Multiplicative inverses using Wilson's Theorem

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

- Use Wilson's Theorem to find the least nonnegative residue modulo a prime .

First, some important algebra for multiplicative inverses
Example 1. (a) Let n be an odd positive integer. Then

$$2\left(\frac{n+1}{2}\right) = n+1 \equiv 1 \pmod{n}.$$

So $\frac{n+1}{2}$ is the multiplicative inverse of 2 modulo n.

Think-Pair-Share 0.1. Why is $\left(\frac{n+1}{2}, n\right) = 1$?

We also have that $n - \frac{n+1}{2} = \frac{n-1}{2}$ and $n-2 \equiv -2 \pmod{n}$, so $\frac{n-1}{2}$ is the multiplicative inverse of $n-2$ modulo n. Another way to see this is

$$-2\left(\frac{n-1}{2}\right) = -n+1 \equiv 1 \pmod{n}.$$

(b) Let m and n be positive integers such that $n \equiv 1 \pmod{m}$. Then there exists $k \in \mathbb{Z}$ such that $n = mk+1$ by the **??**. Then

$$-m\left(\frac{n-1}{m}\right) = -n+1 \equiv 1 \pmod{n}.$$

(c) Let m and n be positive integers such that $n \equiv -1 \pmod{m}$. Then there exists $k \in \mathbb{Z}$ such that $n = mk-1$ by definition. Then

$$m\left(\frac{n+1}{m}\right) = n+1 \equiv 1 \pmod{n}.$$

Example 2. (a) Practice with Wilson's Theorem: Find $\frac{31!}{23!} \pmod{11}$.

$$\begin{aligned} x \equiv \frac{31!}{23!} &\equiv 24(25)(26)(27)(28)(29)(30)(31) \pmod{11} \\ &\equiv 2(3)(4)(5)(6)(7)(8)(9) \pmod{11}. \end{aligned}$$

Then $-x \equiv 10! \equiv -1 \pmod{11}$. Therefore, $x \equiv 1 \pmod{11}$.

(b) Let p be an odd prime p, then $2(p-3)! \equiv -1 \pmod{p}$.

Proof Let p be an odd prime, then $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem. Multiplying both sides of the congruence by -1 gives $(p-2)! \equiv 1 \pmod{p}$. Since $(p-2)! = (p-3)!(p-2)$ by the definition of factorial, $p-2 \equiv -2 \pmod{p}$ is the multiplicative inverse of $(p-3)!$ modulo p. Thus,

$$\begin{aligned} -2(p-3)! &\equiv 1 \pmod{p} \\ 2(p-3)! &\equiv -1 \pmod{p}. \end{aligned}$$

■

Learning outcomes:
Author(s): Claire Merriman