QUADRATIC RECIPROCITY VIA LINEAR ALGEBRA

M. RAM MURTY

Abstract. We adapt a method of Schur to determine the sign in the quadratic Gauss sum and derive from this, the law of quadratic reciprocity.

1. Introduction

Let p and q be odd primes, with $p \neq q$. We define the Legendre symbol (p/q) to be 1 if p is a square modulo q and -1 otherwise. The law of quadratic reciprocity, first proved by Gauss in 1801, states that

$$(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}.$$

It reveals the amazing fact that the solvability of the congruence $x^2 \equiv p(\mathrm{mod}\, q)$ is equivalent to the solvability of $x^2 \equiv q(\mathrm{mod}\, p)$.

There are many proofs of this law in the literature. Gauss himself published five in his lifetime. But all of them hinge on properties of certain trigonometric sums, now called Gauss sums, and this usually requires substantial background on the part of the reader. We present below a proof, essentially due to Schur [2] that uses only basic notions from linear algebra. We say "essentially" because Schur's goal was to deduce the sign in the quadratic Gauss sum by studying the matrix

$$A = (\zeta^{rs}) \qquad 0 \leq r \leq n-1,\ 0 \leq s \leq n-1$$

where $\zeta = e^{2\pi i/n}$. For the case of $n = p$ a prime, Schur's proof is reproduced in [1] and a 'slicker' proof was later supplied by Waterhouse [3]. Our point is to show that Schur's proof can be modified to determine $\mathrm{tr}\, A$ when n is an odd number and this allows us to deduce the law of quadratic reciprocity.

2. The trace of A

Observe that the (u, v)-th entry of A^2 is

$$\sum_{k=0}^{n-1} \zeta^{uk}\zeta^{kv} = \begin{cases} n & \text{if} \quad u+v \equiv 0(\mathrm{mod}\, n) \\ 0 & \text{otherwise} \end{cases}$$

so that

$$A^2 = \begin{pmatrix} n & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & n \\ 0 & 0 & \cdots & n & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & n & \cdots & 0 & 0 \end{pmatrix}.$$

1991 *Mathematics Subject Classification.* Primary: 11A15, Secondary: 11L05.
Key words and phrases. quadratic reciprocity, Gauss sums .

It is easily seen that $A^4 = n^2 I$, from which we deduce that the eigenvalues of A^2 are $\pm n$. For each eigenvalue, we can compute the eigenspace directly. For example, for the eigenvalue n, we get that any eigenvector $(x_0, x_1, \cdots x_{n-1})$ must satisfy the system of equations $x_{n-j} = x_j,\ 1 \leq j \leq n-1$. For n odd, we find the dimension of this eigenspace to be $1 + (n-1)/2 = (n+1)/2$. Similarly, the eigenspace corresponding to $-n$ has dimension $(n-1)/2$. Therefore the characteristic polynomial of A^2 is

$$(x-n)^{(n+1)/2}(x+n)^{(n-1)/2}.$$

We conclude that the eigenvalues of A are $\pm\sqrt{n}, \pm i\sqrt{n}$, where $i = \sqrt{-1}$. Let a, b, c, d denote the multiplicities of the eigenvalues $\sqrt{n}, -\sqrt{n}, i\sqrt{n}$ and $-i\sqrt{n}$ respectively. Then

$$a + b = \frac{n+1}{2}; \quad c + d = \frac{n-1}{2} \tag{2.1}$$

so that

$$\operatorname{tr} A = ((a-b) + (c-d)i)\sqrt{n}. \tag{2.2}$$

On the other hand,

$$|\operatorname{tr} A|^2 = \sum_{k,\ell} \zeta^{k^2-\ell^2} = \sum_{k,\ell} \zeta^{(k-\ell)(k+\ell)}.$$

Setting $k - \ell = \alpha$ in the sum, we obtain

$$|\operatorname{tr} A|^2 = \sum_{\alpha,\ell} \zeta^{\alpha^2+2\alpha\ell}.$$

Since n is odd, the inner sum for α fixed is zero unless $\alpha \equiv 0 (\operatorname{mod} n)$ in which case it is n. We have proved:

Lemma 2.1. *For odd n,*

$$|\operatorname{tr} A| = \sqrt{n}.$$

Corollary 1.

$$\operatorname{tr} A = \begin{cases} \pm\sqrt{n} & \text{if} \quad n \equiv 1 (\operatorname{mod} 4) \\ \pm i\sqrt{n} & \text{if} \quad n \equiv 3 (\operatorname{mod} 4) \end{cases}$$

Proof. From (2.2),

$$|\operatorname{tr} A|^2 = \left((a-b)^2 + (c-d)^2\right) n$$

and we deduce $c - d = 0$ and $a - b = \pm 1$ or $a - b = 0$ and $c - d = \pm 1$. In the first case using (2.1), we solve the system $a + b = (n+1)/2$, $a - b = \pm 1$ and deduce $n \equiv 1 (\operatorname{mod} 4)$. Similarly, in the second case, we deduce $n \equiv 3 (\operatorname{mod} 4)$. This proves the corollary. □

3. The determinant of A

Recall the Vandermonde determinant:

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & \cdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i<j} (x_j - x_i).$$

Now $\det A$ is a Vandermonde determinant. It is somewhat easier to consider $(\det A)^2$:

$$(\det A)^2 = (-1)^{\binom{n}{2}} \prod_{r \neq s} (\zeta^r - \zeta^s).$$

The product is equal to

$$\prod_{j=0}^{n-1} f'(\zeta^j)$$

with $f(x) = x^n - 1$. Thus,

$$(\det A)^2 = (-1)^{\binom{n}{2}} n^n,$$

from which we deduce

$$\det A = \pm i^{\binom{n}{2}} n^{n/2}. \tag{3.1}$$

We would like to determine the sign in (3.1). This is easily done as in [2]. We have

$$\det A = \prod_{s<r} (\zeta^r - \zeta^s) = \prod_{s<r} \eta^{r+s} (\eta^{(r-s)} - \eta^{-(r-s)})$$

where $\eta = e^{\pi i/n}$. Since

$$\sum_{s<r} (r+s) = \sum_{r=1}^{n-1} \sum_{s=0}^{r-1} (r+s) = \sum_{r=1}^{n-1} \left(r^2 + \frac{r(r-1)}{2} \right) = 2n \left(\frac{n-1}{2} \right)^2$$

is divisible by $2n$, we deduce

$$\det A = \prod_{s<r} \left(2i \sin \frac{(r-s)\pi}{n} \right) = i^{\binom{n}{2}} (\text{positive quantity}).$$

Thus, from 3.1 we conclude

Lemma 3.1. *For n odd,*

$$\det A = i^{\binom{n}{2}} n^{n/2}.$$

Corollary 2. *For n odd,*

$$2b + c - d \equiv \binom{n}{2} \pmod 4.$$

Proof. Since $\det A$ is the product of the eigenvalues

$$\det A = (\sqrt{n})^a (-\sqrt{n})^b (i\sqrt{n})^c (-i\sqrt{n})^d = (-1)^{b+d} i^{c+d} n^{n/2} = i^{2b+c+3d} n^{n/2}.$$

Thus, by Lemma 3.1,

$$2b + c + 3d \equiv 2b + c - d \equiv \binom{n}{2} \pmod 4,$$

from which the result follows. □

Corollary 2 can be used to determine $\operatorname{tr} A$ explicitly. Returning to case 1, $c - d = 0$ so that

$$2b \equiv \binom{n}{2} \pmod 4.$$

Thus from (2.1),

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

because $n \equiv 1 (\mathrm{mod}\, 4)$. Similarly in the second case, $a - b = 0$ so that from (2.1) $2b = (n+1)/2$ and

$$c - d \equiv \frac{n(n-1)}{2} + 2b \equiv -\frac{n-1}{2} + \frac{n+1}{2} \equiv 1 (\mathrm{mod}\, 4).$$

This proves:

Theorem 1. *For odd n,*

$$\mathrm{tr}\, A = \sum_{j=0}^{n-1} e^{2\pi i j^2/n} \begin{cases} \sqrt{n} & \text{if } n \equiv 1 (\mathrm{mod}\, 4) \\ i\sqrt{n} & \text{if } n \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

4. The law of quadratic reciprocity

Let

$$S(n,a) = \sum_{j=0}^{n-1} e^{2\pi i j^2 a/n}.$$

We will prove:

Lemma 4.1. *Let m, n be coprime positive integers. Then*

$$S(m,n)S(n,m) = S(mn,1).$$

Proof. We have

$$\sum_{j=0}^{n-1}\sum_{k=0}^{m-1} e^{2\pi i j^2 m/n} e^{2\pi i k^2 n/m} = \sum_{j,k} e^{\frac{2\pi i}{mn}(j^2m^2 + k^2n^2)} = \sum_{j,k} e^{\frac{2\pi i}{mn}(jm+kn)^2}$$

We note that as $0 \leq j \leq n-1$ and $0 \leq k \leq m-1$, the set of integers $jm+kn$ forms a complete set of residue classes modulo mn. The result is now immediate. □

If p, q are primes, note that

$$\sum_{j=0}^{p-1} e^{2\pi i j^2 q/p} = \sum_{k=0}^{p-1} \left(1 + \left(\frac{k}{p}\right)\right) e^{2\pi i k q/p} = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) e^{2\pi i k q/p}$$

because the sum of the p-th roots of unity is zero. Also, the right hand side is equal to

$$\left(\frac{q}{p}\right) \sum_{k=0}^{p-1} \left(\frac{kq}{p}\right) e^{2\pi i k q/p} = \left(\frac{q}{p}\right) S(p,1)$$

by the multiplicative property of the Legendre symbol. Therefore, $S(p,q) = (q/p)S(p,1)$. We can now deduce

Theorem 2.

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

for any distinct odd primes p, q.

Proof. Define for odd n, $e(n) = 1$ if $n \equiv 1 (\mathrm{mod}\, 4)$ and i if $n \equiv 3 (\mathrm{mod}\, 4)$. Then, the result of Theorem 1 can be written as $S(n,1) = e(n)\sqrt{n}$. Thus,

$$e(pq)\sqrt{pq} = S(pq,1) = S(p,q)S(q,p) = (q/p)(p/q)S(p,1)S(q,1) = (q/p)(p/q)e(p)e(q)\sqrt{pq}$$

from which we deduce

$$(q/p)(p/q)e(p)e(q) = e(pq)$$

which is the law of quadratic reciprocity. □

References

[1] Z. Borevich and I. Shafarevich, Number Theory, translated by Newcomb Greenleaf, Academic Press, New York, 1966.
[2] I. Schur, Über die Gausschen Summen, *Nachrichten von der Königlichen Gessellschaft zu Göttingen, Mathematisch - Physikalische Klass*, (1921), 147-153.
[3] W.C. Waterhouse, The sign of the Gaussian sum, *Journal of Number Theory,* **2** (1970), 363.

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