Monday, March 18: Proof of Primitive Root Theorem

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

- Find the number of roots of unity modulo m
- Prove primitive roots exist modulo a prime .

Reading None

Roots of unity (35 minutes)

Finish proof of Proposition 5.8

In-class Problem 1 *Let p be prime, m a positive integer, and $d = (m, p-1)$. Prove that $a^m \equiv 1 \pmod{p}$ if and only if $a^d \equiv 1 \pmod{p}$.*

Solution: *Let p be prime, m a positive integer, and $d = (m, p-1)$. Let $a \in \mathbb{Z}$. If $p \mid a$, then $a^i \boxed{\equiv 0 \pmod{p}}$ for all positive integers i. Thus, we are only considering $a \in \mathbb{Z}$ such that $p \nmid a$. Otherwise, $a^{p-1} \equiv 1 \pmod{p}$ by* $\boxed{\text{Fermat's Little Theorem}}$.

By Proposition 5.1, $a^m \equiv 1 \pmod{p}$ if and only if $\boxed{\operatorname{ord}_p a \mid m}$. Similarly, $\boxed{a^{p-1} \equiv 1 \pmod{p}}$ if and only if $\boxed{\operatorname{ord}_p a \mid p-1}$. Thus, $\boxed{\operatorname{ord}_p a}$ is a common divisor of $\boxed{m}$ and $\boxed{p-1}$. Combining and gives $\operatorname{ord}_p a$ is a common divisor of $\boxed{m}$ and $\boxed{p-1}$ if and only if $\operatorname{ord}_p a \mid d$. One final application of Proposition 5.1 gives $\boxed{\operatorname{ord}_p a \mid d}$ if and only if $\boxed{a^d \equiv 1 \pmod{p}}$.

In-class Problem 2 *Let p be prime and m a positive integer. Prove that*

$$x^m \equiv 1 \pmod{p}$$

has exactly $(m, p-1)$ incongruent solutions modulo p.

Proof *Let p be prime, m a positive integer, and $d = (m, p-1)$. By In-class Problem 1, $x^m \equiv 1 \pmod{p}$ if and only if $x^d \equiv 1 \pmod{p}$. By Proposition 5.8 there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, there are exactly d solutions to $x^m \equiv 1 \pmod{p}$.* ■

Primitive roots modulo a prime (15 minutes)

We will now prove the existence of primivitive roots modulo a prime combining the two methods from the reading: we will show that when $d \mid p-1$, there are $\phi(d)$ incongruent integers of order d modulo p, like Strayer. However, we will prove this using the method from Lemma 10.3.4 instead of results from Chapter 3.

Theorem (Theorem 5.9)**.** *Let p be a prime and let $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p-1$. Then there are exactly $\phi(d)$ incongruent integers of order d modulo p.*

Proof Let p be a prime and let $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p-1$. First we will prove the theorem for $d = q^s$ modulo p where q is prime and s is a nonnegative integer.

By Proposition 5.8, there are exactly q^s incongruent solutions to

$$x^{q^s} \equiv 1 \pmod{p} \tag{1}$$

and exactly q^{s-1} incongruent solutions to

$$x^{q^{s-1}} \equiv 1 \pmod{p}. \tag{2}$$

Since $(x^{q^{s-1}})^q = x^{q^s}$, all solutions to (2) are solutions to (1). Thus, there are exactly $q^s - q^{s-1} = q^{s-1}(q-1)$ integers a where $a^{q^s} \equiv 1 \pmod{p}$ and $a^{q^{s-1}} \not\equiv 1 \pmod{p}$. Thus, by Proposition 5.1, $\operatorname{ord}_p a \mid q^s$ and $\operatorname{ord}_p a \nmid q^{s-1}$. Since q is prime, $\operatorname{ord}_p a = q^s$. By Theorem 3.3, $\phi(q^s) = q^s - q^{s-1} = q^{s-1}(q-1)$, so we have shown there are $\phi(q^s)$ incongruent integers with order q^s modulo p.

Now we will prove the general case. Let

$$d = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$$

for distinct primes $q_1, q_2, \ldots, q_k$ and positive integers $s_1, s_2, \ldots, s_k$. Let $a_1, a_2, \ldots, a_k$ be elements of order $q_1^{s_1}, q_2^{s_2}, \ldots, q_k^{s_k}$ respectively. Consider $a = a_1 a_2 \cdots a_k$ and $a^2, a^3, \ldots, a^d$. By Homework 6, Problem 6, a has order $q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k} = d$. By Proposition 5.8, there are exactly d solutions to $x^d \equiv 1 \pmod{p}$.

Annotation. This is where we ended class on Monday.

Thus, $a, a^2, \ldots, a^d$ are all incongruent solutions to $x^d \equiv 1 \pmod{p}$ by Proposition 5.1. By Proposition 5.4, $\operatorname{ord}_p a^i = \dfrac{d}{(d,i)} = d$ if and only if $(d,i) = 1$. Since there are $\phi(d)$ such integers i, there are in fact $\phi(d)$ incongruent integers with order d modulo p. ■

Corollary (Corollary 5.10)**.** *Let p be prime. There are exactly $\phi(p-1)$ primitive roots modulo p.*

Wednesday, March 20: 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 $\frac{m}{2}$, since $(-a)^2 = a^2$ and $m - a \equiv -a \pmod m$*

In-class Problem 3 *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 nonresidues*
2	1	1	*N/A*
3	$\boxed{1, 2}$	$\boxed{1}$	$\boxed{2}$
4	$\boxed{1, 3}$	$\boxed{1}$	$\boxed{3}$
5	$\boxed{1, 2, 3, 4}$	$\boxed{1, 4}$	$\boxed{2, 3}$
6	$\boxed{1, 5}$	$\boxed{1}$	$\boxed{5}$
7	$\boxed{1, 2, 3, 4, 5}$	$\boxed{1, 2, 4}$	$\boxed{3, 5, 6}$
8	$\boxed{1, 3, 5, 7}$	$\boxed{1}$	$\boxed{3, 5, 7}$
9	$\boxed{1, 2, 4, 5, 7, 8}$	$\boxed{1, 4, 7}$	$\boxed{2, 4, 8}$
10	$\boxed{1, 3, 7, 9}$	$\boxed{1, 9}$	$\boxed{3, 7}$
11	$\boxed{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}$	$\boxed{1, 3, 4, 5, 9}$	$\boxed{2, 6, 7, 8, 10}$
12	$\boxed{1, 5, 7, 11}$	$\boxed{1}$	$\boxed{5, 7, 11}$

Lemma (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 (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 Generalized Porism 4.2 says that there are at least two solutions, since $p > 2$. Theorem 5.7 (Lagrange) 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 (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 Proposition 4.1, 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. ■

Friday, March 22: Legendre symbol

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

- Define the Legendre symbol
- Prove basic facts about the Legendre symbol
- Use the definition and basic facts to find the Legendre symbol for specific examples.

Reading: Strayer Section 4.2 through Example 4

Turn in: Exercise 12 Use Euler's Criterion to evaluate the following Legendre symbols

(a) $\left(\frac{11}{23}\right)$

Solution: $\left(\dfrac{11}{23}\right) \equiv 11^{(23-1)/2} \equiv 11^{11} \pmod{23}$ By Euler's Criterion. Then

$$11^{11} \equiv (11^2)^5(11) \equiv 6^5(11) \equiv (6^2)(6^3)(11) \equiv (13)(9)(11) \equiv (-90)(11) \equiv -1 \pmod{23}$$

(b) $\left(\dfrac{-6}{11}\right)$

Solution: $\left(\dfrac{-6}{11}\right) \equiv (-6)^{(11-1)/2} \equiv (-6)^5 \pmod{11}$ By Euler's Criterion. Then

$$(-6)^5 \equiv ((6)^2)^2(-6) \equiv 3^2(-6) \equiv -54 \equiv 1 \pmod{11}$$