Lagrange's Theorem

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

- Prove Lagrange's Theorem .

Instructor Notes: **Reading** Strayer Section 5.2

Turn in: (a) Exercise 10a: Determine the number of incongruent primitive roots modulo 41

Solution: Since 41 is prime, **??** says there are $\phi(41) = 40$ primitive roots modulo 41.

(b) Exercise 11a: Find all incongruent integers having order 6 modulo 31.

Solution: From Appendix E, Table 3, 3 is a primitive root modulo 31. By **??**, the elements of order 6 modulo 31 are those where

$$6 = \mathrm{ord}_{31}(3^i) = \frac{\phi(31)}{(\phi(31), i)} = \frac{30}{5}.$$

The positive integers less than 31 where $(30, i) = 5$ are $i = 5, 25$. So the elements of order 6 are $3^5, 3^{25}$.

The problem does not ask for the least nonnegative residues. However, we can also find those:

$$3^5 \equiv (-4)(9) \equiv -5 \equiv 26 \pmod{31}$$

$$3^{25} \equiv (-5)^5 \equiv (-6)^2(-5) \equiv -25 \equiv 6 \pmod{31}$$

The goal is to finish proving the **??** with a look at polynomials.

Theorem 1 (Lagrange)**.** *Let p be a prime number and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

for integers $a_0, a_1, \ldots, a_n$. Let d be the greatest integer such that $a_d \not\equiv 0 \pmod{p}t$ then d is the degree of $f(x)$ modulo p*. Then the congruence*

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions. We call these solutions roots of $f(x)$ modulo p.

Proof from class *We proceed by induction on the degree d.*

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$**.** *Then $f(x) \equiv a_1 x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by **??**, there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.*

Learning outcomes:
Author(s): Claire Merriman

Induction Hypothesis: *Assume that for all $k < d$, if $f(x)$ has degree k modulo p, then*

$$f(x) \equiv a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

We will proceed by contradiction. That is, assume that there exists $f(x)$ with degree d modulo p and at least $d+1$ roots modulo p. Call these roots $r_1, r_2, \ldots, r_d, r_{d+1}$. Consider the polynomial

$$g(x) = a_d(x - r_1)(x - r_2) \cdots (x - r_d).$$

Then $f(x)$ and $g(x)$ have the same leading term modulo p. The polynomial $h(x) = f(x) - g(x)$ is either the 0 polynomial or it has degree less than d modulo p.

If $h(x)$ is the 0 polynomial, then

$$h(r_1) \equiv h(r_2) \equiv \cdots \equiv h(r_{d+1}) \equiv 0 \pmod{p}$$

and

$$f(r_1) \equiv f(r_2) \equiv \cdots \equiv f(r_{d+1}) \equiv 0 \pmod{p}$$

implies

$$g(r_1) \equiv g(r_2) \equiv \cdots \equiv g(r_{d+1}) \equiv 0 \pmod{p}.$$

That is,

$$a_d(r_{d+1} - r_1)(r_{d+1} - r_2) \cdots (r_{d+1} - r_d) \equiv 0 \pmod{p}.$$

Since p is prime, repeated applications of Homework 4, Problem 9a gives that one of $a_d, r_{d+1} - r_1, r_{d+1} - r_2, \ldots, r_{d+1} - r_d$ is 0 modulo p. Now, $a_d \not\equiv 0 \pmod{p}$ by assumption, and the r_i are distinct modulo p, so we have a contradiction. Thus, $h(x)$ is not the 0 polynomial.

Since $r_1, r_2, \ldots, r_d$ are roots of both $f(x)$ and $g(x)$, they are also roots of $h(x)$. This contradicts the induction hypothesis, since $h(x)$ has degree less than d by construction.

Thus, $f(x)$ has at most d incongruent solution modulo p. ■

Modified proof from Strayer *We proceed by induction on the degree d.*

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$. *Then $f(x) \equiv a_1 x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by **??**, there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.*

Induction Hypothesis: *Assume that for all $k < d$, if $f(x)$ has degree k modulo p, then*

$$f(x) \equiv a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

If the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions we are done. Otherwise, assume that there exists at least one solution, say a. Dividing $f(x)$ by $(x - a)$ gives

$$f(x) \equiv (x - a)q(x) \pmod{p}$$

where $q(x)$ is a polynomial of degree $d - 1$ modulo p. Since $q(x)$ has at most $d - 1$ roots modulo p by the induction hypothesis, there are at most $d - 1$ incongruent additional roots of $f(x)$ modulo p. Thus, there are a total of at most d incongruent roots modulo p. ■

Proposition 1. *Let p be prime and m a positive integer where $m \mid p-1$. Then*

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

has m incongruent solutions modulo p.

Proof *Let p be prime and m a positive integer where $m \mid p-1$. Then there exists $k \in \mathbb{Z}$ such that $mk = p-1$. Then*

$$x^{p-1} - 1 = (x^m - 1)(x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1)$$

*By **??**, there are $p-1$ incongruent solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$, namely $1, 2, \ldots, p-1$. We will show that m of these are solutions to $x^m - 1 \equiv 0 \pmod{p}$ and the rest are solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$.*

By Lagrange, there are at most $(k-1)m$ solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$. Thus, there are at least $p - 1 - (k-1)m = m$ incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$. Since there are also at least m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ by Lagrange, there are exactly m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ and thus $x^m \equiv 1 \pmod{p}$. ■

Definition 1 (Roots of unity)**.** *Let p be prime and m a positive integer. We call the solutions to*

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

the m^{th} roots of unity modulo p.