1 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...

1.1 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 $x_1 \equiv x_2 \mod p$. If $p \mid (x_1 + x_2)$ then $x_1 \equiv -x_2 \mod p$. 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 $x^2 \equiv a \mod p$. Then take the index of both sides to get $\text{ind}_r x^2 \equiv \text{ind}_r a \mod p-1$ and so $2\text{ind}_r x \equiv \text{ind}_r a \mod p-1$. 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 $r^{2k} \equiv a \mod p$ so $(r^k)^2 \equiv a \mod p$. 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