Calculations with Fermat's Little Theorem and Eluer's Theorem

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

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

Finding least nonnegative residue Fermat's Little Theorem

Example 1. (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 1. *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 0.1. Prove: Let p be a prime. If $a, k \in \mathbb{Z}$ with $p \nmid a$ and $0 \leq k < p$, 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 $0 \leq k < p$, then $a^{p-1} = a^{p-k} a^k$. Thus, $a^{p-k} a^k \equiv 1 \pmod{p}$. ■

Example 2. *Find all incongruent solutions to* $9x \equiv 21 \pmod{23}$.

Since$(9, 23) = 1$, *there is only one incongruent solution modulo* 23. *By* , 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,* $x \equiv 7(8) \equiv 10 \pmod{23}$.

Learning outcomes:

Author(s): Claire Merriman

Example 3. *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 $p \nmid b$.*

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

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

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

■

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

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

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

Multiplicative inverses using Euler's Extension of Fermat's Little Theorem

Example 4. (a) *Find the least nonnegative residue of 29^{202} modulo 20.*

The integers $1, 3, 7, 9, 11, 13, 17, 19$ are relatively prime to 20. Thus $\phi(20) = 8$. Also note that $29 \equiv 9 \pmod{20}$ and $202 = 8(25) + 2$, so

$$29^{202} \equiv 9^{202} \equiv (9^8)^{25}9^2 \equiv 1^{25}9^2 \equiv 1 \pmod{20}$$

(b) *Find the least nonnegative residue of 71^{71} modulo 16.*

The integers $1, 3, 5, 7, 9, 11, 13, 15$ are relatively prime to 16. Thus $\phi(16) = 8$. Also note that $71 \equiv 7 \pmod{16}$ and $71 = 8(8) + 7$, so

$$71^{71} \equiv 7^{71} \equiv (7^8)^8 7^7 \equiv 1^8 7^7 \pmod{16}$$

Since $7^8 \equiv 7^7 7 \equiv 1 \pmod{16}$, 7^7 is the multiplicative inverse of 7 mulod 16.

Using the Euclidean algorithm,

$$\begin{aligned} 16 &= 7(2) + 2, & 2 &= 16 + 7(-2) \\ 7 &= 2(3) + 1, & 1 &= 7 - 2(3) = 7 - (16 + 7(-2))(3) = 16(-3) + 7(7) \end{aligned}$$

Thus, $7(7) \equiv 1 \pmod{16}$, and $7^7 \equiv 7 \pmod{16}$.

Corollary 2. *Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then $a^{\phi(m)-1}$ is the multiplicative inverse of a modulo m.*

Example 5. *Find all incongruent solutions to $9x \equiv 21 \pmod{25}$.*

The only positive integers less than 25 that are not *relatively prime to 25 are $5, 10, 15, 20$. Thus, $\phi(25) = 24 - 4 = 20$.*

Since$(9, 25) = 1$, there is only one incongruent solution modulo 25. By , 9^{19} is the multiplicative inverse of 9 modulo 25. Thus, $x \equiv 21(9^{19}) \pmod{25.}$

Alternately, 3^{18} is the multiplicative inverse of 3^2 modulo 25, so $x \equiv 21(3^{18}) \equiv (3^{19})7 \pmod{25}$.

The previous example does not ask for the least nonnegative residue, but let's find it anyway.

Example 6. *Find the least nonnegative residue of $(9^{19})21$ modulo 25.*

First, note that $(9^{19})21 = (3^2)^1 9(21)$. From here there are two options:

Factor 21**:**

$$(9^{19})21 \equiv (3^2)^19(3)(7) \equiv (3^{39})(7) \equiv (3^{20})(3^{19})(7) \pmod{25}$$

By **??**, $3^{20} \equiv 1 \pmod{25}$ *and by* , 3^{19} *is the multiplicative inverse of* 3 *moddulo* 25. *Since* $3(-8) \equiv -24 \equiv 1 \pmod{25}$, $3^{19} \equiv -8 \pmod{25.}$ *Thus,*

$$(9^{19})21 \equiv (-8)(7) \equiv -56 \equiv 19 \pmod{25}.$$

Using $21 \equiv -4 \pmod{25}$**:**

$$(9^{19})21 \equiv (3^2)^19(-4) \equiv (3^{38})(-4) \equiv (3^{20})(3^{18})(-4) \pmod{25}$$

Since $3^{20} = 3^{18}(3^2) \equiv 1 \pmod{25}$ *by* **??**, 3^{18} *is the multiplicative inverse of* $3^2 = 9$ *modulo* 25. *Since* $9(-11) \equiv -99 \equiv 1 \pmod{25}$, *we have* $3^{18} \equiv -11 \pmod{25}$. *Thus,*

$$(9^{19})21 \equiv (-11)(-4) \equiv 44 \equiv 19 \pmod{25}.$$

In-class Problem 1 Let p, q be distinct primes. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Proof Let p, q be distinct primes. Then $\boxed{q^{p-1} \equiv 1} \pmod{p}$ and $\boxed{p^{q-1} \equiv 1} \pmod{q}$ by Fermat's Little Theorem, and $\boxed{p^{q-1} \equiv 1} \equiv 0 \pmod{p}$ and $\boxed{q^{p-1} \equiv 1} \equiv 0 \pmod{q}$ by $\boxed{\text{definition}}$.

Thus, $p^{q-1} + q^{p-1} \equiv \boxed{1} \pmod{p}$ and $p^{q-1} + q^{p-1} \equiv \boxed{1} \pmod{p}$ by $\boxed{\text{modular addition}}$.

(Finish proof using definition of congruence modulo p and q) ■