Introduction to quadratic residues

Learning Objectives. By the end of class, students will be able to:

- Define a quadratic residue modulo m
- Prove that the quadratic congruence $x^2 \equiv a \pmod{p}$ has zero or one solution modulo a prime when $p \nmid a$
- Use the solution to a quadratic congruence modulo a prime to find the other solution .

Reading: Strayer Section 4.1

Turn in: Exercise 3 Find all incongruent solutions of the quadratic congruence $x^2 \equiv 1 \pmod{8}$. Is it not true that quadratic congruences have either no solutions or exactly two incongruent solutions? Explain.

Solution: As we have seen on many previous questions, $x^2 \equiv 1 \pmod{8}$ for all odd numbers. So there are 4 incongruent solutions modulo 8, which is not a contradiction because 8 is not an odd prime number.

Finish proof of the existence of primitive roots modulo a prime (10 minutes)

Quadratic residues (40 minutes)

Definition 1 (quadratic residue)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The a is said to be a *quadratic residue modulo* m if the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable in $\mathbb{Z}$. Otherwise, a is said to be a *quadratic nonresidue modulo* m.

Remark 1. When finding squares modulo m, we only need to check up to $\dfrac{m}{2}$, since $(-a)^2 = a^2$ and $m - a \equiv -a \pmod{m}$

In-class Problem 1 Find all incongruent quadratic residues and nonresidues modulo $2, 3, 4, 5, 6, 7, 8$, and 9.

Solution: I also included solutions modulo $10, 11, 12$

Modulus	least nonnegative reduced residues	quadratic residues	quadratic non-residues
2	1	1	N/A
3	$1, 2$	1	2
4	$1, 3$	1	3
5	$1, 2, 3, 4$	$1, 4$	$2, 3$
6	$1, 5$	1	5
7	$1, 2, 3, 4, 5$	$1, 2, 4$	$3, 5, 6$
8	$1, 3, 5, 7$	1	$3, 5, 7$
9	$1, 2, 4, 5, 7, 8$	$1, 4, 7$	$2, 4, 8$
10	$1, 3, 7, 9$	$1, 9$	$3, 7$
11	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	$1, 3, 4, 5, 9$	$2, 6, 7, 8, 10$
12	$1, 5, 7, 11$	1	$5, 7, 11$

Learning outcomes:
Author(s): Claire Merriman

Lemma 1 (Generalized Porism 4.2)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable, say with $x = x_0$, then $m - x_0$ is also a solution. If $m > 2$, then $x_0 \not\equiv m - x_0 \pmod{m}$, and solutions occur in pairs.

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable, say with $x = x_0$. Then

$$(m - x_0)^2 \equiv (-x_0)^2 \equiv x_0^2 \equiv a \pmod{m}.$$

If $x_0 \equiv m - x_0 \pmod{m}$, then $2x_0 \equiv m \equiv 0 \pmod{m}$ and $m \mid 2x_0$ by definition. Since $(a, m) = 1$, it must be that $(x_0, m) = 1$ since $(x_0, m) \mid (a, m)$. Thus, $m \mid 2$, so $m = 2$. Therefore, when $m > 2$, then $x_0 \not\equiv m - x_0 \pmod{m}$, and solutions occur in pairs. ■

Remark 2. Since $x_0 \equiv m - x_0 \pmod{m}$ implies $x_0 \equiv \frac{m}{2}$, we can say that if $x^2 \equiv a \pmod{m}$ is solvable and $\frac{m}{2}$ is *not* a solution, then solutions occur in pairs.

Proposition 1 (Proposition 4.1)**.** Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \mid a$. Then the quadratic congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p.

Proof Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \mid a$. Consider the quadratic congruence $x^2 \equiv a \pmod{p}$. If no solutions exist, we are done.

If solutions to the quadratic congruence exist, then **??** says that there are at least two solutions, since $p > 2$. **??** says that there are at most two solutions to $x^2 - a \equiv 0 \pmod{p}$ and therefore $x^2 \equiv a \pmod{p}$. Thus, there are exactly two incongruent solutions modulo p. ■

Proposition 2 (Proposition 4.3)**.** Let p be an odd prime number. Then there are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues modulo p.

Proof Consider the $p - 1$ quadratic congruences

$$\begin{aligned}
x^2 &\equiv 1 \pmod{p} \\
x^2 &\equiv 2 \pmod{p} \\
&\vdots \\
x^2 &\equiv p - 1 \pmod{p}.
\end{aligned}$$

Since each congruence has either zero or two incongruent solutions modulo p by **??**, and no integer is a solution to more than one of the congruences, exactly half are solvable. Therefore, there are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues modulo p. ■