Existence of primitive roots modulo a prime

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.

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 Reading Lemma 10.3.4 instead of results from Chapter 3.

Theorem 1. *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 **??**, 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 **??**, $\operatorname{ord}_p a \mid q^s$ and $\operatorname{ord}_p a \nmid q^{s-1}$. Since q is prime, $\operatorname{ord}_p a = q^s$. By **??**, $\phi(q^s) = q^s - q^{s-1} = q^{s-1}(q-1)$, 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 **??**, there are exactly d solutions to $x^d \equiv 1 \pmod p$. Thus, $a, a^2, \ldots, a^d$ are all incongruent solutions to $x^d \equiv 1 \pmod p$ by **??**. By **??**, $\operatorname{ord}_p a^i = \dfrac{d}{(d,i)} = d$ 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 1. *Let p be prime. There are exactly $\phi(p-1)$ primitive roots modulo p.*

Learning outcomes:

Author(s): Claire Merriman