The 11th International Seminar on
Linear Algebra and it's Applications
Feb 2022

Linear Algebra and Quadratic Reciprocity Law

Mohammadreza Darafsheh*

School of mathematics, statistics and computer science, College of science, University of Tehran, Tehran, Iran

Abstract

The quadratic reciprocity law was proved by Gauss who produced six different proofs of this law in his life. Although there are different proofs of this well-known theorem, we adopt concepts from linear algebra to calculate the Gauss sum and give a different proof of this theorem.

Keywords: Gauss sum, quadratic reciprocity, trace, equivalence.
Mathematics Subject Classification [2010]: 11A15, 11L05.

1 Introduction

Let p be an odd prime and a an integer. The Legendre symbol $(\frac{a}{p})$ is defined to be 1 if the quadratic equation $x^2 \equiv a(\mod p)$ has a solution, otherwise $(\frac{a}{p}) = -1$. If $(\frac{a}{p}) = 1$, then a is called a quadratic residue modulo 1, otherwise a non-quadratic residue modulo 1.

Let p and q be district odd primes, then the quadratic reciprocity law states that

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

This law first proved by Gauss in 1801 [3], while he was only 19 years old, but he proved six different proof of this law in his life time. Up to present time many different proofs of this law has been published whose number exceeds 150, see [1]. The proofs use number theory, trigonometry, character theory, etc. For an elementary proof see [4]. In this paper we present a proof that uses linear algebra.

2 Preliminaries

Let A be an abelian group. If the composition law in A is written addively a character of A is a function $\chi : A \longrightarrow \mathbb{C}^\times$ such that $\chi(x + y) = \chi(x)\chi(y)$, for all $x, y \in A$, If the law of composition in A is written multiplicatively $\chi(xy) = \chi(x)\chi(y)$, where $\mathbb{C}^\times$ denotes the non-zero complex numbers under multiplication.

*Speaker. Email address: darafsheh@ut.ac.ir

Let p be an odd prime. Then $\chi : \mathbb{Z}_p^\times \longrightarrow \mathbb{C}$ defined by $\chi(a) = (\frac{a}{p})$, $a \in \mathbb{Z}_p^\times$, is a character because of the property of the Legendre symbol $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Let ξ be a primitive pth of unity, i. e. $\xi = e^{\frac{2\pi i}{p}}$. We let $e(x) = e^{2\pi i x}$. The additive group of $\mathbb{Z}_p$ is generated by 1, then the function $\chi : \mathbb{Z}_p \longrightarrow \mathbb{C}^\times$ defined by $\chi(1) = \xi$, extended by $\chi(k) = \xi^k$, is a character of $\mathbb{Z}_p$. All characters of $\mathbb{Z}_p$ are of this type. If $1 \leq r \leq p$, then $\chi_r : \mathbb{Z}_p \longrightarrow \mathbb{C}^\times$ defined by $\chi_r(s) = \xi^{rs}$, $1 \leq s \leq p$, is a character of $\mathbb{Z}_p$ and all the r characters of $\mathbb{Z}_p$ are of this form.

The character table of $\mathbb{Z}_p$ is a $p \times p$ matrix $X = (\xi^{rs})_{1 \leq r,s \leq p}$. If we use the orthogonality relation on the character table of X, [2], we obtain

$$\overline{X}^t X = \begin{bmatrix} p & & & & \\ & p & & \mathbf{0} & \\ & & \ddots & & \\ & \mathbf{0} & & \ddots & \\ & & & & p \end{bmatrix} = pI_p$$

where $\overline{X}$ is the matrix obtained from X by conjugation of entries and t denotes transpose.

If we take the determinate we obtain:

$|\det X|^2 = p^p$. It is known that either $\det X$ is real or pure imaginary. Therefore $\det X = p^{\frac{p}{2}}$ or $\det X = ip^{\frac{p}{2}}$.

3 Main Result

It we take the trace of X we obtain $tr\ X = \sum_{r=1}^{p} \xi^{r^2} = \sum_{r=1}^{p} (\frac{r}{p})\xi^r$.

Corollary 3.1.

$$tr\ X = \begin{cases} \sqrt{p}, & if\ p \equiv 1 (mod 4), \\ i\sqrt{p}, & if\ p \equiv 3 (mod 4). \end{cases}$$

Proof. With respect tour ordering of the rows and columns of the matrix X we have:

$$X = \begin{bmatrix} \xi & \xi^2 & \xi^3 & \dots & \xi^{p-1} & 1 \\ \xi^2 & \xi^4 & \xi^6 & \dots & \xi^{2(p-1)} & 1 \\ \vdots & & \vdots & & & \vdots \\ \xi^{p-1} & \xi^{2(p-1)} & \xi^{3(p-1)} & \dots & \xi^{(p-1)^2} & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}$$

We compute the matrix X^2. If $X^2 = (c_{ij})_{1 \leq i,j \leq p}$, then

$$c_{ij} = \sum_{k=1}^{p} \xi^{rk}\xi^{ks} = \sum_{k=1}^{p} \xi^{k(r+s)} = \begin{cases} p, & if\ p \mid r+s, \\ 0, & otherwise. \end{cases}$$

Therefore

$$X^2 = \begin{bmatrix} 0 & 0 & 0 & \cdots & p & 0 \\ 0 & 0 & \cdots & p & 0 & 0 \\ \vdots & & & \vdots & & \vdots \\ p & 0 & & \cdots & & 0 \\ 0 & 0 & & \cdots & & p \end{bmatrix} = PS$$

where

$$S = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & & & \vdots & & \vdots \\ 1 & 0 & & \cdots & 0 & 0 \\ 0 & 0 & & \cdots & 0 & 1 \end{bmatrix}$$

is the permutation matrix corresponding to the permutation

$$(1 \;\; p-1)(2 \;\; p-2)\cdots(\frac{p-1}{2} \;\; \frac{p+1}{2})(p)$$

of the symmetric group $\mathbb{S}_p$. Therefore we can calculate the eigenvalues of X to be $\pm\sqrt{p}$, $\pm i\sqrt{p}$. Further calculators reveal the trace of X as indicated in the Corollary. □

Definition 3.2. Using the formula for $tr\ X$ we define $G_p(a) = \sum_{r=1}^{p} (\frac{r}{p})\xi^{r^2 a}$, where $(a,p) = 1$ and ξ is a primitive pth root of unity in $\mathbb{C}$.

It is clear that $G_p(1) = tr\ X = \sqrt{p}$ or $i\sqrt{p}$. We set $t(p) = 1$ if $p \equiv 1(mod\ 4)$ and $t(p) = i$ if $p \equiv 3(mod\ 4)$, hence $tr\ X = t(p)\sqrt{p}$.

Lemma 3.3. *Let p and q be distinct odd prime numbers. Then $G_p(q)G_q(p) = G_{pq}(1)$.*

Proof. We have $G_p(q) = \sum_{r=1}^{p} e^{\frac{2\pi i r^2 q}{p}}$ and $G_q(p) = \sum_{s=1}^{q} e^{\frac{2\pi i s^2 p}{q}}$. Therefore

$$\begin{aligned} G_p(q)G_q(p) &= \sum_{r=1}^{p} e^{\frac{2\pi i r^2 q}{p}} \sum_{s=1}^{q} e^{\frac{2\pi i s^2 p}{q}} = \sum_{r=1}^{p}\sum_{s=1}^{q} e^{\frac{2\pi i}{pq}(r^2q^2 + s^2p^2)} \\ &= \sum_{r,s} e^{\frac{2\pi i}{pq}(rq+sp)^2} = G_{pq}(1) \end{aligned}$$

This is because $rq + sp$ forms a complete residue classes moduls pq. □

Theorem 3.4 (quadratic reciprocity law)**.** *Let p and q be district odd primes, then:*

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

Proof. By convention $G_p(1) = t(p)\sqrt{p}$. Thus,

$$t(pq)\sqrt{pq} = G_{pq}(1) = G_p(q)G_q(p) = (\frac{q}{p})(\frac{p}{q})G_p(1)G_q(1) = (\frac{q}{p})(\frac{p}{q})t(p)t(q)\sqrt{pq}$$

Therefore $(\frac{q}{p})(\frac{p}{q})t(p)t(q) = t(pq)$, implying $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$. □

References

[1] O. Baumgurt, *The quadratic reciprocity law*, A collection of classical proofs, Edited and translated by F. Lemmermey, Birkhavsec, 2015.

[2] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge university press, second edition 2001.

[3] C. F. Gauss, *Disquisitiones Arithmetica*, Leipzig, 1801: Worke, Vol. I; English translation by A. A. Clarke, Yale university press, New Haven, 1966.

[4] I. Niven and H. S. Zuekerman, *An introduction to the theory of numbers*, second edition, John Wiley and sons, Inc., New York 1960.