Math 406 Section 11.1: Quadratic Residues and Nonresidues

1. **Introduction:** There's a reasonable reason to jump from Chapter 9 to Chaper 11 which is that both sections concern themselves with solutions to equations. Chapter 11 is much more specific and essentially attempts to address the question:

   Which integers are perfect squares mod m?

   For example if $p = 7$ which integers are perfect squares? We could of course work backwards, squaring everything:

   $$\{0, 1, 2, 3, 4, 5, 6\}^2 \equiv \{0, 1, 4, 2, 2, 4, 1\} \bmod 7$$

   Then we'd know that $\{0, 1, 2, 4\}$ are all perfect squares. But how could we approach this in general?

2. **Quadratic Residues and Nonresidues**

   The following definitions do not correspond exactly with the concept of being a perfect square but they're the simplest approach that allows us to develop some formulas.

   Definition:

   Suppose $\gcd(a, m) = 1$. We say that $a \in \mathbb{Z}$ is a *quadratic residue (QR) mod* m if $x^2 \equiv a \bmod m$ has a solution, meaning a is a perfect square.

   Definition

   Otherwise we say a is a *quadratic nonresidue (QNR) mod* m. Sometimes I'll abbreviate QR and QNR.

   Note:

   If $\gcd(a, m) \neq 1$ then a is neither a QR nor a QNR. The definitions simply don't apply.

   Example:

   The quadratic residues mod 7 are $\{1, 2, 4\}$ while the quadratic nonresidues are $\{3, 5, 6\}$. According to our definition 0 is neither because it's not coprime to 7.

   Example:

   Mod $m = 10$ we have:

   $$\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2\} \equiv \{0, 1, 4, 9, 6, 5, 6, 9, 4, 1\} \bmod 10$$

   The quadratic residues mod 10 are $\{1, 9\}$ while the quadratic nonresidues are $\{3, 7\}$. According to our definition $\{0, 2, 4, 5, 6, 8\}$ are neither because they're not coprime to 10.

3. **Primes v Composites**

   The previous example is slightly annoying because we'd think of 4 as a perfect square mod 10, which it is, but it's not a quadratic residue.

   However when the modulus is a prime p then because all of $\{1, ..., p - 1\}$ are coprime to p the concept of being a quadratic residue and being a perfect square correspond, except for $a \equiv 0 \bmod p$ which is neither.

4. **Quadratic Residues and Nonresidues for Primes - Some Theorems**

(a) **Theorem:**

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

Proof:

If there are no solutions we are done. If x is one solution then $x^2 \equiv a \bmod p$ and then note that $(-x)^2 \equiv a \bmod p$ and so $-x$ is another solution. It is different because $x \equiv -x \bmod p$ would imply that $p \mid 2x$ but since $p \nmid 2$ this means that $p \mid x$ and so $p \mid x^2$ and so $x^2 \equiv 0 \bmod p$ and so $a \equiv 0 \bmod p$ which contradicts $p \nmid a$.

But what if there are more than two? Suppose x_1 and x_2 are any two solutions, then $x_1^2 \equiv a \equiv x_2^2 \bmod p$ and so $p \mid (x_1^2 - x_2^2) = (x_1 - x_2)(x_1 + x_2)$ which tells us that either $p \mid (x_1 - x_2)$ or $p \mid (x_1 + x_2)$. The first gives us $x_1 \equiv x_2 \bmod p$ and the second gives us $x_1 \equiv -x_2 \bmod p$. Thus there can only be the two which are the negatives of one another. $\mathcal{QED}$

(b) **Theorem:**

If p is an odd prime then there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues mod p.

Proof:

If we square all of $\{1, 2, ..., p-1\}$ mod p we will get values in $\{1, 2, ..., p-1\}$ (only 0^2 yields 0 mod p). We know that each result will occur twice and so there will $(p-1)/2$ quadratic residues. The remaining will be the quadratic nonresidues. $\mathcal{QED}$

(c) **Theorem:**

Let p be an odd prime and r be a primitive root of p (primes always have primitive roots). Then any a with $p \nmid a$ is a quadratic residue of p iff $\text{ind}_r a$ is even.

Proof:

$\Longleftarrow$: If $\text{ind}_r a$ is even then observe that $\left(r^{\frac{1}{2}\text{ind}_r a}\right)^2 \equiv a \bmod p$ and so a is a quadratic residue mod p.

$\Longrightarrow$: Suppose a is a quadratic residue mod p so there exists some x with $x^2 \equiv a \bmod p$. Then we 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. $\mathcal{QED}$

Example:

Here is a table of indices for $r = 6$, a primitive root of $p = 11$:

x	1	2	3	4	5	6	7	8	9	10
$\text{ind}_6 x$	0	9	2	8	6	1	3	7	4	5

The theorem tells us that mod 11 the quadratic residues are $\{1, 3, 4, 5, 9\}$ (even indices) while the quadratic nonresidues are $\{2, 6, 7, 8, 10\}$ (odd indices).

5. **The Legendre Symbol and Properties**

(a) **Notation:**

If p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. We define the *Legendre symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{iff } a \text{ is a quadratic residue mod } p \text{ iff } x^2 \equiv a \bmod p \text{ has (two) solutions} \\ -1 & \text{iff } a \text{ is a quadratic nonresidue mod } p \text{ iff } x^2 \equiv a \bmod p \text{ has no solutions} \end{cases}$$

Note:

We'll use the terms *numerator* and *denominator* even though these aren't fractions.

Example:

We have:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \quad \text{and} \quad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

(b) **Theorem (Euler's Criterion):**

If p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$ then:

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

Proof:

Suppose $\left(\frac{a}{p}\right) = 1$ and so let x satisfy $x^2 \equiv a \bmod p$. Then we also have:

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

The last equality is by Fermat's Little Theorem. Thus they are equal.

On the other hand suppose $\left(\frac{a}{p}\right) = -1$. First note that for each $x \in \{1, 2, ..., p-1\}$ there is some unique $y \in \{1, 2, ..., p-1\}$ with $xy \equiv a \bmod p$ (because it is a linear congruence with variable y and $\gcd(x, p) = 1 \mid a$). Moreover $y \not\equiv x \bmod p$ otherwise we would have $x^2 \equiv a \bmod p$, contradicting $\left(\frac{a}{p}\right) = -1$.

Therefore the values $1, 2, ..., p-1$ group into $(p-1)/2$ pairs each of which have a product of a taken mod p. That is:

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

But Wilson's Theorem states that:

$$(p-1)! \equiv -1 \bmod p$$

The result follows. $\mathcal{QED}$

Example:

We have:

$$\left(\frac{6}{11}\right) \equiv 6^{(11-1)/2} \equiv 6^5 \equiv 10 \equiv -1 \bmod 11$$

and so 6 is a quadratic residue mod 11.

(c) **Theorem (Properties):**

If p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$, then:

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

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

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

Proof:

i. Clear because $x^2 \equiv a \bmod p$ iff $x^2 \equiv b \bmod p$ because $a \equiv b \bmod p$.

ii. We have:

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

Now then since $p \geq 3$ and $p \mid \left[\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right]$ but that difference can only be -2, 0 or 2 (because the two terms can only be ± 1) we must have that difference being 0.

iii. Follows immediately from ii.

(d) **Gauss' Lemma:**

Suppose p is an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. If s is the number of least positive residues of $\{a, 2a, 3a, ..., ((p-1)/2)a\}$ mod p which are greater than $p/2$ then $\left(\frac{a}{p}\right) = (-1)^s$.

Proof:

Omit. This proof is fairly lengthy. $\mathcal{QED}$

Note:

This is a fairly bizarre theorem devoid of much intuition but it's good to do an example.

Example:

Consider $p = 13$ with $a = 8$. We have $(p-1)/2 = 6$ and so we examine:

$$\{a, 2a, 3a, 4a, 5a, 6a\} = \{8, 16, 24, 32, 40, 48\} \equiv \{8, 3, 11, 6, 1, 9\} \bmod 13$$

Since 3 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.

6. **Special Cases: -1 and 2**

(a) **Theorem (When is -1 a QR mod p?):**
If 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 $k \in \mathbb{Z}$ and 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 $k \in \mathbb{Z}$ and so:

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

$\mathcal{QED}$

(b) **Theorem (When is 2 a QR mod p?):**
If 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:
Omitted as it's fairly lengthy.
Note:
This is equivalent to:

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