Quadratic Reciprocity via Linear Algebra

Steve Fan

Feburary 7th, 2023

Table of Contents

Quadratic Residues & Non-residues

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. We say that a is a *quadratic residue* (mod p) if the congruence equation $x^2 \equiv a \pmod{p}$ is soluble in $\mathbb{Z}$, i.e., $a \in \mathbb{F}_p^{\times 2}$.

Quadratic Residues & Non-residues

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. We say that a is a *quadratic residue* (mod p) if the congruence equation $x^2 \equiv a \pmod{p}$ is soluble in $\mathbb{Z}$, i.e., $a \in \mathbb{F}_p^{\times 2}$.

An integer $a \in \mathbb{Z}$ is called a *quadratic non-residue* (mod p) if $a \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}$.

Examples

1. $3^2 \equiv 2 \pmod{7} \Rightarrow 2$ is a quadratic residue (mod 7);
2. $\mathbb{F}_{17}^{\times 2} = \{\pm 1, \pm 2, \pm 4, \pm 8\} \Rightarrow 3$ is a quadratic non-residue (mod 17).

Quadratic Residues & Non-residues

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. We say that a is a *quadratic residue* (mod p) if the congruence equation $x^2 \equiv a \pmod{p}$ is soluble in $\mathbb{Z}$, i.e., $a \in \mathbb{F}_p^{\times 2}$.

An integer $a \in \mathbb{Z}$ is called a *quadratic non-residue* (mod p) if $a \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}$.

Examples

1. $3^2 \equiv 2 \pmod{7} \Rightarrow 2$ is a quadratic residue (mod 7);
2. $\mathbb{F}_{17}^{\times 2} = \{\pm 1, \pm 2, \pm 4, \pm 8\} \Rightarrow 3$ is a quadratic non-residue (mod 17).

Facts

1. For any odd prime p, $\#\mathbb{F}_p^{\times 2} = \#(\mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}) = (p-1)/2$.
2. $R \times R = R$, $N \times N = R$, and $R \times N = N$.

The Legendre Symbol

We define the Legendre symbol by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \in \mathbb{F}_p^{\times 2}, \\ -1, & \text{if } a \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}, \\ 0, & \text{if } p \mid a. \end{cases}$$

Then Fact 2 can be reformulated as

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for $a, b \in \mathbb{F}_p^{\times}$.

The Legendre Symbol

We define the Legendre symbol by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \in \mathbb{F}_p^{\times 2}, \\ -1, & \text{if } a \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}, \\ 0, & \text{if } p \mid a. \end{cases}$$

Then Fact 2 can be reformulated as

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for $a, b \in \mathbb{F}_p^{\times}$.

Proposition 1.1 (Euler's Criterion)

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Theorem 1.2 (Euler)

For any odd prime p, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

The Law of Quadratic Reciprocity

Theorem 1.2 (Euler)

For any odd prime p, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem 1.3 (Law of Quadratic Reciprocity)

Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

The Law of Quadratic Reciprocity

Theorem 1.2 (Euler)

For any odd prime p, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem 1.3 (Law of Quadratic Reciprocity)

Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Example

3 is a quadratic non-residue (mod 17), because

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Counting Proofs of Theorem 1.3

There are now over 240 published proofs!

1. Induction
2. Binary quadratic forms
3. Gauss sums
4. Lattice points counting
5. Trigonometric functions
6. Galois theory applied to cyclotomic fields
7. Matrix theory
8. Fourier analysis on $\mathbb{Z}/N\mathbb{Z}$
9. Dedekind sums
10. Brauer groups
11. K-groups
12. Formal groups
13. Theta functions
14. Recurring sequences
15. Elliptic curves
16. Quaternion algebras

. . .

I will present a simple, elementary proof, essentially due to Schur, based on tools from linear algebra.

Table of Contents

Starting with A Matrix

It all starts with the symmetric matrix $A = (\zeta_n^{rs})$:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \dots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \dots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \zeta_n^9 & \dots & \zeta_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \dots & \zeta_n^{(n-1)^2} \end{bmatrix},$$

where $n \in \mathbb{N}$ is odd and $\zeta_n := e^{2\pi i/n}$.

Starting with A Matrix

It all starts with the symmetric matrix $A = (\zeta_n^{rs})$:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \zeta_n^3 & \dots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \zeta_n^6 & \dots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \zeta_n^9 & \dots & \zeta_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \zeta_n^{3(n-1)} & \dots & \zeta_n^{(n-1)^2} \end{bmatrix},$$

where $n \in \mathbb{N}$ is odd and $\zeta_n := e^{2\pi i/n}$. Note that A is an $n \times n$ Vandermonde matrix with trace

$$\operatorname{tr}(A) = \sum_{r=0}^{n-1} \zeta_n^{r^2}.$$

The Magic within A^2

One can compute

$$A^2 = \begin{bmatrix} n & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & n \\ 0 & 0 & 0 & \dots & 0 & n & 0 \\ 0 & 0 & 0 & \dots & n & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & n & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

The Magic within A^2

One can compute

$$A^2 = \begin{bmatrix} n & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & n \\ 0 & 0 & 0 & \dots & 0 & n & 0 \\ 0 & 0 & 0 & \dots & n & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & n & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

Note that A^2/n is a permutation matrix with determinant $(-1)^{\frac{n-1}{2}}$. So $\det(A^2) = (-1)^{\frac{n-1}{2}} n^n$.

The Determinant of A

We compute the determinant of A as follows:

$$\det(A) = \prod_{0 \le s < r \le n-1} (\zeta_n^r - \zeta_n^s) = \prod_{0 \le s < r \le n-1} \zeta_{2n}^{r+s} \left(\zeta_{2n}^{r-s} - \zeta_{2n}^{-(r-s)} \right).$$

The Determinant of A

We compute the determinant of A as follows:

$$\det(A) = \prod_{0 \le s < r \le n-1} (\zeta_n^r - \zeta_n^s) = \prod_{0 \le s < r \le n-1} \zeta_{2n}^{r+s} \left(\zeta_{2n}^{r-s} - \zeta_{2n}^{-(r-s)} \right).$$

Observe

$$\begin{aligned} 2 \sum_{0 \le s < r \le n-1} (r+s) &= \sum_{0 \le s < r \le n-1} (r+s) + \sum_{0 \le r < s \le n-1} (r+s) \\ &= \sum_{r,s=0}^{n-1} (r+s) - \sum_{r=0}^{n-1} 2r \\ &= 2n \sum_{r=0}^{n-1} r - 2 \sum_{r=0}^{n-1} r \\ &= 2(n-1) \cdot \frac{n(n-1)}{2} = n(n-1)^2. \end{aligned}$$

The Determinant of A

So

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

The Determinant of A

So

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

Hence

$$\det(A)=\prod_{0\le s<r\le n-1}\left(\zeta_{2n}^{r-s}-\zeta_{2n}^{-(r-s)}\right)=i^{\frac{n(n-1)}{2}}P_n,$$

where

$$P_n:=\prod_{0\le s<r\le n-1}2\sin\frac{(r-s)\pi}{n}>0.$$

It is clear that $\det(A^2)=\det(A)^2=(-1)^{\frac{n-1}{2}}P_n^2$.

The Determinant of A

So

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

Hence

$$\det(A)=\prod_{0\le s<r\le n-1}\left(\zeta_{2n}^{r-s}-\zeta_{2n}^{-(r-s)}\right)=i^{\frac{n(n-1)}{2}}P_n,$$

where

$$P_n:=\prod_{0\le s<r\le n-1}2\sin\frac{(r-s)\pi}{n}>0.$$

It is clear that $\det(A^2)=\det(A)^2=(-1)^{\frac{n-1}{2}}P_n^2$. But we just proved that $\det(A^2)=(-1)^{\frac{n-1}{2}}n^n$. Therefore, $P_n=n^{\frac{n}{2}}$ and $\det(A)=i^{\frac{n(n-1)}{2}}n^{\frac{n}{2}}$.

The Trace of A

Recall that

$$\mathrm{tr}(A) = \sum_{r=0}^{n-1} \zeta_n^{r^2}.$$

The Trace of A

Recall that

$$\mathrm{tr}(A) = \sum_{r=0}^{n-1} \zeta_n^{r^2}.$$

From this it follows that

$$\begin{aligned} |\mathrm{tr}(A)|^2 &= \sum_{r,s=0}^{n-1} \zeta_n^{r^2-s^2} = \sum_{r,s=0}^{n-1} \zeta_n^{(r+s)(r-s)} \\ &= \sum_{t=0}^{n-1} \sum_{s=0}^{n-1} \zeta_n^{(t+2s)t} \qquad (t = r-s) \\ &= n, \end{aligned}$$

which gives $|\mathrm{tr}(A)| = \sqrt{n}$.

The Magic Continues!

Let us revisit

$$A^2 = \begin{bmatrix} n & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & n \\ 0 & 0 & 0 & \dots & 0 & n & 0 \\ 0 & 0 & 0 & \dots & n & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & n & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

One can show that $A^4 = n^2 I$ and that A^2 has eigenvalues n with multiplicity $(n+1)/2$ and $-n$ with multiplicity $(n-1)/2$.

The Magic Continues!

Let us revisit

$$A^2 = \begin{bmatrix} n & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & n \\ 0 & 0 & 0 & \dots & 0 & n & 0 \\ 0 & 0 & 0 & \dots & n & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & n & 0 & \dots & 0 & 0 & 0 \end{bmatrix}.$$

One can show that $A^4 = n^2 I$ and that A^2 has eigenvalues n with multiplicity $(n+1)/2$ and $-n$ with multiplicity $(n-1)/2$.

Suppose that A has eigenvalues $i^k\sqrt{n}$ with multiplicity a_k for each $k \in \{0, 1, 2, 3\}$. Then

$$a_0 + a_2 = \frac{n+1}{2} \quad \text{and} \quad a_1 + a_3 = \frac{n-1}{2}.$$

The Magic Continues!

Since $\mathrm{tr}(A) = [(a_0 - a_2) + i(a_1 - a_3)]\sqrt{n}$, we have

$$n = |\mathrm{tr}(A)|^2 = [(a_0 - a_2)^2 + (a_1 - a_3)^2]n,$$

which yields

$$(a_0 - a_2)^2 + (a_1 - a_3)^2 = 1.$$

The Magic Continues!

Since $\mathrm{tr}(A) = [(a_0 - a_2) + i(a_1 - a_3)]\sqrt{n}$, we have

$$n = |\mathrm{tr}(A)|^2 = [(a_0 - a_2)^2 + (a_1 - a_3)^2]n,$$

which yields

$$(a_0 - a_2)^2 + (a_1 - a_3)^2 = 1.$$

Moreover,

$$i^{\frac{n(n-1)}{2}} n^{\frac{n}{2}} = \det(A) = \prod_{k=0}^{3} (i^k \sqrt{n})^{a_k} = i^{a_1+2a_2+3a_3} n^{\frac{n}{2}},$$

which implies

$$a_1 + 2a_2 + 3a_3 \equiv \frac{n(n-1)}{2} \pmod 4.$$

The Trace of A

In summary, we have proved the following:

1. $$\mathrm{tr}(A) = \sum_{r=0}^{n-1} \zeta_n^{r^2} = [(a_0 - a_2) + i(a_1 - a_3)]\sqrt{n}.$$
2. $$a_0 + a_2 = \frac{n+1}{2} \quad \text{and} \quad a_1 + a_3 = \frac{n-1}{2}.$$
3. $$(a_0 - a_2)^2 + (a_1 - a_3)^2 = 1, \quad a_k \in \mathbb{Z}_{\geq 0}.$$
4. $$a_1 + 2a_2 + 3a_3 \equiv \frac{n(n-1)}{2} \pmod 4.$$

Combining these four facts, one can obtain

$$\mathrm{tr}(A) = \sum_{r=0}^{n-1} \zeta_n^{r^2} = \begin{cases} \sqrt{n}, & \text{if } n \equiv 1 \pmod 4, \\ i\sqrt{n}, & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Table of Contents

Gauss Sums

For $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we define

$$S_n(m) := \sum_{r=0}^{n-1} \zeta_n^{r^2 m},$$

so that $\mathrm{tr}(A) = S_n(1)$.

Gauss Sums

For $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we define

$$S_n(m) := \sum_{r=0}^{n-1} \zeta_n^{r^2 m},$$

so that $\mathrm{tr}(A) = S_n(1)$.

Proposition 3.1

Given $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, we have $S_m(n)S_n(m) = S_{mn}(1)$.

Gauss Sums

For $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we define

$$S_n(m) := \sum_{r=0}^{n-1} \zeta_n^{r^2 m},$$

so that $\mathrm{tr}(A) = S_n(1)$.

Proposition 3.1

Given $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$, we have $S_m(n)S_n(m) = S_{mn}(1)$.

Let p be an odd prime. We define the *Gauss sum* $G_p(m)$ by

$$G_p(m) := \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta_p^{rm}.$$

Clearly, $G_p(m) = 0$ if $p \mid m$.

Gauss Sums

The relationship between S and G can be deduced as follows:

$$S_p(m) = \sum_{r=0}^{p-1} \zeta_p^{r^2 m} = \sum_{r=0}^{p-1} \left(1 + \left(\frac{r}{p}\right)\right) \zeta_p^{rm} = G_p(m).$$

Gauss Sums

The relationship between S and G can be deduced as follows:

$$S_p(m) = \sum_{r=0}^{p-1} \zeta_p^{r^2 m} = \sum_{r=0}^{p-1} \left(1 + \left(\frac{r}{p}\right)\right) \zeta_p^{rm} = G_p(m).$$

Moreover, the values of $G_p(m)$ are completely determined by (m/p) and $G_p(1)$:

$$\begin{aligned} G_p(m) &= \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta_p^{rm} = \left(\frac{m}{p}\right) \sum_{r=0}^{p-1} \left(\frac{rm}{p}\right) \zeta_p^{rm} \\ &= \left(\frac{m}{p}\right) \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta_p^{r} = \left(\frac{m}{p}\right) G_p(1), \end{aligned}$$

provided that $p \nmid m$.

Table of Contents

Proof of Quadratic Reciprocity

Let p and q be distinct odd primes. We have seen that

$$S_p(1) = G_p(1) = \mathrm{tr}(A) = \delta(p)\sqrt{p}$$

for $n = p$, where

$$\delta(p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ i, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof of Quadratic Reciprocity

Let p and q be distinct odd primes. We have seen that

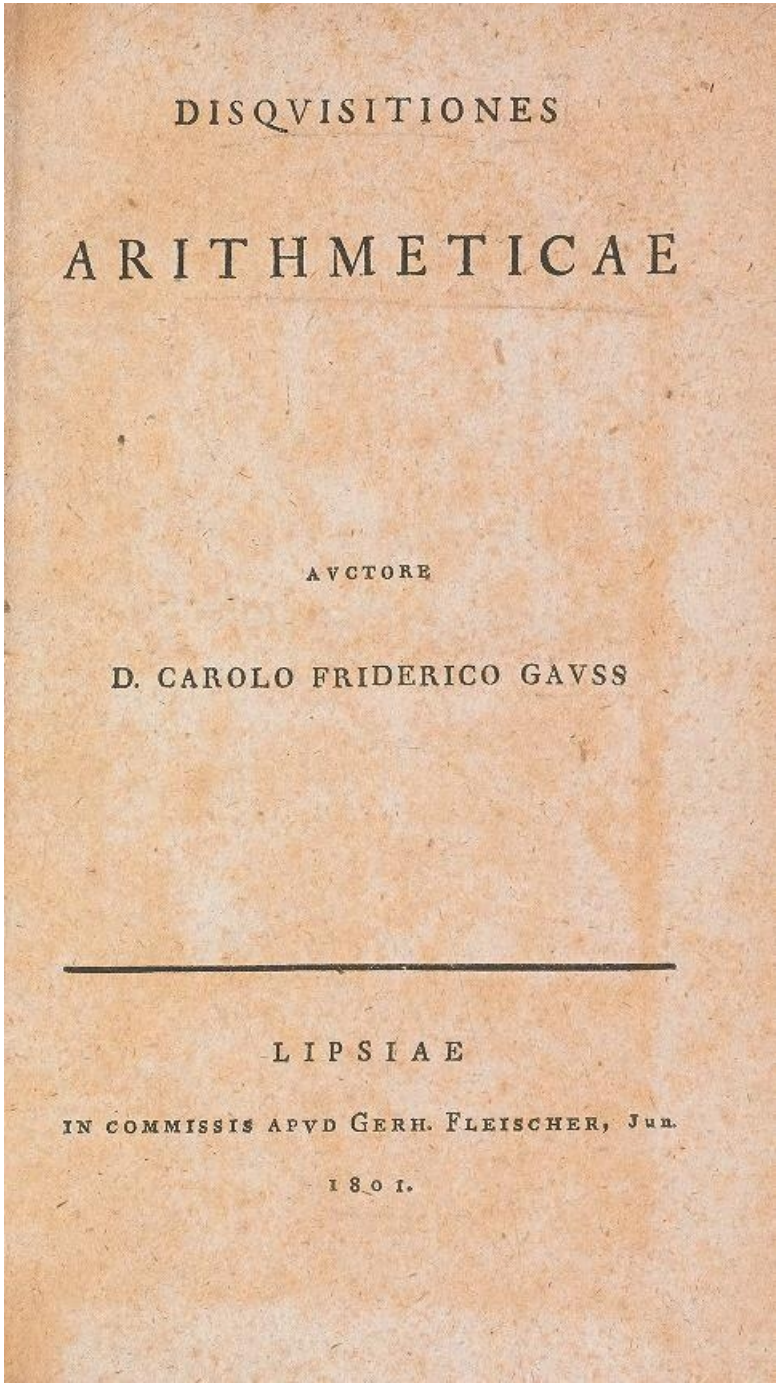
$$S_p(1) = G_p(1) = \mathrm{tr}(A) = \delta(p)\sqrt{p}$$

for $n = p$, where

$$\delta(p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ i, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

By Proposition 3.1, we have

$$\begin{aligned} \delta(pq)\sqrt{pq} = G_{pq}(1) = G_q(p)G_p(q) &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) G_q(1)G_p(1) \\ &= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\delta(p)\delta(q)\sqrt{pq}. \qquad Q.E.D. \end{aligned}$$


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

The fundamental theorem must certainly be regarded as one of the most elegant of its type.

— *C. F. Gauss*