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. □

(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:

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

□

(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. □

Note: This is equivalent to

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

11.2 Quadratic Reciprocity and Calculation Examples

1. **Introduction:** The Law of Quadratic reciprocity establishes that for odd primes p and q there is a connection between when p is a quadratic residue mod q when q is a quadratic residue mod p.

2. **Theorem:** If p, q are odd primes then

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

Proof. Omitted due to length. □

Use for Calculation: Under what circumstances will $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ be identical? We would need $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ to be even. This happens if and only if one of the two is even, say $\frac{p-1}{2}$ is even. That is, $\frac{p-1}{2} = 2k$ for some $k \in \mathbb{Z}$, so $p - 1 = 4k$ so $p \equiv 1 \bmod 4$. Thus, for calculation, we get:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if either } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \text{ (or both).} \\ -\left(\frac{q}{p}\right) & \text{if both } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4. \end{cases}$$

3. **Theorem:**

(a) If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Call this "reducing".

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Call this "splitting".

(c) $\left(\frac{a^2}{p}\right) = 1$. Call this the "square rule".

(d) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \\ -1 & \text{if } n \equiv 3 \bmod 4 \end{cases}$. Call this the "-1 rule".

(e) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \bmod 8 \\ -1 & \text{if } n \equiv 3, 5 \bmod 8 \end{cases}$. Call this the "2 rule".

4. **Examples:**
Ex. Calculate $\left(\frac{48}{29}\right)$:

$$\left(\frac{48}{29}\right) = \left(\frac{19}{29}\right) \text{ by reducing}$$

$$\left(\frac{19}{29}\right) = \left(\frac{29}{19}\right) \text{ by LoQR since } 19 \equiv 1 \bmod 4.$$

$$\left(\frac{29}{19}\right) = \left(\frac{10}{19}\right) \text{ by reducing.}$$

$$\left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right) \text{ by splitting.}$$

Then, we calculate these separately. First $\left(\frac{2}{19}\right) = -1$ by the "2 rule" because $19 \equiv 2 \bmod 8$. Then second,

$$\begin{aligned} \left(\frac{5}{19}\right) &= \left(\frac{19}{5}\right) \text{by LoQR since } 5 \equiv 1 \bmod 4. \\ \left(\frac{19}{5}\right) &= \left(\frac{4}{5}\right) \text{by reducing.} \\ \left(\frac{4}{5}\right) &= 1 \text{by square rule.} \end{aligned}$$

Thus $\left(\frac{48}{29}\right) = (-1)(1) = -1$.

Ex. Calculate $\left(\frac{105}{1009}\right)$. Note that 105 is not prime so we cannot use the LoQR immediately.

$$\left(\frac{105}{1009}\right) = \left(\frac{3}{1009}\right)\left(\frac{5}{1009}\right)\left(\frac{7}{1009}\right) \text{by splitting.}$$

Then we calculate these separately. First,

$$\begin{aligned} \left(\frac{3}{1009}\right) &= \left(\frac{1009}{3}\right) \text{by LoQR since } 1009 \equiv 1 \bmod 4. \\ \left(\frac{1009}{3}\right) &= \left(\frac{1}{3}\right) \text{by reducing} \\ \left(\frac{1}{3}\right) &= 1 \end{aligned}$$

Second,

$$\begin{aligned} \left(\frac{5}{1009}\right) &= \left(\frac{1009}{5}\right) \text{by LoQR since } 1009 \equiv 1 \bmod 4. \\ \left(\frac{1009}{5}\right) &= \left(\frac{4}{5}\right) \text{by reducing} \\ \left(\frac{4}{5}\right) &= 1 \text{ by the square rule} \end{aligned}$$

Third,

$$\begin{aligned} \left(\frac{7}{1009}\right) &= \left(\frac{1009}{7}\right) \text{by LoQR since } 1009 \equiv 1 \bmod 4. \\ \left(\frac{1009}{7}\right) &= \left(\frac{1}{7}\right) \text{by reducing} \\ \left(\frac{1}{7}\right) &= 1 \end{aligned}$$

Thus, $\left(\frac{105}{1009}\right) = (1)(1)(1) = 1$.

11.3 The Jacobi Symbol

1. **Introduction:** The Jacobi symbol is a generalization of the Legendre symbol for when the denominator is odd but not necessarily prime. It preserves many of the same useful properties and almost the same meaning.

2. **Definition:** Let n be an odd positive integer with prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and let $\alpha \in \mathbb{Z}$ be coprime to n. Define:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

   Thus the Jacobi symbol is defined in terms of the Legendre symbol.

3. **Theorem:** Assume $\gcd(a, n) = \gcd(b, n) = 1$.

   (a) If $a \equiv b \bmod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

   (b) $\left(\frac{a^2}{n}\right) = 1$

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

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

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

   (f) $\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{m}{n}\right) & \text{if either } m \equiv 1 \bmod 4,\ n \equiv 1 \bmod 4 \\ -\left(\frac{n}{m}\right) & \text{if both } m \equiv 3 \bmod 4 \text{ and } n \equiv 3 \bmod 4 \end{cases}$

   Proof. Lots of calculation. □

4. **Question:** We know $\left(\frac{a}{p}\right)$ tells us if a is a QR or QNR mod p. Does $\left(\frac{a}{n}\right)$ tell us if a is a QR or QNR mod n? Well, half-yes.

   Theorem: Suppose $\gcd(a, n) = 1$ and n is an odd prime.

   (a) If a is a QR mod n then $\left(\frac{a}{n}\right) = 1$.

   (b) If $\left(\frac{a}{n}\right) = 1$ then we cannot conclude a is a QR mod n.

   Proof. Suppose a is a QR mod n, then $\exists x$ such that $x^2 \equiv a \bmod n$ has solutions then $n \mid (x^2 - a)$ and so for every p in the prime factorization of n we have $p \mid (x^2 - a)$ and so $x^2 \equiv a \bmod p$ which then tells us that $\left(\frac{a}{p}\right) = 1$. It follows that $\left(\frac{a}{n}\right) = 1$ because $\left(\frac{a}{n}\right)$ is simply a product of

1s. The reverse cannot be guaranteed, for example $x^2 \equiv 2 \bmod 15$ has no solution (can be verified by trial and error). However $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{2}{5}\right) = -1$ and so $\left(\frac{2}{15}\right) = (-1)(-1) = 1$. □

5. **Calculations:** We can then calculate Jacobi symbols essentially as we did with Legendre symbols. The biggest thing to watch out for is making sure that we obey the rules at each step of the calculation.

   Ex. Let's calculate $\left(\frac{1009}{2307}\right)$. We have:

$$\begin{aligned}
\left(\frac{1009}{2307}\right) &= \left(\frac{2307}{1009}\right) && \text{by LoQR since } 1009 \equiv 1 \bmod 4.\\
&= \left(\frac{289}{1009}\right) && \text{by reducing.}\\
&= \left(\frac{1009}{289}\right) && \text{by LoQR since } 1009 \equiv 1 \bmod 4.\\
&= \left(\frac{142}{289}\right) && \text{by reducing.}\\
&= \left(\frac{2}{289}\right)\left(\frac{71}{289}\right) && \text{by splitting.}
\end{aligned}$$

   Then we calculate the first, $\left(\frac{2}{289}\right) = 1$ by the 2 rule, since $289 \equiv 1 \bmod 8$. For the second part,

$$\begin{aligned}
\left(\frac{71}{289}\right) &= \left(\frac{289}{71}\right) && \text{by LoQR since } 289 \equiv 1 \bmod 4.\\
&= \left(\frac{5}{71}\right) && \text{by reducing.}\\
&= \left(\frac{71}{5}\right) && \text{by LoQR since } 5 \equiv 1 \bmod 4.\\
&= \left(\frac{1}{5}\right) && \text{by reducing.}
\end{aligned}$$

   Thus, $\left(\frac{1009}{2307}\right) = 1$. We cannot conclude if 1009 is a QR or a QNR mod 2307.

Ex. Let's calculate $\left(\frac{1999}{2315}\right)$. We have:

$$\begin{aligned}
\left(\frac{1999}{2315}\right) &= -\left(\frac{2315}{1999}\right) \text{ by LoQR since } 1999 \equiv 3 \bmod 4 \text{ and } 2315 \equiv 1 \bmod 4. \\
&= -\left(\frac{316}{1999}\right) \text{ by reducing.} \\
&= -\left(\frac{2^2}{1999}\right)\left(\frac{79}{1999}\right) \text{ by splitting.} \\
&= -(1)\left(\frac{79}{1999}\right) \\
&= -\left(-\left(\frac{1999}{79}\right)\right) \text{ by LoQR since } 1999, 79 \equiv 3 \bmod 4. \\
&= \left(\frac{24}{79}\right) \text{ by reducing.} \\
&= \left(\frac{2}{79}\right)^3\left(\frac{3}{79}\right)
\end{aligned}$$

Then, $\left(\frac{2}{79}\right) = 1$ since $79 = 7 \bmod 8$. Then, $\left(\frac{3}{79}\right) = -\left(\frac{79}{3}\right)$ since $79, 3 \equiv 3 \bmod 4$. Which then becomes $-\left(\frac{1}{3}\right) = -1$ from reducing. Therefore, $\left(\frac{1999}{2315}\right) = -1$ and 1999 is a QNR mod 2315.

11.4 Problems

1. Determine, by squaring, which of $1, ..., 16$ are quadratic residues of $p = 17$.
2. Calculate $\left(\frac{3}{17}\right)$ by
   (a) Euler's Criterion
   (b) Gauss's Lemma
3. Prove that if p and $q = 2p + 1$ are both odd primes then -4 is a primitive root of q.
4. Prove that if $p \equiv 1 \mod 4$ is a prime then -4 and $(p-1)/4$ are both quadratic residues of p.
5. Calculate each of the following:
   (a) $\left(\frac{21}{59}\right)$
   (b) $\left(\frac{1463}{89}\right)$
   (c) $\left(\frac{1547}{1913}\right)$

6. Using the Law of Quadratic Reciprocity, show that if p is an odd prime that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 12 \\ -1 & \text{if } p \equiv \pm 5 \mod 12 \end{cases}$$

7. Classify all primes p with $\left(\frac{5}{p}\right) = 1$

8. Calculate each of the following using properties of the Jacobi Symbol, not by raw calculation.

   (a) $\left(\frac{5}{21}\right)$

   (b) $\left(\frac{1009}{2307}\right)$

   (c) $\left(\frac{27}{101}\right)$

9. Categorize all positive integers n which are relatively prime to 15 and for which $\left(\frac{15}{n}\right) = 1$.

10. Show that if $a > 0$ is not a perfect square then there exists a positive integer n such that $\left(\frac{a}{n}\right) = -1$.