Quadratic Residues

Tristan Shin

29 Sep 2018

In this handout, we investigate quadratic residues and their properties and applications. Unless otherwise specified, p is an odd prime.

1 Basic Properties

Definition. We say that an integer m is a *quadratic residue* (QR) mod n if there exists an integer x for which $x^2 \equiv m \pmod{n}$.

Definition. We say that an integer m is a *quadratic non-residue* (QNR) mod n if it is not a quadratic residue.

Example 1.1

0 and 1 are always quadratic residues mod n.

Definition. A QR $m \pmod{n}$ is a *non-zero QR* if $m \not\equiv 0 \pmod{n}$.

We use the *Legendre symbol* to help keep track of when an integer is a QR.

Definition. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a non-zero QR mod } p \\ -1 & \text{if } a \text{ is a QNR mod } p. \end{cases}$$

It is clear that $a \equiv b \pmod{p}$ implies $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Lemma 1.2: Euler's Criterion

For all positive integers a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Proof. If $p \mid a$, this is obvious, so assume $p \nmid a$. If a is a QR mod p, then let $a \equiv x^2 \pmod{p}$. Then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Otherwise, suppose that a is a QNR mod p. The roots of the polynomial $X^{\frac{p-1}{2}} - 1$ in $\mathbb{F}_p$ are already identified as the $\frac{p-1}{2}$ non-zero QRs mod p, so $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. But $p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ by Fermat's Little Theorem, so $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Hence this equivalence is true. ■

Corollary 1.3

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

Remark. Because the Legendre symbol $\left(\frac{a}{p}\right)$ makes sense as long as $a \pmod p$ makes sense, we can write things like $\left(\frac{1/5}{7}\right) = \left(\frac{3}{7}\right) = -1$. Specifically, we also have

$$\left(\frac{1/a}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{1/a}{p}\right) = \left(\frac{a}{p}\right).$$

2 Quadratic Reciprocity

Theorem 2.1: Quadratic Reciprocity

If p and q are distinct odd primes, then

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

In other words, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv 3 \pmod 4$.

To prove this, we first prove a lemma.

Lemma 2.2: Eisenstein's Lemma

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\lfloor 2kq/p\rfloor}$$

for an odd prime p and arbitrary prime $q \neq p$.

Proof. We use the notation that $(m\%n)$ gives the remainder when m is divided by n. Consider the numbers $r(k) = \left((-1)^{(2kq\%p)}(2kq\%p)\%p\right)$ for $k = 1, 2, \ldots, \frac{p-1}{2}$. If $(2kq\%p)$ is even, then this is just $(2kq\%p)$. If $(2kq\%p)$ is odd, then this is $p - (2kq\%p)$. Either way, this is an even integer between 0 and $p-1$, inclusive.

Note that $r(k) \equiv (-1)^{(2kq\%p)}2kq \pmod p$. Observe that $r(k) \neq 0$ otherwise $k \equiv 0 \pmod p$, so $r(k) \in \{2, 4, \ldots, p-1\}$. Now, if $r(k_1) = r(k_2)$, then

$$(-1)^{(2k_1q\%p)}2k_1q \equiv (-1)^{(2k_2q\%p)}2k_2q \pmod p,$$

so $k_1 \equiv \pm k_2 \pmod p$. Since $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, we have that the $r(k)$ are distinct.

Thus,

$$\begin{aligned}2\times 4\times\cdots\times(p-1) &\equiv r(1)\times r(2)\times\cdots\times r\left(\frac{p-1}{2}\right)\\ &\equiv(-1)^{(2q\%p)}2q\times(-1)^{(4q\%p)}4q\times\cdots\times(-1)^{((p-1)q\%p)}(p-1)q \pmod p\\ &\equiv(-1)^{\sum_{k=1}^{(p-1)/2}(2kq\%p)}2\times 4\times\cdots\times(p-1)q^{\frac{p-1}{2}} \pmod p.\end{aligned}$$

But note that $2kq = p\left\lfloor\frac{2kq}{p}\right\rfloor + (2kq\%p)$, so $\left\lfloor\frac{2kq}{p}\right\rfloor \equiv (2kq\%p) \pmod 2$, hence we have that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}(2kq\%p)} = (-1)^{\sum_{k=1}^{(p-1)/2}\lfloor 2kq/p\rfloor}$$

as desired. ■

Now, we complete the proof of quadratic reciprocity.

Proof. It suffices to show that $\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{2kq}{p}\right\rfloor+\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{2kp}{q}\right\rfloor$ and $\frac{p-1}{2}\cdot\frac{q-1}{2}$ have the same parity.

Observe that when $k>\frac{p}{2}$, $\left\lfloor\frac{2kq}{p}\right\rfloor \equiv q-1-\left\lfloor\frac{2kq}{p}\right\rfloor \pmod 2$ but

$$\begin{aligned}q-1-\left\lfloor\frac{2kq}{p}\right\rfloor &= q-1-\frac{2kq}{p}+\left\{\frac{2kq}{p}\right\} = \frac{(p-2k)q}{p}-\left(1-\left\{\frac{2kq}{p}\right\}\right)\\ &= \frac{(p-2k)q}{p}-\left\{\frac{(p-2k)q}{p}\right\} = \left\lfloor\frac{(p-2k)q}{p}\right\rfloor,\end{aligned}$$

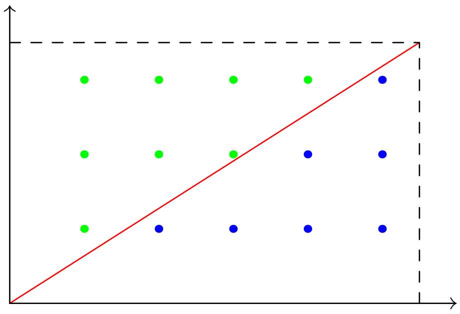
so $\left\lfloor\frac{2kq}{p}\right\rfloor \equiv \left\lfloor\frac{(p-2k)q}{p}\right\rfloor \pmod 2$. Hence

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{2kq}{p}\right\rfloor \equiv \sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor \pmod 2.$$

Similarly,

$$\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{2kp}{q}\right\rfloor \equiv \sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor \pmod 2.$$

Now, consider the lattice grid with $0<x<\frac{p}{2}$ and $0<y<\frac{q}{2}$, as well as the dividing diagonal $y=\frac{q}{p}x$. Note that there are no lattice points in the grid on the diagonal. Since $\left\lfloor\frac{jq}{p}\right\rfloor$ counts the number of lattice points in the grid below or on the diagonal with x-coordinate j, we have that $\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor$ gives the number of lattice points in the grid below the diagonal. Similarly, $\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor$ gives the number of lattice points in the grid to the left of the diagonal.



But these encompass all points in the grid, of which there are $\frac{p-1}{2}\cdot\frac{q-1}{2}$, so we have the identity

$$\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor+\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

and hence the congruence mod 2 is proven, so the proof is complete. ■

Lemma 2.3

$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Proof. The value of $\left(\frac{-1}{p}\right)$ is obvious by Euler's Criterion. To compute $\left(\frac{2}{p}\right)$, use Eisenstein's Lemma. It suffices to show that $\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{4k}{p}\right\rfloor$ is even if and only if $p\equiv\pm1\pmod 8$. But $\left\lfloor\frac{4k}{p}\right\rfloor\le\left\lfloor\frac{2p-2}{p}\right\rfloor<2$, so $\left\lfloor\frac{4k}{p}\right\rfloor$ is odd if and only if it equals 1. This is equivalent to $1\le\frac{4k}{p}<2$, or $\frac{p}{4}\le k<\frac{p}{2}$. If $p\equiv1\pmod 4$, there are $\frac{p-1}{2}-\frac{p+3}{4}+1=\frac{p-1}{4}$ such k, while if $p\equiv3\pmod 4$, there are $\frac{p-1}{2}-\frac{p+1}{4}+1=\frac{p+1}{4}$ such k. This is even if and only if $p\equiv\pm1\pmod 8$, as desired. ■

Using a combination of quadratic reciprocity and lemma 2.3, we can easily compute $\left(\frac{a}{p}\right)$ by using prime factorization.

Example 2.4

$$\begin{aligned}\left(\frac{167}{101}\right)&=\left(\frac{66}{101}\right)=\left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{11}{101}\right)=(-1)\left(\frac{101}{3}\right)\left(\frac{101}{11}\right)\\&=(-1)\left(\frac{2}{3}\right)\left(\frac{2}{11}\right)=(-1)(-1)(-1)=-1\end{aligned}$$

2.1 Jacobi Symbol

Definition. For an arbitrary positive integer $n = p_1 p_2 \cdots p_k$ the product of k (not necessarily distinct) odd primes, we define the *Jacobi symbol* $\left(\frac{a}{n}\right)$ to be

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

Theorem 2.5

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

(b) $\left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$

(c) If $a \equiv b \pmod{c}$, then $\left(\frac{a}{c}\right) = \left(\frac{b}{c}\right)$.

(d) If m, n are odd and relatively prime, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

(e) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

(f) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Proof. (a) Let $c = p_1 p_2 \cdots p_k$, then

$$\left(\frac{ab}{c}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right).$$

(b) Let $b = p_1 p_2 \cdots p_k$ and $c = q_1 q_2 \cdots q_l$, then

$$\left(\frac{a}{bc}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)\sum_{j=1}^{l}\left(\frac{a}{q_j}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right).$$

(c) Let $c = p_1 p_2 \cdots p_k$, then

$$\left(\frac{a}{c}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{b}{p_i}\right) = \left(\frac{b}{c}\right).$$

(d) Let $m = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_l$, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

It suffices to show that the count of (p_i, q_j) that are $(3,3) \pmod{4}$ is odd if and only if $(m,n) \equiv (3,3) \pmod{4}$. But the count of such (p_i, q_j) is odd if and only if there are an odd number of $p_i \equiv 3 \pmod{4}$ and $q_j \equiv 3 \pmod{4}$. This is equivalent to m and n are both $3 \pmod{4}$ as desired.

(e) Note that
$$\left(\frac{-1}{bc}\right) = \left(\frac{-1}{b}\right)\left(\frac{-1}{c}\right) = (-1)^{\frac{b-1}{2}+\frac{c-1}{2}} = (-1)^{\frac{bc-1}{2}}$$
if b and c are both odd, so we can induct on the number of primes that n is a product of.

(f) Note that
$$\left(\frac{2}{bc}\right) = \left(\frac{2}{b}\right)\left(\frac{2}{c}\right) = (-1)^{\frac{b^2-1}{8}+\frac{c^2-1}{8}} = (-1)^{\frac{b^2c^2-1}{8}}$$
if b and c are both odd, so we can induct on the number of primes that n is a product of.

■

Example 2.6

$$\begin{aligned}\left(\frac{167}{101}\right) &= \left(\frac{66}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{33}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{101}{33}\right)\\ &= \left(\frac{2}{101}\right)\left(\frac{2}{33}\right) = \left(\frac{2}{3333}\right) = -1\end{aligned}$$

Example 2.7

Is it possible that $\left(\frac{m}{n}\right) = 1$ but m is a QNR mod n?

3 Legendre Symbol Sums

There are many sums that we can easily compute involving the Legendre symbol.

Theorem 3.1

$$\sum_{n=0}^{p-1}\left(\frac{n}{p}\right) = 0$$

Proof. There are $\frac{p-1}{2}$ non-zero QRs and $\frac{p-1}{2}$ QNRs, so they cancel out. ■

Theorem 3.2

There are $\left\lceil \frac{p}{4} \right\rceil$ residues $a \in \mathbb{F}_p$ such that a and $a+1$ are both QRs.

Proof. Consider the quantity $\frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)$ for $a \neq 0, -1$. If a and $a+1$ are both QRs, this is 1. If either is a QNR, this is 0. Thus, $\sum_{a=1}^{p-2} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)$ gives the count of valid a when $1 \leq a \leq p-2$. Clearly $a=0$ is valid and $a=-1$ is valid only if $\frac{1}{2}\left(1+\left(\frac{-1}{p}\right)\right)=1$ (otherwise it equals 0), so the total count is

$$1+\frac{1}{2}\left(1+\left(\frac{-1}{p}\right)\right)+\sum_{a=1}^{p-2} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right).$$

Since $\frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)$ is $\frac{1}{2}$ at $a=0$ and $\frac{1}{4}\left(1+\left(\frac{-1}{p}\right)\right)$ at $a=-1$, this sum is equal to

$$\begin{aligned}&\frac{1}{2}+\frac{1}{4}\left(1+\left(\frac{-1}{p}\right)\right)+\sum_{a=0}^{p-1} \frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)\\ &=\frac{3+(-1)^{\frac{p-1}{2}}}{4}+\frac{1}{4}\sum_{a=0}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right).\end{aligned}$$

Examine the sum. It is also equal to

$$\sum_{a=0}^{p-1} 1+\left(\frac{a}{p}\right)+\left(\frac{a+1}{p}\right)+\left(\frac{a^2+a}{p}\right).$$

The sum of the 1's is clearly p. The sum of the $\left(\frac{a}{p}\right)$ and $\left(\frac{a+1}{p}\right)$ terms are 0 by Theorem 3.1. So it suffices to compute the sum of $\left(\frac{a^2+a}{p}\right)=\left(\frac{1+1/a}{p}\right)$ for $a \neq 0$. As a ranges from 1 to $p-1$, $1+1/a$ ranges between 0 and $p-1$ except for 1. Hence the sum of $\left(\frac{a^2+a}{p}\right)$ is $\left(\frac{0}{p}\right)=0$ plus $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)-\left(\frac{1}{p}\right)=-1$. Thus, we have that the sum evaluates to $p-1$ and hence the total count is $\frac{p+2+(-1)^{\frac{p-1}{2}}}{4}=\left\lceil\frac{p}{4}\right\rceil$ as desired. ∎

Theorem 3.3

$$\sum_{n=0}^{p-1}\left(\frac{(n-a)(n-b)}{p}\right)=\begin{cases}-1 & \text{if } a \neq b\\ p-1 & \text{if } a=b\end{cases}$$

Proof. If $a=b$, the result is clear (the summand is 1 unless $n=a$ in which case it is 0). Otherwise, replace n with $n+a$ and take the indices mod p so this is $\sum_{n=0}^{p-1}\left(\frac{n^2+(a-b)n}{p}\right)=\sum_{n=1}^{p-1}\left(\frac{1+(a-b)/n}{p}\right)$. As before, $1+(a-b)/n$ takes on the values besides 1, so this sum is $\sum_{m=1}^{p-1}\left(\frac{m}{p}\right)-\left(\frac{1}{p}\right)=-1$. ∎

4 Gauss Sums

Gauss sums are a special type of Legendre Symbol Sums.

Definition. The Gauss sum g_p is $\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^n$, where $\zeta = e^{i\cdot\frac{2\pi}{p}}$.

Theorem 4.1

$g_p^2 = p^*$, where $p^* = (-1)^{\frac{p-1}{2}}p$.

Proof. Observe that

$$g_p\overline{g_p} = \sum_{n=0}^{p-1}\sum_{m=0}^{p-1}\left(\frac{nm}{p}\right)\zeta^{n-m} = \sum_{d=0}^{p-1}\zeta^d\sum_{n=0}^{p-1}\left(\frac{n\left(n-d\right)}{p}\right).$$

By Theorem 3.3, the inner sum is -1 unless $d=0$ in which case it is $p-1$. Thus,

$$g_p\overline{g_p} = (p-1) - \sum_{d=1}^{p-1}\zeta^d = p.$$

But

$$\overline{g_p} = \sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\zeta^{-m} = \sum_{m=0}^{p-1}\left(\frac{-m}{p}\right)\zeta^{m} = (-1)^{\frac{p-1}{2}}g_p,$$

hence $g_p^2 = (-1)^{\frac{p-1}{2}}p$. ■

Theorem 4.2

$$g_p = \begin{cases}\sqrt{p} & \text{if } p\equiv 1 \pmod 4\\ i\sqrt{p} & \text{if } p\equiv 3 \pmod 4\end{cases}$$

Proof. Consider the polynomials

$$g\left(X\right) = \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)X^n$$

so that $g\left(\zeta\right) = g_p$ and

$$h\left(X\right) = \prod_{k=1}^{\frac{p-1}{2}}\left(X^{-k/2} - X^{k/2}\right),$$

where exponents in the definition of h are taken mod p.

We know from above that $g(\zeta)^2 = p^*$. We show that $h(\zeta)^2 = p^*$. Observe that

$$h(\zeta)^2 = \prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{-k/2} - \zeta^{k/2}\right)^2 = \prod_{k=1}^{\frac{p-1}{2}} \left(\zeta^{-k} - 1\right)\left(1 - \zeta^k\right)$$
$$= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{p-1} \left(1 - \zeta^k\right) = (-1)^{\frac{p-1}{2}} \Phi_p(1) = (-1)^{\frac{p-1}{2}} p,$$

hence $h(\zeta)^2 = p^* = g(\zeta)^2$. Thus, $g(\zeta) = \epsilon h(\zeta)$ for some $\epsilon \in \{1, -1\}$. Then ζ is a root of the polynomial $g(X) - \epsilon h(X)$. Since the minimal polynomial of ζ is Φ_p, we have that $\Phi_p(X)$ must divide $g(X) - \epsilon h(X)$. In other words, there exists a polynomial $d(X)$ such that

$$g(X) - \epsilon h(X) = \Phi_p(X)\, d(X).$$

Taking this mod p,

$$g(X) - \epsilon h(X) \equiv (X-1)^{p-1} d(X)$$

since $\Phi_p(X) = \frac{X^p - 1}{X-1} \equiv \frac{(X-1)^p}{X-1} = (X-1)^{p-1}$ by the Frobenius endomorphism. Then $g(X) \equiv \epsilon h(X) \pmod{(X-1)^{p-1}}$ in $\mathbb{F}_p$, so $g(X) \equiv \epsilon h(X) \pmod{(X-1)^{\frac{p+1}{2}}}$ in $\mathbb{F}_p$. Write $Y = X - 1$ so that $g(1+Y) \equiv \epsilon h(1+Y) \pmod{Y^{\frac{p+1}{2}}}$ in $\mathbb{F}_p$.

First, let us expand $g(1+Y)$ in $\mathbb{F}_p$. It is

$$g(1+Y) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)(1+Y)^n$$
$$= \sum_{n=0}^{p-1} \sum_{m=0}^{n} \left(\frac{n}{p}\right)\binom{n}{m} Y^m$$
$$= \sum_{m=0}^{p-1} \left(\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right)\right) Y^m.$$

Suppose that $m < \frac{p-1}{2}$. Consider the sum $\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right)$ mod p. If we write $\binom{n}{m} = \frac{1}{m!}\left(a_{m,m}n^m + a_{m,m-1}n^{m-1} + \ldots + a_{m,1}n + a_{m,0}\right)$ as a polynomial in n, we get that this is

$$\sum_{n=m}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right) = \sum_{n=0}^{p-1} \binom{n}{m}\left(\frac{n}{p}\right)$$
$$\equiv \sum_{n=0}^{p-1} \sum_{j=0}^{m} \frac{a_{m,j}}{m!} n^j n^{\frac{p-1}{2}}$$
$$= \sum_{j=0}^{m} \frac{a_{m,j}}{m!} \sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}}.$$

Take a primitive root e in $\mathbb{F}_p$. Then

$$\sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}} \equiv \sum_{n=0}^{p-1} (en)^{j+\frac{p-1}{2}} = e^{j+\frac{p-1}{2}} \sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}}$$

and since $0 < j + \frac{p-1}{2} < p-1$, $e^{j+\frac{p-1}{2}} \not\equiv 1$ and hence $\sum_{n=0}^{p-1} n^{j+\frac{p-1}{2}} \equiv 0 \pmod{p}$. Thus, $\sum_{n=m}^{p-1} \binom{n}{m} \left(\frac{n}{p}\right) \equiv 0 \pmod{p}$. On the other hand, if $m = \frac{p-1}{2}$, then

$$\sum_{n=m}^{p-1} \binom{n}{m} \left(\frac{n}{p}\right) \equiv \sum_{j=0}^{m} \frac{a_{m,j}}{m!} \sum_{n=0}^{p-1} n^{m+\frac{p-1}{2}} \equiv \frac{a_{m,m}}{m!} (p-1) = -\frac{a_{m,m}}{m!}$$

by the above work and Fermat's Little Theorem. It is obvious that $a_{m,m} = 1$, so this sum evaluates to $-\frac{1}{\left(\frac{p-1}{2}\right)!} \pmod{p}$. Hence

$$g(1+Y) \equiv -\frac{1}{\left(\frac{p-1}{2}\right)!} Y^{\frac{p-1}{2}} \pmod{Y^{\frac{p+1}{2}}}$$

in $\mathbb{F}_p$.

Now, let us expand $h(1+Y)$ in $\mathbb{F}_p$. Observe that

$$(1+Y)^{-k/2} - (1+Y)^{k/2} \equiv \left(1 - \frac{k}{2}Y\right) - \left(1 + \frac{k}{2}Y\right) \equiv -kY \pmod{Y^2}$$

in $\mathbb{F}_p$, so

$$h(1+Y) \equiv (-1)(-2)\cdots\left(-\frac{p-1}{2}\right) Y^{\frac{p-1}{2}} \equiv \left(\frac{p+1}{2}\right) \cdots (p-2)(p-1) Y^{\frac{p-1}{2}} \pmod{Y^{\frac{p+1}{2}}}$$

in $\mathbb{F}_p$.

Combining these, we have that

$$-\frac{1}{\left(\frac{p-1}{2}\right)!} Y^{\frac{p-1}{2}} \equiv \epsilon \left(\frac{p+1}{2}\right) \cdots (p-2)(p-1) Y^{\frac{p-1}{2}} \pmod{Y^{\frac{p+1}{2}}}$$

in $\mathbb{F}_p$. Dividing out, this implies that

$$-1 \equiv \epsilon (p-1)! \pmod{Y}$$

in $\mathbb{F}_p$. But $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem, so $\epsilon = 1$ and hence $g(\zeta) = h(\zeta)$.

Now, check that $\zeta^{-k/2} - \zeta^{k/2} = -2i \sin \frac{2\pi(k/2)}{p}$ ($k/2$ taken mod p) is a positive multiple of i, specifically $2i \sin \frac{\pi k}{p}$, when k is odd and a negative multiple of i, specifically $-2i \sin \frac{\pi k}{p}$, when k is even. Thus, there is always the same number of minus signs as there are complete copies of $i^2 = -1$ in the product representation of $h(\zeta)$, so $h(\zeta) = g_p$ is always a positive real or a positive multiple of i. The conclusion follows from Theorem 4.1. ■

We can actually prove quadratic reciprocity using Theorem 4.1.

Proof. Observe that

$$g_p^{q-1} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q},$$

so $g_p^q \equiv \left(\frac{p^*}{q}\right) g_p \pmod q$ (here we use an extension of $\mathbb{F}_p$ that includes ζ). But at the same time, by the Frobenius Endomorphism,

$$g_p^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{qn} \equiv \left(\frac{q}{p}\right) \sum_{n=0}^{p-1} \left(\frac{qn}{p}\right) \zeta^{qn} \equiv \left(\frac{q}{p}\right) g_p \pmod q.$$

Then since g_p is non-zero mod q, this implies that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, which can be unravelled to deduce reciprocity. ■

5 Problems

Here are some assorted problems about quadratic residues.

1. Prove that $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.
2. If m and n are relatively prime and n is an odd positive integer such that m is a quadratic residue mod n, prove that $\left(\frac{m}{n}\right) = 1$.
3. (2018 MP4G #18) Evaluate the expression
$$\left| \prod_{k=0}^{15} \left(1 + e^{2\pi i k^2/31}\right) \right|.$$
4. Prove that if n is a quadratic residue mod p for an odd prime p, then n is quadratic residue mod p^k for any positive integer k.
5. If $a^2 + b^2 = p$ is a prime and a is odd, prove that a is a quadratic residue mod p.
6. Let $p \equiv 1 \pmod 4$ be a prime and r, s a QR and QNR, respectively, mod p. Set $a = \frac{1}{2} \sum_{i=0}^{p-1} \left(\frac{i\left(i^2 - r\right)}{p}\right)$ and $b = \frac{1}{2} \sum_{i=0}^{p-1} \left(\frac{i\left(i^2 - s\right)}{p}\right)$. Prove that $a^2 + b^2 = p$.
7. Prove that $F_p \equiv \left(\frac{p}{5}\right) \pmod p$, where $p \geq 5$ is a prime.
8. (Easier than 2016 TSTST #3) Let $Q(x) = 420\left(x^2 - 1\right)^2$. Prove that for every $n > 2$, the numbers
$$Q(0), Q(1), Q(2), \ldots, Q(n-1)$$
produce at most $0.499n$ distinct residues when taken mod n.
9. (2000 Taiwan TST) Let m and n be relatively prime positive integers. Prove that $\varphi\left(5^m - 1\right) \neq 5^n - 1$.
10. Prove that there are no positive integers a, b, c such that $4abc - a - b$ is a square.
11. Prove that 16 is an 8th-power residue mod any integer.