Using modular arithmetic to spped up calculations

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

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

Reading None

Multiplicative inverses using Wilson's Theorem

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 $\dfrac{31!}{23!} \pmod{11}$.*

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

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

Learning outcomes:
Author(s): Claire Merriman

(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,*
>
> $$-2(p-3)! \equiv 1 \pmod{p}$$
> $$2(p-3)! \equiv \qquad\qquad\qquad\qquad -1 \pmod{p}.$$

$\blacksquare$

Finding least nonnegative residue Fermat's Little Theorem

Example 3.   (a) *Find the least nonnegative residue of* 29^{202} *modulo* 13.

> *First, note that* $29 \equiv 3 \pmod{13}$ *and* $202 = 12(10) + 82 = 12(10) + 12(6) + 10 = 12(16) + 10$. *Thus,*
>
> $$29^{202} \equiv 3^{202} \equiv (3^{12})^{16}3^{10} \equiv 1^{16}3^{10} \pmod{13}$$
>
> *From here, we have two options:*
>
> **Keep reducing:** *For this problem, this is the easier method:*
>
> $$3^{10} \equiv (3^3)^3 3 \equiv (27)^3 3 \equiv 3 \pmod{13}.$$
>
> **Find inverse:** *Note that* $3^{12} \equiv 1 \pmod{13}$, *so* 3^{10} *is the multiplicative inverse of* $3^2 \equiv 9 \pmod{13}$. *Since* $9(3) \equiv 1 \pmod{13}$, $3^{10} \equiv 1 \pmod{13}$.

(b) *Find the least nonnegative residue of* 71^{71} *modulo* 17.

> *First, note that* $71 \equiv 3 \pmod{17}$ *and* $71 = 8(8) + 7$. *Thus,*
>
> $$71^{71} \equiv 3^{71} \equiv (3^8)^8 3^7 \equiv 1^8 3^7 \pmod{17}$$
>
> *Then*
>
> $$3^7 \equiv 3^3(3^3)(3) \equiv 10(10)(3) \equiv 10(-4) \equiv -6 \equiv 11 \pmod{17}.$$

Corollary (Corollary 2.14). *Let p be a prime. If* $a \in \mathbb{Z}$ *with* $p \nmid a$, *then* a^{p-2} *is the multiplicative inverse of a modulo p.*

Think-Pair-Share 0.2. Prove: Let p be a prime. If $a, k \in \mathbb{Z}$ with $p \nmid a$ and $0 \le k < p$, then a^{p-k} is the multiplicative inverse of a^k modulo p.

Proof   Let p be a prime. If $a \in \mathbb{Z}$ with $p \nmid a$, then by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.) If $k \in \mathbb{Z}$ with $0 \le k < p$, then $a^{p-1} = a^{p-k}a^k$. Thus, $a^{p-k}a^k \equiv 1 \pmod{p}$. $\blacksquare$

Example 4. *Find all incongruent solutions to* $9x \equiv 21 \pmod{23}$.

Since $(9, 23) = 1$, *there is only one incongruent solution modulo* 23. *By Corollary 2.14,* 9^{21} *is the multiplicative inverse of* 9 *modulo* 23. *Thus,* $x \equiv 21(9^{21}) \pmod{23}$.

Alternately, 3^{20} *is the multiplicative inverse of* 3^2 *modulo* 23, *so* $x \equiv 21(3^{20}) \equiv (3^{21})7 \pmod{23}$. *Since* 3^{21} *is the multiplicative inverse of* 3 *modulo* 23, *so* $3^{21} \equiv 8 \pmod{23}$. *Thus,* $x \equiv 7(8) \equiv 10 \pmod{23}$.

Example 5. *Let p be prime and* $a, b \in \mathbb{Z}$ *with* $p \nmid a$ *and* $p \nmid b$. *Then* $a^p \equiv b^p \pmod{p}$ *if and only if* $a \equiv b \pmod{p}$.

Proof   *Let p be prime and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$.*

($\Longleftarrow$) If $a \equiv b \pmod{p}$, then $a^p \equiv b^p \pmod{p}$ by repeated applications of Proposition 2.4.

($\Longrightarrow$) If $a^p \equiv b^p \pmod{p}$, then by Fermat's Little Theorem,

$$a \equiv a^{p-1}a \equiv b^{p-1}b \equiv b \pmod{p}.$$

$\blacksquare$

Warning 1. *This statement is only true for primes. Since*

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8}, \quad 2^2 \equiv 6^2 \pmod{8},$$

$$1^8 \equiv 3^8 \equiv 5^8 \equiv 7^8 \pmod{8}, \quad 2^8 \equiv 6^8 \pmod{8}.$$