Monday, February 26: Modular arithmetic 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 (30 min)

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

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

We also have that $n - \dfrac{n+1}{2} = \dfrac{n-1}{2}$ and $n-2 \equiv -2 \pmod{n}$, so $\dfrac{n-1}{2}$ 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 $a \equiv b \pmod{m}$. 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, $x \equiv 1 \pmod{11}$.

(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,*

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

■

Finding least nonnegative residue Fermat's Little Theorem (20 min)

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 $0 \leq k < p$, 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 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 $p \nmid b$.*

($\Leftarrow$) 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*

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

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

Wednesday, February 28: Modular arithmetic calculations and the $\phi-$function

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

- Use Euler's Theorem to find the least nonnegative residue modulo a composite
- Use Euler's Theorem to find the multiplicative inverse of an integer modulo m
- Prove $\phi(4)\phi(5) = \phi(20)$ using an outline that mirrors the proof that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

Reading None

Multiplicative inverses using Euler's Extension of Fermat's Little Theorem (30 min)

Example 6. (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 (Corollary 2.19)**.** *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 7. *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 Corollary 2.19,* 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 8. *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**:**

$$(9^{19})21 \equiv (3^2)^1 9(3)(7) \equiv (3^{39})(7) \equiv (3^{20})(3^{19})(7) \pmod{25}$$

By Euler's Generalization of Fermat's Little Theorem, $3^{20} \equiv 1 \pmod{25}$ *and by Corollary 2.19,* 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 $21 \equiv -4 \pmod{25}$**:**

$$(9^{19})21 \equiv (3^2)^1 9(-4) \equiv (3^{38})(-4) \equiv (3^{20})(3^{18})(-4) \pmod{25}$$

Since $3^{20} = 3^{18}(3^2) \equiv 1 \pmod{25}$ *by Euler's Generalization of Fermat's Little Theorem,* 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) ■

The Euler ϕ-function (20 min)

We will also find a formula for $\phi(n)$ in general. The following exercise will outline the general proof:

In-class Problem 2 *Let us prove that* $\phi(20) = \phi(4)\phi(5)$. *First, note that* $\phi(4) = \boxed{2}$ *and* $\phi(5) = \boxed{4}$, *so* $\phi(20) = \boxed{8}$.

(a) *A number* a *is relatively prime to* 20 *if and only if* a *is relatively prime to* $\boxed{4}$ *and* $\boxed{5}$

(b) *We can partition the positive integers less that* 20 *into*

$$0 \equiv \boxed{4} \equiv \boxed{8} \equiv \boxed{12} \equiv \boxed{16} \pmod 4$$
$$1 \equiv \boxed{5} \equiv \boxed{9} \equiv \boxed{13} \equiv \boxed{17} \pmod 4$$
$$2 \equiv \boxed{6} \equiv \boxed{10} \equiv \boxed{14} \equiv \boxed{18} \pmod 4$$
$$3 \equiv \boxed{7} \equiv \boxed{11} \equiv \boxed{15} \equiv \boxed{19} \pmod 4$$

For any b *in the range* $0, 1, 2, 3$, *define* s_b *to be the number of integers* a *in the range* $0, 1, 2, \ldots, 19$ *such that* $a \equiv b \pmod 4$ *and* $\gcd(a, 20) = 1$. *Thus,* $s_0 = \boxed{0}, s_1 = \boxed{4}, s_2 = \boxed{0}$, *and* $s_3 = \boxed{4}$.

We can see that when $(b, 4) = 1$, $s_b = \phi(\boxed{5})$ *and when* $(b, 4) > 1$, $s_b = \boxed{0}$.

(c) $\phi(20) = s_0 + s_1 + s_2 + s_3$. *Why?*

Solution: *All of the positive integers less than or equal to* 20 *is in exactly one of the congruence classes above. The* s_i *count how many integers in each congruence class are relatively prime to* 20. *If we add them up, we have counted all positive integers less than or equal to* 20.

(d) *We have seen that* $\phi(20) = s_0 + s_1 + s_2 + s_3$, *that when* $(b, 4) = 1$, $s_b = \phi(5)$, *and that when* $(b, 4) > 1$, $s_b = 0$. *Thus, we can say that* $\phi(20) = 0 + \phi(\boxed{5}) + 0 + \phi(\boxed{5})$. *To finish the "proof" we show that there are* $\phi(\boxed{4})$ *integers* b *where* $(b, 4) = 1$.

Solution: *There are* $\boxed{4}$ *congruence classes modulo 4. Of these,* $\boxed{2} = \phi(\boxed{4})$ *have elements that are relatively prime to* 20. *Thus,* $\phi(20) = \phi(4)\phi(5)$.

Friday, March 1: The $\phi-$ function and a preview of primitive roots

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

- Prove that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

Reading None

Turn In Paper 2

Quiz (10 min)

The Euler ϕ-function (20 min)

We will use In-class Problem 2 as an outline to prove

Theorem (Theorem 3.2)**.** *Let m and n be positive integers where $(m, n) = 1$. Then $\phi(mn) = \phi(m)\phi(n)$.*

maybe works?

Proof First, we note that an integer a is relatively prime to mn if and only if it is relatively prime to m and n, since m and n (together) have the same prime divisors as mn.

We can partition the positive integers less that mn into

$$\begin{array}{llllll}
0 & \equiv m & \equiv 2m & \equiv \cdots \equiv (n-1)m & \pmod{m} \\
1 & \equiv m+1 & \equiv 2m+1 & \equiv \cdots \equiv (n-1)m+1 & \pmod{m} \\
2 & \equiv m+2 & \equiv 2m+2 & \equiv \cdots \equiv (n-1)m+2 & \pmod{m} \\
\vdots & \vdots & \vdots & \vdots & \\
m-1 & \equiv 2m-1 & \equiv 3m-1 & \equiv \cdots \equiv nm-1 & \pmod{m}
\end{array}$$

For any b in the range $0, 1, 2, \ldots, m-1$, define s_b to be the number of integers a in the range $0, 1, 2, \ldots, mn-1$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. For each equivalence class b, $\gcd(b, m) \mid km + b$ by linear combination. Thus, $s_b = 0$ if $(b, m) > 1$. If $\gcd(b, m) = 1$, the arithmetic progression, {b, m + b, 2m + b, …, (n-1)m+ b} contains n elements. By In-class Problem 3, the arithmetic progression is a complete residue system modulo n, so $\phi(n)$ elements are relatively prime to n and thus mn.

Thus, can see that when $(b, m) = 1$, $s_b = \phi(n)$ and when $(b, m) > 1$, $s_b = 0$.

Since all of the positive integers less than or equal to mn is in exactly one of the congruence classes above and t he s_i count how many integers in each congruence class are relatively prime to mn, $phi(mn) = s_0 + s_1 + \cdots + s_{m-1}$.

Since $\phi(m)$ of the $s_i = \phi(n)$ and the rest are 0, $\phi(mn) = s_0 + s_1 + \cdots + s_{m-1} = \phi(m)\phi(n)$.

■

In-class Problem 3 *Complete the proof of Theorem 3.2 by proving that, if m, n, and i are positive integers with $(m, n) = (m, i) = 1$, then the integers $i, m+i, 2m+i, ..., (n-1)m+i$ form a complete system of residues modulo n.*