11 Quadratic Residues

Introduction: The concept of Quadratic Residues is a fundamental tool which has ramifications in lots of other number theory places: Cryptography, Factoring, etc...

11.1 Quadratice Residues & Nonresidues

---

1. **Introduction:** Suppose we asked the following, given a modulus m: Which numbers are perfect squares mod m?

   Ex. Let $m = 7$. What are the perfect squares? We could of course work backwards, squaring each value:

$$\begin{aligned} 0^2 &\equiv 0 \bmod 7 \\ 1^2 &\equiv 1 \bmod 7 \\ 2^2 &\equiv 4 \bmod 7 \\ 3^2 &\equiv 2 \bmod 7 \\ 4^2 &\equiv 2 \bmod 7 \\ 5^2 &\equiv 4 \bmod 7 \\ 6^2 &\equiv 1 \bmod 7 \end{aligned}$$

   Then the perfect squares are $0, 1, 2, 4$ and $3, 5, 6$ are not.

2. **Quadratice Residues & Nonresidues - Counting**

   (a) **Definition:** Let m be a modulus and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. We say a is a *quadratic residue mod m* if $\exists x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod m$. Otherwise, we say a is a *quadratic nonresidue mod m* if $\nexists x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod m$.

   Ex. If $m = 7$ then QR:$1, 2, 4$, QNR:$3, 5, 6$, and Neither:0.

   (b) **Theorem:** If p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a \implies \gcd(p, a) = 1$, then $x^2 \equiv a \bmod p$ has either no solutions or exactly two solutions mod p.

   Proof. If there are none, we are done. Suppose x is one solution to $x^2 \equiv a \bmod p$. Claim $-x$ is also a solution. Then $2x \equiv 0 \bmod p$. Since p is odd we can do $x \equiv 0 \bmod p$ which implies $p \mid x \implies p \mid x^2$. Then, $x^2 \equiv 0 \bmod p \implies a \equiv 0 \bmod p$ which contradicts $p \nmid a$.

   Let's show that for any two solutions, they are negative of one another. Suppose $x_1^2 \equiv a \bmod p$ and $x_2^2 \equiv a \bmod p$. Then $x_1^2 - x_2^2 \equiv 0 \bmod p$ so

$p \mid (x_1^2 - x_2^2)$ so $p \mid (x_1 - x_2)(x_1 + x_2)$ so $p \mid (x_1 - x_2)$ or $p \mid (x_1 + x_2)$. If $p \mid (x_1 - x_2)$ then $x_1 \equiv x_2 \bmod p$. If $p \mid (x_1 + x_2)$ then $x_1 \equiv -x_2 \bmod p$. Thus, there can only be the two which are negatives of one another ☐

(c) **Theorem:** Suppose p is an odd prime. Then $\exists \frac{p-1}{2}$ QR and $\exists \frac{p-1}{2}$ QNR.

Proof. If we square all of $1, 2, 3, \cdots, p-1$ the results will be in pairs (two of every result) the $\frac{p-1}{2}$ we do get are the QR. We miss $\frac{p-1}{2}$ results, those are the QNR. ☐

(d) **Theorem:** Let p be an odd prime and r a primitive root mod p. Suppose $p \nmid a$, then a is a QR mod p if and only if $\text{ind}_r a$ is even.

Proof.
$\rightarrow$ Suppose a is a quadratice residue mod p, $\exists x$ such that $x^2 \equiv a \bmod p$. Then take the index of both sides to get $\text{ind}_r x^2 \equiv \text{ind}_r a \bmod p-1$ and so $2\text{ind}_r x \equiv \text{ind}_r a \bmod p-1$. From here we see $\text{ind}_r a = 2\text{ind}_r x + k(p-1)$ for some $k \in \mathbb{Z}$ and so since $p-1$ is even we know $\text{ind}_r a$ is even.

$\leftarrow$ Suppose $\text{ind}_r a$ is even. Say $\text{ind}_r a = 2k$ for $k \in \mathbb{Z}$ so $r^{2k} \equiv a \bmod p$ so $(r^k)^2 \equiv a \bmod p$. Then, a is a quadratice residue mod p. ☐

To illustrate: $r = 3$ is a primitive root mod 17.

a mod 17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	$\underline{16}$	$\underline{14}$	1	$\underline{12}$	5	15	11	$\underline{10}$	$\underline{2}$	3	7	13	$\underline{4}$	9	$\underline{6}$	$\underline{8}$

So what this theorem tells us is that $a = 1, 2, 4, 8, 9, 13, 15, 16$ are the quadratic residues

3. **The Legendre Symbol and Properties**

(a) **Definition:** Given an odd prime p and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$, define the Legendre Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratice residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

Ex. If $p = 7$ we have:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Since $1, 2, 4$ are QR mod 7 and $3, 5, 6$ are QNR mod 7.

(b) **Euler's Criterion:** If p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$ then:

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

Proof. Suppose $\left(\frac{a}{p}\right) = 1$ then $\exists x$ such that $x^2 \equiv a \bmod p$. Then observe, $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} = x^{p-1} \equiv 1 \bmod p$ by Euler's Theorem/Fermat's Little Theorem they are equal.

Suppose $\left(\frac{a}{p}\right) = -1$. Consider the list $\{1, 2, \cdots, p-1\}$, each is coprime to p and there are an even number of them because p is odd. Suppose $b \in \{1, 2, \cdots, p-1\}$, then consider the equation $bx \equiv a \bmod p$. Since $\gcd(b,p) = 1 \mid a$, $\exists!$ solution. Could $x \equiv b \bmod p$? No because if $b \cdot b \equiv a \bmod p \implies b^2 \equiv a \bmod p$ but then a would be a QR mod p. Since the solution is not b it is another element in the set $\{1, 2, \cdots, p-1\}$. Thus all of $\{1, 2, \cdots, p-1\}$ pair up to give pairs whose products are a. Thus,

$$\underbrace{(1)(2)\cdots(p-1)}_{\text{Wilson's Theorem}} \equiv a^{(p-1)/2} \bmod p$$

$$a^{(p-1)/2} \equiv -1 \bmod p$$

□

Ex. $\left(\frac{6}{11}\right) = 6^{(11-1)/2} = 6^5 \equiv 10 \equiv -1 \bmod 11$. So 6 is a QNR mod 11. i.e. $x^2 \equiv 6 \bmod 11$ has no solution.

(c) **Theorem:** If p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = \gcd(b,p) = 1$ then:

i. If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. This statements that we can reduce the numerator mod the denominator.

Proof. Clear because $x^2 \equiv a \bmod p$ if and only if $x^2 \equiv b \bmod p$ because $a \equiv b \bmod p$. □

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

Proof. Well,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$$

So $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$ so $p \mid \left[\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right]$ but $p \geq 3$ Since $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ is between -2 and 2 and p divides it, we know that it must be 0. Therefore, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

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

Proof. Obvious. $\square$

(d) **Gauss' Lemma:** Suppose p is an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. Let s be the number of least nonnegative residues in the set $\{a, 2a, \cdots, ((p-1)/2)\, a\}$ which are $> p/2$. Then $\left(\frac{a}{p}\right) = (-1)^s$.

Ex. Consider $\left(\frac{8}{13}\right)$. Note that $\left(\frac{p-1}{2}\right) = \frac{12}{2} = 6$ so look at

$$\{8, 2 \cdot 8, 3 \cdot 8, \cdots, 6 \cdot 8\} \equiv \{8, 3, 11, 6, 1, 9\} \bmod 13$$

Since only three of these are greater than $p/2 = 6.5$ we have $\left(\frac{8}{13}\right) = (-1)^3 = -1$. Thus, 8 is a quadratic nonresidue mod 13.

4. **Two Special Cases**

These will turn out to be really useful after 11.2 and 11.3 .

(a) **Theorem:** Suppose p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

Proof. By Euler's Criterion we have,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p$$

If $p \equiv 1 \bmod 4$ then $p = 4k+1$ for some $k \in \mathbb{Z}$ so:

$$(-1)^{(p-1)/2} = (-1)^{(4k+1-1)/2} = (-1)^{2k} = 1$$

If $p \equiv 3 \bmod 4$ then $p = 4k+3$ for some $k \in \mathbb{Z}$ so:

$$(-1)^{(p-1)/2} = (-1)^{(4k+3-1)/2} = (-1)^{2k+1} = -1$$

$\square$

(b) **Theorem:** Suppose p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \bmod 8 \\ -1 & \text{if } p \equiv 3, 5 \bmod 8 \end{cases}$$

Proof. Not obvious as it uses Gauss' Lemma and is lengthy. $\square$

Note: This is equivalent to

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