m)\big)^2$ are n and $-n$. Consequently, the eigenvalues of $\mathcal{A}(n,m)$ are $\pm\sqrt{n}$ and $\pm i\sqrt{n}$. Let a,b,c,d be the multiplicities of $\sqrt{n}, -\sqrt{n}, i\sqrt{n}$ and $-i\sqrt{n}$ respectively. Thus,

$$\operatorname{Tr}\mathcal{A}(n,m) = \sqrt{n}\big((a-b)+i(c-d)\big), \tag{2.3}$$

for some natural numbers a,b,c and d.

Now, if $[x_0, x_1, \cdots, x_{n-1}]$ is an eigenvector of $\big(\mathcal{A}(n,m)\big)^2$ with eigenvalue n, then due to (2.1), it satisfies $x_i = x_{n-i}$ for $1 \le i \le n-1$. Hence, the dimension of the eigenspace corresponding to the eigenvalue n of $\big(\mathcal{A}(n,m)\big)^2$ is $(n+1)/2$ if n is odd and $n/2+1$ if n is even. Since the n-eigenspace of $\big(\mathcal{A}(n,m)\big)^2$ comprises of the $\pm\sqrt{n}$-eigenspace of $\mathcal{A}(n,m)$, we get the relations

$$a+b = (n+1)/2 \qquad \text{and} \qquad c+d = (n-1)/2, \tag{2.4}$$

when n is odd and

$$a+b = (n/2)+1 \quad \text{and} \quad c+d = (n/2)-1, \tag{2.5}$$

when n is even. Before proceeding, we prove the following lemma:

Lemma 2.1. *For any natural number n and $(m,n)=1$, let $\mathcal{A}(n,m) = (\zeta_n^{mrs})$ with $0 \le r,s \le n-1$. Then we have*

$$\big|\operatorname{Tr}\mathcal{A}(n,m)\big| = \begin{cases} \sqrt{n} & \text{if } n \text{ is odd,} \\ \sqrt{2n} & \text{if } n \equiv 0 \bmod 4, \\ 0 & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

Proof. Observe that

$$\begin{aligned} \big|\operatorname{Tr}\mathcal{A}(n,m)\big|^2 &= \big(\operatorname{Tr}\mathcal{A}(n,m)\big)\big(\overline{\operatorname{Tr}\mathcal{A}(n,m)}\big) \\ &= \Big(\sum_{k=0}^{n-1} \zeta_n^{m\,k^2}\Big)\Big(\sum_{l=0}^{n-1} \zeta_n^{-m\,l^2}\Big) \\ &= \sum_{k=0}^{n-1}\sum_{l=0}^{n-1} \zeta_n^{m(k^2-l^2)} \quad = \quad \sum_{l=0}^{n-1}\sum_{k=0}^{n-1} \zeta_n^{m(k-l)(k+l)}. \end{aligned}$$

The above sums depend only on the residue class of k and l modulo n and run over all residue classes mod n. Thus, for each fixed l mod n, we can make the linear change of variable $j = k-l$, which again runs over all residue classes mod n. Therefore, we have

$$\big|\operatorname{Tr}\mathcal{A}(n,m)\big|^2 = \sum_{l=0}^{n-1}\sum_{j=0}^{n-1} \zeta_n^{mj(j+2l)} = \sum_{j=0}^{n-1} \zeta_n^{mj^2} \sum_{l=0}^{n-1} \zeta_n^{2mjl}.$$

Since $(m,n)=1$, the inner sum is non-zero only if $2j \equiv 0 \pmod n$. If n is odd, then the only value of j which satisfies this congruence is $j=0$. Thus, $|\operatorname{Tr}\mathcal{A}(n,m)|$ evaluates to n when n is odd. If n is even, there are two values of j that satisfy the congruence, namely, $j=0$ and $j=n/2$. Hence, the sum becomes

$$\big|\operatorname{Tr}\mathcal{A}(n,m)\big|^2 = \big(1+\zeta_n^{mn^2/4}\big)n = (1+i^{mn})n,$$

which is zero if $n \equiv 2 \pmod 4$ and $2n$ if $n \equiv 0 \pmod 4$. This proves the lemma. □

Note that Lemma 2.1 proves Theorem 1.1 when $n \equiv 2 \pmod 4$. As a consequence of the above lemma, we have

Corollary 1. *For an odd natural number n,*

$$\operatorname{Tr} \mathcal{A}(n,m) = \begin{cases} \pm\sqrt{n} & \text{if } n \equiv 1 \bmod 4, \\ \pm i\sqrt{n} & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Proof. From (2.3),

$$\left|\operatorname{Tr} \mathcal{A}(n,m)\right| = \sqrt{n}\left((a-b)^2 + (c-d)^2\right)^{1/2}.$$

When n is odd, Lemma 2.1 leads us to deduce that either

$$(1)\ a-b = \pm 1 \text{ and } c = d, \qquad \text{or} \qquad (2)\ a = b \text{ and } c-d = \pm 1.$$

In Case (1), equation (2.4) implies that $c+d = 2d = (n-1)/2$, i.e, $d = (n-1)/4 \in \mathbb{N}$ and hence $n \equiv 1 \pmod 4$. In Case (2), equation (2.4) implies that $a+b = 2b = (n+1)/2$, i.e, $b = (n+1)/4 \in \mathbb{N}$ so that $n \equiv 3 \pmod 4$. □

We observe that the quadratic Gauss sums have the following multiplicative property.

Lemma 2.2. *For a natural number $n = n_1 n_2$ with $(n_1, n_2) = 1$ and $(m,n) = 1$, define $\mathcal{A}(n,m) = (\zeta_n^{mrs})$ for $0 \le r, s \le n-1$. Then we have,*

$$\operatorname{Tr} \mathcal{A}(n,m) = \operatorname{Tr} \mathcal{A}(n_1, mn_2) \operatorname{Tr} \mathcal{A}(n_2, mn_1).$$

Proof. The right hand side can be simplified as follows

$$\begin{aligned} \operatorname{Tr} \mathcal{A}(n_1, mn_2) \operatorname{Tr} \mathcal{A}(n_2, mn_1) &= \sum_{j=0}^{n_1-1} \sum_{k=0}^{n_2-1} e^{2\pi i m n_2 j^2/n_1}\, e^{2\pi i m n_1 k^2/n_2} \\ &= \sum_{j=0}^{n_1-1} \sum_{k=0}^{n_2-1} e^{2\pi i m ({n_2}^2 j^2 + {n_1}^2 k^2)/n_1 n_2} \\ &= \sum_{j=0}^{n_1-1} \sum_{k=0}^{n_2-1} e^{2\pi i m (n_2 j + n_1 k)^2/n}, \end{aligned}$$

as $e^{2\pi i m (2jk n_1 n_2)/n} = 1$. Now, since $(n_1, n_2) = 1$, the Chinese remainder theorem gives that as j and k range from 0 to $n_1 - 1$ and 0 to $n_2 - 1$ respectively, $n_2 j + n_1 k$ ranges over all residue classes modulo n. Hence, we have $\operatorname{Tr} \mathcal{A}(n_1, mn_2) \operatorname{Tr} \mathcal{A}(n_2, mn_1) = \sum_{r=0}^{n-1} e^{2\pi i m r^2/n} = \operatorname{Tr} \mathcal{A}(n,m)$. □

3. Proof of Theorem 1.1 for n odd

As seen earlier, $\mathcal{G}(2) = \operatorname{Tr} \mathcal{A}(n,1)$. Thus, we consider the case $m = 1$ in this section. Corollary 1 gives the value of the desired sum up to sign. To determine the sign in each case, we consider the determinant of the matrix $\mathcal{A}(n,1)$, which is the product of its eigenvalues counted with multiplicities.

Lemma 3.1. *Let $\mathcal{A} := \mathcal{A}(n,1) = (\zeta_n^{rs})$ for $0 \le r, s \le n-1$. Then*

$$\det \mathcal{A} = \begin{cases} i^{\binom{n}{2}}\, n^{n/2} & \text{if } n \text{ is odd}, \\ i^{\binom{n}{2}+1}\, n^{n/2} & \text{if } n \text{ is even}. \end{cases} \tag{3.1}$$

Proof. Observe that $\mathcal{A}$ is a Vandermonde matrix, that is, $\mathcal{A}$ is of the form

$$\begin{bmatrix} 1 & x_1 & {x_1}^2 & {x_1}^3 & \dots & {x_1}^{n-1} \\ 1 & x_2 & {x_2}^2 & {x_2}^3 & \dots & {x_1}^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & {x_n}^2 & {x_n}^3 & \dots & {x_n}^{n-1} \end{bmatrix}.$$

The determinant of an $n \times n$ Vandermonde matrix is well-known to be

$$\prod_{1 \le i < j \le n} (x_j - x_i).$$

Hence, we have that

$$\det \mathcal{A} = \prod_{0 \le r < s \le n-1} (\zeta_n^s - \zeta_n^r). \tag{3.2}$$

From the explicit computation of $\mathcal{A}(n,1)^2$ in (2.2), we see that this matrix is nI up to interchanging of rows. Moreover, interchanging 2 rows of a matrix only changes the sign of the determinant. Hence, $\det \mathcal{A}^2 = \pm n^n$. In particular, the number of row interchanges to transform $\mathcal{A}^2$ to nI is $(n-1)/2$ when n is odd and $(n-2)/2$ when n is even. This is because we need to interchange rows corresponding to r and $n-r$ for $1 \le r \le n-1$ to get nI. This is precisely $(n-1)/2$ number of distinct changes for odd n. When n is even, the row corresponding to $r = n/2$ has its diagonal entry as n, which need not be changed. For reasons evident from the calculations below, we write this as

$$\det \mathcal{A} = \begin{cases} \pm i^{\binom{n}{2}}\, n^n & \text{if } n \text{ is odd,} \\ \pm i^{\binom{n}{2}+1}\, n^n & \text{if } n \text{ is even.} \end{cases} \tag{3.3}$$

To determine the sign in the above computation, we calculate product in equation (3.2) in another way. For notational convenience, we will write $r < s$ for $0 \le r < s \le n-1$ and simplify (3.2) as follows -

$$\begin{aligned} \det \mathcal{A} = \prod_{r<s} \left(\zeta_n^s - \zeta_n^r\right) &= \prod_{r<s} \left(e^{2\pi i s/n} - e^{2\pi i r/n}\right) \\ &= \prod_{r<s} e^{i\pi s/n} e^{i\pi r/n} \left(e^{(i\pi s - i\pi r)/n} - e^{-(i\pi s - i\pi r)/n}\right) \\ &= i^{\binom{n}{2}} \prod_{r<s} \left[e^{i\pi(r+s)/n}\right] \prod_{r<s} \left[2\sin\left(\frac{(s-r)\pi}{n}\right)\right], \end{aligned} \tag{3.4}$$

as $\sin\theta = (e^{i\theta} - e^{-i\theta})/2i$. Now, note that

$$\begin{aligned} \sum_{\substack{r,s=0, \\ r \ne s}}^{n-1} (r+s) = \sum_{r=0}^{n-2} \sum_{s=r+1}^{n-1} (r+s) &= \sum_{s=1}^{n-1} \sum_{r=0}^{s-1} (r+s) \\ &= \sum_{s=1}^{n-1} \left(\frac{s(s-1)}{2} + s^2\right) \end{aligned}$$

$$= \sum_{s=1}^{n-1} \frac{3s^2 - s}{2}$$
$$= \frac{3}{2}\,\frac{(n-1)n(2n-1)}{6} - \frac{1}{2}\,\frac{n(n-1)}{2} \quad = \quad 2n\left(\frac{n-1}{2}\right)^2.$$

Therefore, the first product in (3.4) becomes

$$e^{i\pi(\sum_{r<s}(r+s))/n} = e^{i\pi(2n(n-1)^2/4n)} = i^{(n-1)^2},$$

which is 1 when n is odd and i when n is even. Since $0 < (s-r)\pi/n < \pi$, the second product in (3.4) is a positive quantity. Thus, the determinant becomes $i^{\binom{n}{2}}n^n$ when n is odd and $i^{\binom{n}{2}+1}n^n$ when n is even. □

Since the determinant of a matrix is the product of its eigenvalues, we have

$$\det \mathcal{A} = (\sqrt{n})^a(-\sqrt{n})^b(i\sqrt{n})^c(-i\sqrt{n})^d = i^{2b+c+3d}\, n^{n/2}.$$

Comparing this with Lemma 3.1 and noting that $3 \equiv -1 \bmod 4$, we get the conditions that

$$2b + c - d \equiv {}^nC_2 \bmod 4, \tag{3.5}$$

when n is odd. We will use this congruence to determine a, b, c, d as follows.

Suppose n is odd and $n \equiv 1 \pmod 4$. By Corollary 1, we know that $a-b = \pm 1$ and $c - d = 0$. Thus, (2.4) and (3.5) lead to

$$a - b = a + b - 2b \equiv \frac{n+1}{2} - \frac{n(n-1)}{2} \bmod 4 \equiv \frac{n+1-n+1}{2} \bmod 4 \equiv 1 \bmod 4.$$

Therefore, $a - b = 1$, which proves that $\mathcal{G}(2) = \operatorname{Tr}\mathcal{A}(n,1) = \sqrt{n}$ when $n \equiv 1 \pmod 4$. Now, suppose $n \equiv 3 \pmod 4$. Corollary 1 tells us that $a = b$ and $c - d = \pm 1$. Thus, (2.4) and (3.5) give

$$c - d \equiv \frac{n(n-1)}{2} - 2b \bmod 4 \equiv \frac{3(n-1)}{2} - \frac{n+1}{2} \bmod 4$$
$$\equiv \frac{3n-3-n-1}{2} \bmod 4 \equiv \frac{2n-4}{2} \bmod 4 \equiv 1 \bmod 4.$$

Therefore, when $n \equiv 3 \bmod 4$, we deduce that $\mathcal{G}(2) = \operatorname{Tr}\mathcal{A}(n,1) = i\sqrt{n}$ as in Theorem 1.1.

4. The law of quadratic reciprocity

Let a be a natural number and p be an odd prime. The Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution}, \\ -1 & \text{if } x^2 \equiv a \bmod p \text{ has no solution}. \end{cases}$$

We connect the quadratic Gauss sum $\mathcal{G}(2)$ with the Legendre symbol in the following lemma.

Lemma 4.1. *Let p be an odd prime and $(m,p)=1$. Define $\mathcal{A}(p,m)=(\zeta_p^{mrs})$ for $0\le r,s\le p-1$. Then*

$$\operatorname{Tr}\mathcal{A}(p,m)=\left(\frac{m}{p}\right)\operatorname{Tr}\mathcal{A}(p,1),$$

where $(\frac{m}{p})$ is the Legendre symbol.

Proof. We note that

$$\left(\frac{k}{p}\right)+1=\begin{cases}1 & \text{if } p\,|\,k,\\ 2 & \text{if } p\not|\,k,\ k \text{ is a quadratic residue } \bmod p,\\ 0 & \text{otherwise.}\end{cases}$$

For any $0\le k\le p-1$, the polynomial x^2-k has at most two roots in $\mathbb{F}_p$, the finite field with p elements. Also, if j is a root of this polynomial, then so is $p-j$ (which is distinct from j as p is odd). Hence, for each $k\in\mathbb{F}_p$ and $k\neq 0$, there are either 2 values of j satisfying $j^2\equiv k \pmod p$ or none. Thus, the quadratic Gauss sum can be rewritten as

$$\begin{aligned}\operatorname{Tr}\mathcal{A}(p,m)=\sum_{j=0}^{p-1}e^{2\pi imj^2/p}&=\sum_{k=0}^{p-1}\left[\left(\frac{k}{p}\right)+1\right]e^{2\pi imk/p}\\ &=\sum_{k=0}^{p-1}\left[e^{2\pi imk/p}\right]+\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)e^{2\pi imk/p}\\ &=\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)e^{2\pi imk/p},\end{aligned}\tag{4.1}$$

as the first sum is the sum of all p-th roots of unity and vanishes. Since the Legendre symbol is multiplicative, we multiply the second sum by $1=(\frac{m}{p})^2$ and have

$$\begin{aligned}\operatorname{Tr}\mathcal{A}(p,m)=\left(\frac{m}{p}\right)^2\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)e^{2\pi imk/p}&=\left(\frac{m}{p}\right)\sum_{k=0}^{p-1}\left(\frac{km}{p}\right)e^{2\pi ikm/p}\\ &=\left(\frac{m}{p}\right)\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)e^{2\pi ij/p}=\left(\frac{m}{p}\right)\operatorname{Tr}\mathcal{A}(p,1),\end{aligned}$$

by taking $m=1$ in (4.1). □

The law of quadratic reciprocity can be stated as follows.

Theorem 4.2. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}.$$

Proof. For convenience of notation, we define

$$e(n)=\begin{cases}1 & \text{if } n\equiv 1 \bmod 4,\\ i & \text{if } n\equiv 3 \bmod 4.\end{cases}$$

Thus, Theorem 1.1 states that for odd n, $\operatorname{Tr}\mathcal{A}(n,1) = e(n)\sqrt{n}$. Therefore, taking $n = pq$, we have

$$e(pq)\sqrt{pq} = \operatorname{Tr}\mathcal{A}(pq,1) = \Big(\operatorname{Tr}\mathcal{A}(p,q)\Big)\Big(\operatorname{Tr}\mathcal{A}(q,p)\Big),$$

by Lemma 2.2. Using Lemma 4.1, we get

$$e(pq)\sqrt{pq} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\Big(\operatorname{Tr}\mathcal{A}(p,1)\Big)\Big(\operatorname{Tr}\mathcal{A}(q,1)\Big) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)e(p)e(q)\sqrt{pq},$$

which implies that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{e(pq)}{e(p)e(q)}.$$

We observe that the right hand side is 1 if at least one of p or q is congruent to 1 (mod 4) and -1 otherwise. This is precisely as stated in the law of quadratic reciprocity. □

5. Evaluation of $\operatorname{Tr}\mathcal{A}(n,m)$ for odd n

In Section 3, we evaluated $\operatorname{Tr}\mathcal{A}(n,1)$ for odd natural numbers n. We use this computation to determine $\operatorname{Tr}\mathcal{A}(n,m)$ for n odd and $(m,n) = 1$ in general. Before proceeding, we recall the Jacobi symbol, which is a generalization of the Legendre symbol. For any positive integer a and an odd natural number $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, where p_j are distinct odd primes, the Jacobi symbol $(\frac{a}{n})$ is defined as a product of the Legendre symbols,

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k}\left(\frac{a}{p_j}\right)^{\alpha_j}.$$

Recall that the law of quadratic reciprocity extends to the Jacobi symbol by elementary number theory considerations.

Lemma 5.1. *For an odd natural number n and $(m,n) = 1$, we have*

$$\operatorname{Tr}\mathcal{A}(n,m) = \left(\frac{m}{n}\right)\operatorname{Tr}\mathcal{A}(n,1),$$

where $(\frac{m}{n})$ is the Jacobi symbol.

Proof. Let $\omega_3(n)$ be the number of prime divisors p of n with $p \equiv 3 \pmod 4$ counted with multiplicity. We claim that for any odd n,

$$\operatorname{Tr}\mathcal{A}(n,1) = \delta(n)\prod_{p|n}\operatorname{Tr}\mathcal{A}(p,1), \tag{5.1}$$

where $\delta(n) = \pm 1$ and the product is over primes dividing n repeated with multiplicity. Indeed, we know that the product on the right hand side of (5.1) can be evaluated by the already proven cases of Theorem 1.1 to be

$$\prod_{p|n}\operatorname{Tr}\mathcal{A}(p,1) = i^{\omega_3(n)}\sqrt{n}.$$

Also, since

$$n \equiv \begin{cases} 1 \bmod 4 & \text{if } \omega_3(n) \text{ is even,} \\ 3 \bmod 4 & \text{if } \omega_3(n) \text{ is odd,} \end{cases}$$

and the results from Section 3, the left hand side of (5.1) is $\sqrt{n}$ if $\omega_3(n)$ is even and $i\sqrt{n}$ if $\omega_3(n)$ is odd. Thus, $\operatorname{Tr}\mathcal{A}(n,1)$ and the product agree up to sign (which of course depends on n) so that(5.1) is immediate.

Writing (5.1) explicitly,

$$\sum_{j=0}^{n-1} e^{2\pi i j^2/n} = \delta(n) \prod_{p|n} \left[\sum_{k=0}^{p-1} e^{2\pi i k^2/p} \right] = \delta(n) \prod_{p|n} \left[\sum_{k=0}^{p-1} \left(e^{2\pi i k^2/n} \right)^{n/p} \right],$$

we observe that all terms in (5.1) lie in the n-th cyclotomic field, $\mathbb{Q}(\zeta_n)$. Thus, by applying the Galois automorphism that sends ζ_n to ζ_n^m, and noting that this automorphism fixes the rationals (and hence $\delta(n)$), (5.1) becomes

$$\sum_{j=0}^{n-1} e^{2\pi i m j^2/n} = \delta(n) \prod_{p|n} \left[\sum_{k=0}^{p-1} \left(e^{2\pi i m k^2/n} \right)^{n/p} \right] = \delta(n) \prod_{p|n} \left[\sum_{k=0}^{p-1} e^{2\pi i m k^2/p} \right].$$

Each term in the above product is $\operatorname{Tr}\mathcal{A}(p,m)$ for an odd prime p and $(m,p)=1$. Hence, by Lemma 4.1, we get

$$\operatorname{Tr}\mathcal{A}(n,m) = \delta(n) \left[\prod_{p|n} \left(\frac{m}{p} \right) \right] \left[\prod_{p|n} \operatorname{Tr}\mathcal{A}(p,1) \right].$$

Thus, by (5.1), $\operatorname{Tr}\mathcal{A}(n,m) = \left(\frac{m}{n} \right) \operatorname{Tr}\mathcal{A}(n,1)$. □

6. Proof of Theorem 1.1 for n even

The case $n \equiv 2 \pmod 4$ was settled in Lemma 2.1. Thus, we assume that $4|n$. We begin with the following elementary result which will be proved by induction.

Lemma 6.1. *Let r and s be natural numbers with $r \geq 2$ and s odd. Then*

$$\operatorname{Tr}\mathcal{A}(2^r, s) = \left(\frac{2^r}{s} \right) (1 + i^s) \sqrt{2^r}.$$

Proof. We proceed by induction on r. The base cases are $r = 2$ and $r = 3$. For $r = 2$,

$$\operatorname{Tr}\mathcal{A}(4,s) = 1 + e^{2\pi i s/4} + e^{2\pi i s} + e^{2\pi i s 9/4} = 2(1 + i^s).$$

For $r = 3$,

$$\operatorname{Tr}\mathcal{A}(8,s) = 2(1 + (-1)^s + 2e^{i\pi s/4}),$$

by considering squares modulo 8. Thus, $\operatorname{Tr}\mathcal{A}(8,s) = 4e^{i\pi s/4}$. Using $e^{i\theta} = \cos\theta + i\sin\theta$, we get that $\operatorname{Tr}\mathcal{A}(8,s) = 4(\cos(s\pi/4) + i\sin(s\pi/4))$, which is $2\sqrt{2}(1+i)$ if $s \equiv 1 \pmod 4$ and $-2\sqrt{2}(1-i)$ if $s \equiv 3 \pmod 4$. Hence, we see that Lemma 6.1 is true when $r = 2, 3$.

Suppose that $r \geq 4$ and Lemma 6.1 holds for all $2 \leq \alpha \leq r-1$. To prove it for r, we note that

$$\begin{aligned}\operatorname{Tr}\mathcal{A}(2^r, s) &= \sum_{j=1}^{2^r} e^{2\pi i s j^2/2^r} \\ &= \sum_{\substack{j=1,\\ j-\text{odd}}}^{2^r} e^{2\pi i s j^2/2^r} + \sum_{\substack{j=1,\\ j-\text{even}}}^{2^r} e^{2\pi i s j^2/2^r} \\ &= \frac{1}{2}\Bigg(\sum_{\substack{j=1,\\ j-\text{odd}}}^{2^r} e^{2\pi i s j^2/2^r} + e^{2\pi i s (j+2^{r-2})^2/2^r} \Bigg) + \sum_{k=1}^{2^{r-1}} e^{2\pi i s k^2/2^{r-2}},\end{aligned}$$

where in the first sum, we pair the terms corresponding to j and $j+2^{r-2}$ (which are distinct as j is odd) and in the second sum, we change the index of summation by setting $j = 2k$. Now, each summand of the first term is

$$\begin{aligned}e^{2\pi i s j^2/2^r} + e^{2\pi i s (j+2^{r-2})^2/2^r} &= e^{2\pi i s j^2/2^r} + e^{2\pi i s j^2/2^r}\, e^{2\pi i s (2^{r-1} j)/2^r} \\ &= e^{2\pi i s j^2/2^r} - e^{2\pi i s j^2/2^r} \quad = \quad 0,\end{aligned}$$

as j is odd. We recognize the second term as $2\operatorname{Tr}\mathcal{A}(2^{r-2})$, which is equal to

$$(2^{r-2}/s)\ 2\ (1+i^s)\sqrt{2^{r-2}}$$

by the induction hypothesis. Thus, the principle of mathematical induction implies that

$$\operatorname{Tr}\mathcal{A}(2^r, s) = (2^r/s)(1+i^s)\sqrt{2^r}$$

for all $r \geq 2$. □

We now derive Theorem 1.1 in the case $4|n$ as a consequence of the proposition below.

Proposition 6.2. *Let n be natural number with $4|n$ and $(m,n)=1$. Then*

$$\operatorname{Tr}\mathcal{A}(n, m) = (n/m)\,(1+i^m)\,\sqrt{n}.$$

Proof. Write $n = 2^u v$, with $u \geq 2$ and v odd. We would like to evaluate $\operatorname{Tr}\mathcal{A}(2^u v, m)$ for $(m,n)=1$. By Lemma 2.2, we get

$$\operatorname{Tr}\mathcal{A}(2^u v, m) = \Big(\operatorname{Tr}\mathcal{A}(2^u, vm) \Big) \Big(\operatorname{Tr}\mathcal{A}(v, 2^u m) \Big). \tag{6.1}$$

We note that v is odd and $(v, 2^u m) = 1$. Hence, by Lemma 5.1,

$$\operatorname{Tr}\mathcal{A}(v, 2^u m) = \left(\frac{2^u m}{v}\right) \operatorname{Tr}\mathcal{A}(v, 1), \tag{6.2}$$

which is known by the results in Section 3. Since $4|n$ and $(m,n)=1$, m is odd. Therefore, vm is odd and $(2^u, vm) = 1$. To determine $\operatorname{Tr}\mathcal{A}(2^u, vm)$, we use Lemma 6.1.

Thus, by (6.1), (6.2) and Lemma 6.1, we have

$$\operatorname{Tr}\mathcal{A}(2^u v, m) = \sqrt{2^u} \left(\frac{2^u m}{v}\right) \left(\frac{2^u}{vm}\right) (1+i^{vm}) \operatorname{Tr}\mathcal{A}(v, 1),$$

which can be simplified using the multiplicativity of the Jacobi symbol to

$$\operatorname{Tr}\mathcal{A}(2^u v, m) = \sqrt{2^u}\ (2^u/m)\ \epsilon_{v,m},$$

where

$$\epsilon_{v,m} = (m/v)\ (1 + i^{vm}) \operatorname{Tr}\mathcal{A}(v, 1).$$

Hence we see that the value of trace depends on whether v and m are congruent to 1 or 3 modulo 4. We remark that the case of odd n from Theorem 1.1 can be re-written as

$$\operatorname{Tr}\mathcal{A}(n, 1) = i^{(n-1)^2/4}\sqrt{n}.$$

Since both v and m are odd, we can use the law of quadratic reciprocity to deduce

$$\left(\frac{m}{v}\right)\left(\frac{v}{m}\right) = \begin{cases} -1 & \text{if both } m, v \equiv 3 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, we have the following table of values of $\epsilon_{v,m}$:

v \ m	1 mod 4	3 mod 4
1 mod 4	$\left(\frac{v}{m}\right)(1+i)\sqrt{v}$	$\left(\frac{v}{m}\right)(1-i)\sqrt{v}$
3 mod 4	$\left(\frac{v}{m}\right)(1-i)i\sqrt{v}$	$-\left(\frac{v}{m}\right)(1+i)i\sqrt{v}$

Observe that $i(1-i) = (1+i)$ and $i(1+i) = -(1-i)$. Thus, whenever $4|n$, we have $\operatorname{Tr}\mathcal{A}(n, m) = (n/m)(1 + i^m)\sqrt{n}$. □

In particular, for $m = 1$, Proposition 6.2 implies Theorem 1.1 for $n \equiv 0 \bmod 4$.

7. Concluding Remarks

We observe that determining the quadratic Gauss sum in the case $4|n$ is more delicate than the case n odd. The study of the eigenvalues and their multiplicites of the matrix $\mathcal{A}(n, m)$ lies deeper than the law of quadratic reciprocity. The matrix $\mathcal{A}(n, m)$ also appears in the context of the discrete Fourier transform of periodic arithmetical functions. Thus, the study of its eigenvalues and their multiplicities is interesting in its own right. Moreover, the investigation of the eigenvectors of $\mathcal{A}(n, 1)$ is even deeper than the study of its eigenvalues and their multiplicites (for example, see [6]). Surprisingly, the explicit construction of these eigenvectors was first done as late as 1972 in the paper of McClellan and Parks [5].

Acknowledgements. We thank the referee and Anup Dixit for helpful comments on an earlier version of this paper.

References

[1] Borevich, Z. and Shafarevich, I., *Number Theory*, translated by Newcomb Greenleaf, Academic Press, New York, 1966.

[2] Berndt, B. and Evans, R., The determination of Gauss sums, *Bull. Amer. Math. Soc.*, **5**, No. 2 (1981), 107–129.

[3] Ireland, K. and Rosen, M., *A classical introduction to modern number theory*, Graduate Texts in Mathematics, Springer-Verlag, (1990), 66–78.

[4] Lang, S., *Algebraic Number Theory*, Second Edition, Graduate Texts in Mathematics, Springer-Verlag, (1994), 87–90.

[5] McClellan, J. H. and Parks, T. W., *Eigenvalue and eigenvector decomposition of the discrete Fourier transform*, IEEE Transactions Audio Electroacoust., Vol. AU-**20**, (1972), 66–74.

[6] Mehta, M. L., Eigenvalues and eigenvectors of the finite Fourier transform, *Journal of Mathematical Physics*, **28**, (1987), 781–785.

[7] Ram Murty, M., *Problems in Analytic Number Theory*, First Edition, Graduate Texts in Mathematics, Springer-Verlag, (2000), 81 and 323–324.

[8] Ram Murty, M., Quadratic Reciprocity via linear algebra, *Bona Mathematica*, **12**, No. 4 (2001), 75–80.

[9] Schur, I., Über die Gausschen Summen, *Nachrichten von der Königlichen Gessellschaft zu Göttingen, Mathematisch - Physikalische Klass*, (1921), 147–153.

[10] Waterhouse, W. C., The sign of the Gauss sum, *Journal of Number Theory*, **2** (1970), 363.

M. Ram Murty
Department of Mathematics and Statistics
Queen's University, Kingston, Canada, ON K7L 3N6.
E-mail: *murty@mast.queensu.ca*

Siddhi Pathak
Department of Mathematics and Statistics
Queen's University, Kingston, Canada, ON K7L 3N6.
E-mail: *siddhi@mast.queensu.ca*