Quadratic Residues

Number Theory Handout
12 Feb 2022

---

1 Quadratic Residues

For simplicity, let p and q always denote **primes** in this handout.

Let p be an odd prime. Let's consider a quadratic equation mod p:

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

To solve it, we can first complete the square.

$$\left(x + \frac{b}{2a}\right)^2 \equiv \frac{1}{a}\left(\frac{b}{2a}\right)^2 - \frac{c}{a} \pmod{p}$$

Therefore, it remains to study equations in the form

$$X^2 \equiv k \pmod{p}$$

Definition. A **quadratic residue mod** p is an integer $k \equiv x^2 \pmod{p}$ for some integer x.

Exercise. k is a QR mod p if and only if $x^2 - \bar{k}$ is irreducible in $\mathbb{F}_p$, i.e. $\bar{k}$ has a square root.

Exercise. How many quadratic residues are there mod p?

Definition. For ODD prime p, the Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \not\equiv 0 \pmod{p} \text{ is a QR} \\ -1 & \text{if } a \not\equiv 0 \pmod{p} \text{ is not a QR} \end{cases}$$

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

Proof. For $p \mid a$, obvious. Assume $a \in \mathbb{F}_p^\times$. Note that $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ as $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1$.
If $a \equiv x^2$ is a QR, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$.
There are $\frac{p-1}{2}$ QRs in $\mathbb{F}_p^\times$, and $\deg\left(X^{\frac{p-1}{2}} - 1\right) = \frac{p-1}{2}$, so we are done. □

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

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

Exercise. Prove Proposition 1 using primitive roots instead.

Proposition 1 is helpful, because it tells us that we don't have to list out all possible k^2 for $k = 1, \cdots, p-1$ to know which are QRs and which are not. However, **we can do better!**

Theorem 1. The following are true:

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ for odd primes p, q.

Before we prove this theorem, let's show how powerful the above theorem is.

Example. Is 69 a QR mod 101?

$$\begin{aligned}
\left(\frac{69}{101}\right) &= \left(\frac{23}{101}\right)\left(\frac{3}{101}\right) \\
&= \left(\frac{101}{23}\right)(-1)^{\frac{(101-1)(23-1)}{4}}\left(\frac{101}{3}\right)(-1)^{\frac{(101-1)(3-1)}{4}} \\
&= \left(\frac{101}{23}\right)\left(\frac{101}{3}\right) \\
&= \left(\frac{9}{23}\right)\left(\frac{2}{3}\right) \\
&= 1 \cdot (-1)^{\frac{3^2-1}{8}} = -1
\end{aligned}$$

and hence 69 is NOT a QR mod 101.

Let's prove Theorem 1. The first property was already proven, so we focus on the second and third. For any odd p and any integer a, denote the *least residue* $LR_p(a)$ to be the integer congruent to a mod p but lies between $-p/2$ and $p/2$.

Lemma. Let μ be the number of $x \in \left[1, \frac{p-1}{2}\right]$ such that $LR_p(ax) < 0$. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Proof.

$$\begin{aligned}
a \cdot 2a \cdot \cdots \cdot \left(\frac{p-1}{2}\right) a &\equiv LR_p(a) \cdot LR_p(2a) \cdot \cdots \cdot LR_p\left(\left(\frac{p-1}{2}\right) a\right) \pmod{p} \\
a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &\equiv (-1)^{\mu}\left(\frac{p-1}{2}\right)! \pmod{p} \\
a^{\frac{p-1}{2}} &\equiv (-1)^{\mu} \pmod{p}
\end{aligned}$$

and we are done since both sides are ± 1. $\square$

We are ready to first prove $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. The Lemma tells us we just have to count the parity of the number of $1 \leq x \leq \dfrac{p-1}{2}$ such that $LR_p(2x) < 0$, i.e.

$$\frac{p+1}{2} \leq 2x \leq p-1 \quad \Leftrightarrow \quad \left\lceil \frac{p+1}{4} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{2} \right\rfloor$$

which is just $\left\lfloor \frac{p-1}{2} \right\rfloor - \left\lceil \frac{p+1}{4} \right\rceil + 1$. It can be easily verified that

$$\left\lfloor \frac{p-1}{2} \right\rfloor - \left\lceil \frac{p+1}{4} \right\rceil + 1 \begin{cases} \text{is odd when } p \equiv 3,5 \pmod 8 \\ \text{is even when } p \equiv 1,7 \pmod 8 \end{cases}$$

and that $\dfrac{p^2-1}{8}$ also satisfies this property, so we are done. $\square$

We now prove the third statement. Let μ_p be the number of $1 \leq x \leq \dfrac{p-1}{2}$ such that $LR_p(qx) < 0$. For every such x, there is hence a unique y such that $-p/2 < qx - py < 0$. All such y must satisfy $qx/p < y < 1/2 + qx/p$ which is surely strictly between 0 and $q/2$. Therefore, μ_p is also the number of lattice points in

$$\left\{ (x,y) \in \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right] : -\frac{p-1}{2} \leq qx - py \leq -1 \right\}$$

Let μ_q be the number of $1 \leq y \leq \dfrac{q-1}{2}$ such that $LR_q(py) < 0$. Similarly μ_q is the number of lattice points in

$$\left\{ (x,y) \in \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right] : -\frac{q-1}{2} \leq py - qx \leq -1 \right\}$$

We want to find $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu_p + \mu_q}$ and hence we need to find the parity of $\mu_p + \mu_q$. Combining the two lattice point sets above, we see that $\mu_p + \mu_q$ is the number of lattice points in

$$\left\{ (x,y) \in \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{q-1}{2}\right] : -\frac{p-1}{2} \leq qx - py \leq \frac{q-1}{2} \right\}$$

This set is in fact symmetric about the centre $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$ of the rectangle (We leave this as an exercise). Therefore $\mu_p + \mu_q$ is usually even, with the only exception being when $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$ is itself in the set. Therefore

$$\mu_p + \mu_q \begin{cases} \text{is odd when } p \equiv q \equiv -1 \pmod 4 \\ \text{is even otherwise} \end{cases}$$

which is also obeyed by $\frac{(p-1)(q-1)}{4}$, so we are done. $\square$

2 Exercises

1. (Hong Kong 5th) Let p be a prime such that $p \equiv 1 \pmod 4$. Find $\sum_{k=1}^{p-1} \left\{ \frac{k^2}{p} \right\}$ where $\{x\} = x - \lfloor x \rfloor$.

2. (Korea 16th) $m \in \mathbb{N}$. If $2^{m+1} + 1 \mid 3^{2^m} + 1$, show that $2^{m+1} + 1$ is prime. Is the converse true?

3. (Austria 2007) Find all integers $0 \leq a < 2007$ so that $x^2 + a \equiv 0 \pmod{2007}$ has exactly two roots that are less than 2007.

4. (Singapore 2004) Find all $(a, b) \in \mathbb{N}^2$ such that $a, b \leq 2004$ and $x^2 + ax + b = 167y$ has integer solutions (x, y).

5. Find all primes p such that $y^2 \equiv x^3 - x \pmod p$ has exactly p solution pairs $(x, y) \in \mathbb{N}^2$ such that $0 \leq x, y \leq p$.

6. Find a way to determine whether a residue is a cubic residue mod p.