Wilson's Theorem

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

- Characterize when a is its own inverse modulo a prime.
- Prove Wilson's Theorem and its converse .

Read: Strayer, Section 2.4

Turn: Does this match with your conjecture from Exercise 5? If not, what is the difference?

Lemma 1. Let p be a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo m if and only if $a \equiv \pm 1 \pmod p$.

Proof Let p be a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo m if and only if $a^2 \equiv 1 \pmod p$ if and only if $p \mid a^2 - 1 = (a-1)(a+1)$. Since p is prime, $p \mid a - 1$ or $a + 1$ by **??**. Thus, $a \equiv \pm 1 \pmod p$. ■

Corollary 1. Let p be a prime. Then $x^2 \equiv 1 \pmod p$ if and only if $x \equiv \pm 1 \pmod p$.

Remark 1. It is important to note why we require p is prime. **??** is only true for primes:

- $8 \mid ab$ is true when $8 \mid a$, $8 \mid b$, $4 \mid a$ and $2 \mid b$, or $2 \mid a$ and $4 \mid b$.

Let $a = 2k + 1$ for some integer k. Then

$$a^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Since either k or $k + 1$ is even, $a^2 = 8m + 1$ for some $m \in \mathbb{Z}$. Thus, $a^2 \equiv 1 \pmod 8$ for all odd integers $a \in \mathbb{Z}$.

- When $a \equiv 1 \pmod 8$, then $8 \mid (a - 1)$.
- When $a \equiv 3 \pmod 8$, then $8k = a - 3$ for some $k \in \mathbb{Z}$. Thus $2 \mid (a - 1)$ and $4 \mid (a + 1)$.
- When $a \equiv 5 \pmod 8$, then $8k = a - 5$ for some $k \in \mathbb{Z}$. Thus $4 \mid (a - 1)$ and $2 \mid (a + 1)$.
- When $a \equiv 7 \pmod 8$, then $8 \mid (a + 1)$.

Theorem 1 (Wilson's Theorem)**.** Let p be a prime number. Then

$$(p-1)! \equiv -1 \pmod p.$$

Proof When $p = 2$, $(2-1)! = 1 \equiv -1 \pmod 2$. Now consider p an odd prime. By **??**, each $a = 1, 2, \ldots, p-1$ has a unique multiplicative inverse modulo p. **??** says the only elements that are their own multiplicative inverse are 1 and $p - 1$. Thus $(p-2)!$ is the product of 1 and $\frac{p-3}{2}$ pairs of a, a' where $aa' \equiv 1 \pmod p$. Therefore,

$$\begin{aligned} (p-2)! &\equiv 1 \pmod p \\ (p-1)! &\equiv p - 1 \equiv -1 \pmod p. \end{aligned}$$

■

Wilson's Theorem is normally stated as above, but the converse is also true. It can also be a (very ineffective) prime test.

Proposition 1 (Converse of Wilson's Theorem)**.** Let n be a positive integer. If $(n-1)! \equiv 1 \pmod n$, then n is prime.

Learning outcomes:
Author(s): Claire Merriman

Proof Let a and b be positive integers where $ab = n$. It suffices to show that if $1 \leq a < n$, then $a = 1$. If $a = n$, then $b = 1$. If $1 \leq a < n$, then $a \mid (n-1)!$ by the definition of factorial. Then $(n-1)! \equiv -1 \pmod{n}$ implies $a \mid (n-1)! + 1$ by transitivity of division. Thus, $a \mid (n-1)! + 1 - (n-1)! = 1$ by linear combination and $a = 1$. Therefore, the only positive factors of n are 1 and n, so n is prime. ■

In-class Problem 1 (Part of Strayer, Chapter 2 Exercise 47) Let p be an odd prime. Use (a) $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ to show

(b) If $p \equiv 1 \pmod{4}$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$

(c) If $p \equiv 3 \pmod{4}$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$