Monday, February 19: Chinese Remainder Theorem

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

- Solve system of linear equations in one variable.
- Prove the Chinese Remainder Theorem. .

Reading None

Multiplicative inverses (20 min)

From Friday

Corollary (Corollary 2.8)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. The linear congruence in one variable $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$. If $(a, m) = 1$, then the solution is unique modulo m.*

Definition (multiplicative inverse of a modulo m)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. We call the unique incongruent solution to $ax \equiv 1 \pmod{m}$ the *multiplicative inverse of a modulo m.*

Example 1. *Examples of multiplicative inverses:*

- $5(3) \equiv 1 \pmod{7}$ *so* 3 *is the multiplicative inverse of* 5 *modulo* 7 *and* 5 *is the multiplicative inverse of* 3 *modulo* 7.
- $9(5) \equiv 1 \pmod{11}$ *so* 5 *is the multiplicative inverse of* 9 *modulo* 11 *and* 9 *is the multiplicative inverse of* 5 *modulo* 11.
- $8(-4) \equiv 8(7) \equiv 1 \pmod{11}$ *so* $7 \equiv -4 \pmod{11}$ *is the multiplicative inverse of* 8 *modulo* 11 *and* 8 *is the multiplicative inverse of* $7 \equiv -4 \pmod{11}$ *modulo* 11.
- $8(5) \equiv 1 \pmod{13}$ *so* 5 *is the multiplicative inverse of* 8 *modulo* 13 *and* 8 *is the multiplicative inverse of* 5 *modulo* 13.

Example using multiplicative inverses:

$$\begin{aligned}
6! &\equiv 6 * 5 * 4 * 3 * 2 * 1 \pmod{7} \\
&\equiv 6 * 5(3) * 4(2) * 1 \pmod{7} \\
&\equiv 6 \pmod{7}
\end{aligned}$$

Think-Pair-Share 0.1. Find $10! \pmod{11}$ and $12! \pmod{13}$. Is there a pattern?

Solution:

$$\begin{aligned}
10! &\equiv 10 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 \pmod{11} \\
&\equiv 10 * 9(5) * 8(7) * 6(2) * 4(3) * 1 \pmod{11} \\
&\equiv 1 \pmod{11}
\end{aligned}$$

$$\begin{aligned}12! &\equiv 12 * 11 * 10 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 \pmod{13}\\ &\equiv 12 * 11(6) * 10(4) * 9(3) * 8(5) * 7(2) * 1 \pmod{13}\\ &\equiv 1 \pmod{13}\end{aligned}$$

For a prime p, $(p-1)! \equiv 1 \pmod{p}$.

Remark 1. *We do need the condition that p is prime. For example, $3! \equiv 2 \pmod{4}$, and $8! \equiv 0 \pmod{9}$.*

Simultaneous Linear congruences in one variable (30 min)

Example 2. *Consider the system of linear equations*

$$\begin{aligned}x &\equiv 2 \pmod{5}\\ x &\equiv 3 \pmod{7}\\ x &\equiv 1 \pmod{8}.\end{aligned}$$

A slow way to find an integer x that satisfies all three congruences is to write out the congruence classes:

$$\begin{aligned}&2, 2+5, 2+5(2), \boxed{2+5(3)}, \ldots\\ &3, 3+7, \boxed{3+7(2)}, 3+7(3), \ldots\\ &1, 1+8, 1+8(2), \boxed{1+8(3)}, \ldots\end{aligned}$$

and see what integers are on all three lists. In addition to being tedius, we this doesn't help find all *such integers.*

To find all such integers, define $M = 5(7)(8) = 280$, and $M_1 = \frac{M}{5} = 7(8), M_2 = \frac{M}{7} = 5(8), M_3 = \frac{M}{8} = 5(7)$. Then each M_i is relatively prime to M by construction. Thus, by Corollary 2.8 the congruences

$$\begin{aligned}M_1x_1 &\equiv 1 \pmod{5}, & 7(8)x_1 &\equiv x_1 \equiv 1 \pmod{5}\\ M_2x_2 &\equiv 1 \pmod{7}, & 5(8)x_2 &\equiv 5x_2 \equiv 1 \pmod{7}\\ M_3x_3 &\equiv 1 \pmod{8}, & 5(7)x_3 &\equiv 3x_3 \equiv 1 \pmod{8}\end{aligned}$$

have solutions. Thus, $x_1 \equiv 1 \pmod{5}, x_2 \equiv 3 \pmod{7}$, and $x_3 \equiv 3 \pmod{8}$.

Note that

$$\begin{aligned}M_1x_1(2) &= 56(1)(2) \equiv 2 \pmod{5}, & M_2 &\equiv M_3 \equiv 0 \pmod{5}\\ M_2x_2(3) &= 40(3)(3) \equiv 3 \pmod{7}, & M_1 &\equiv M_3 \equiv 0 \pmod{7}\\ M_3x_3(1) &= 35(3)(1) \equiv 1 \pmod{8}, & M_1 &\equiv M_2 \equiv 0 \pmod{8}\end{aligned}$$

Thus,

$$x = M_1x_1(2) + M_2x_2(3) + M_3x_3(1) = 56(1)(2) + 40(3)(3) + 35(3)(1)$$

is a solution to all three congruences.

Theorem (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots m_k$ be pairwise relatively prime positive integers (that is, any pair $\gcd(m_i, m_j) = 1$ when $i \neq j$). Let $b_1, b_2, \ldots, b_k$ be integers. Then the system of congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_k$. This solution has the form

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k,$$

where $M_i = \dfrac{M}{m_i}$ and $M_i x_i \equiv 1 \pmod{m_i}$.

Proof Let $m_1, m_2, \ldots m_k$ be pairwise relatively prime positive integers. We start by constructing a solution modulo $M = m_1 m_2 \ldots m_k$. By construction, $M_i = \dfrac{M}{m_i}$ is an integer. Since each the m_i are pairwise relatively prime, $(M_i, m_i) = 1$. Thus, by Corollary 2.8, for each i there is an integer x_i where $M_i x_i \equiv 1 \pmod{m_i}$. Thus $M_i x_i b_i \equiv b_i \pmod{m_i}$. We also have that $(M_i, m_j) = m_j$ when $i \neq j$, so $M_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Let

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k.$$

Then $x \equiv M_i x_i b_i \equiv b_i \pmod{m_i}$ for each $i = 1, 2, \ldots, k$ and $x \equiv M_i x_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Thus, we have found a solution to the system of equivalences.

To show the solution is unique modulo M, consider two solutions x_1, x_2. Then $x_1 \equiv x_2 \pmod{m_i}$ for each $i = 1, 2, \ldots, k$. Thus $m_i \mid x_2 - x_1$. Since $(m_i, m_j) = 1$ when $i \neq j$, $M = [m_1, m_2, \ldots, m_k]$ and $M \mid x_2 - x_1$. Thus, $x_1 \equiv x_2 \pmod{M}$. ■

Wednesday, February 21: 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 .

Reading Strayer, Section 2.4

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

Wilson's Theorem (50 min)

Corollary (Lemma 2.10)**.** *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 Lemma 1.14. 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 2. *It is important to note why we require p is prime. Lemma 1.14 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 (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 Corollary 2.8, each $a = 1, 2, \ldots, p-1$ has a unique multiplicative inverse modulo p. Lemma 2.10 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 (Proposition 2.12)**.** *Let n be a positive integer. If $(n-1)! \equiv 1 \pmod{n}$, then n is prime.*

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 *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 $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$

Solution: *(b) Let p be a prime with $p \equiv 1 \pmod 4$. Then $p = 4k+1$ for some $k \in \mathbb{Z}$. From part (a),*

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+1+1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod p.$$

(c) Let p be a prime with $p \equiv 3 \pmod 4$. Then $p = 4k+3$ for some $k \in \mathbb{Z}$. From part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+3+1)/2} \equiv (-1)^{2k+2} \equiv 1 \pmod p.$$

Theorem (On Paper 2, Polynomial Factorization option)**.** *Let p be a prime number. The congruence $x^2 \equiv -1 \pmod p$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Friday, February 23: Euler's Theorem and Fermat's Little Theorem

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

- Define and find a reduced residue system modulo m
- Define the Euler ϕ-function $\phi(n)$
- Prove Euler's Generalization of Fermat's Little Theorem .

Read Strayer, Section 2.5

Turn in Exercise 50. Prove that $9^{10} = 1 \pmod{11}$ by following the steps of the proof of Fermat's Little Theorem.

Solution: Consider the 10 integers given by $9, 2(9), 3(9), \ldots, 9(10)$. Note that $11 \mid 9i$ for $i = 1, 2, \ldots, 10$ since 11 is prime and $11 \nmid 10$ and $11 \nmid i$. By Corollary 2.8, since $(9, 11) = 1$ if $9i \equiv 9j \pmod{11}$ implies $i \equiv j \pmod{11}$. Therefore, no two of $9, 2(9), 3(9), \ldots, 9(10)$ are congruent modulo 11. So the least nonnegative residues modulo 11 of the integers $9, 2(9), 3(9), \ldots, 9(10)$, taken in some order, must be $1, 2, \ldots, p-1$. Then

$$(9)(2(9))(3(9)) \cdots (9(10)) \equiv (1)(2) \cdots (10) \pmod{11}$$

or, equivalently,

$$9^{10} 10! \equiv 10! \pmod{11}.$$

By Wilson's Theorem, the congruence above becomes $-9^{10} \equiv -1 \pmod{11}$, which is equivalent to $9^{10} \equiv 1 \pmod{11}$.

Quiz (10 min)

Euler's Generalization of Fermat's Little Theorem (40 min)

There are several different ways to present the material in Sections 2.4 through 2.6. In class, we will do the other order: Fermat's Little Theorem to prove Wilson's Theorem. I will keep the result numbering from the book, so they will be out of order.

Definition (reduced residue system modulo m)**.** Let m be a positive integer. We say that $\{r_1, r_2, \ldots, r_k\}$ is a *reduced residue system modulo* m if

- $(r_i, m) = 1$ for all $i = 1, 2, \ldots, k$,
- $r_i \not\equiv r_j \pmod{m}$ when $i \neq j$,
- for all $a \in \mathbb{Z}$ with $(a, m) = 1$, $a \equiv r_1 \pmod{p}$ for some $i = 1, 2, \ldots, k$.

Example 3.

- *The sets* $\{1, 2, 3, 4, 5, 6\}$ *and* $\{5, 10, 15, 20, 25, 30, 35\}$ *are both reduced residue systems modulo* 7.
- *If* p *is prime, then* $\{1, 2, \ldots, p-1\}$ *is a complete residue system modulo* p*. If* $p \neq 5$, $\{5, 10, \ldots, 5(p-1)\}$ *is a complete residue system modulo* p.
- *The sets* $\{1, 5, 7, 11\}$ *and* $\{5, 25, 35, 55\}$ *are both reduced residue systems modulo* 12.

Corollary (Porism 2.18)**.** *Let* m *be a positive integer and let* $\{r_1, r_2, \ldots, r_k\}$ *be a reduced residue system modulo* m*. If* $a \in \mathbb{Z}$ *with* $(a, m) = 1$*, then* $\{ar_1, ar_2, \ldots, ar_k\}$ *is a reduced residue system modulo* m.

This result is also implicitly used in the proof of Fermat's Little Theorem since $\{1, 2, \ldots, p-1\}$ is a reduced residue system.

Proof Let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system modulo m and $a \in \mathbb{Z}$ with $(a, m) = 1$. Since $\{r_1, r_2, \ldots, r_k\}$ and $\{ar_1, ar_2, \ldots, ar_k\}$ have the same number of elements, it suffices to show that $(ar_i, m) = 1$ and $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$. If there exist some prime p such that $p \mid (ar_i, m)$ then $p \mid ar_i$ and $p \mid m$ by Definition (greatest common divisor). By Lemma 1.14, $p \mid a$ or $p \mid r_i$, so either $p \mid (a, m)$ or $p \mid (r_i, m)$. which is a contradiction. Thus, $(ar_i, m) = 1$.

By **??**, $ar_i \equiv ar_j \pmod{m}$ if and only $r_i \equiv r_j \pmod{\frac{m}{(a,m)}}$. Since $(a, m) = 1$, $ar_i \not\equiv ar_j \pmod{m}$ when $i \neq j$. ■

Definition (Euler ϕ-function)**.** Let n be a positive integer. The *Euler ϕ-function* $\phi(n)$ is

$$\phi(n) = \#\{a \in \mathbb{Z} : a > 0 \text{ and } (a, m) = 1\}.$$

Remark 3. *For a positive integer* m, $\phi(m)$ *is the number of reduced residues modulo* m

Example 4.

- $\phi(7) = 6$
- *If* p *is prime,* $\phi(p) = p - 1$
- $\phi(12) = 4$

Theorem (Euler's Generalization of Fermat's Little Theorem)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Corollary (Fermat's Little Theorem)**.** *Let p be prime and $a \in \mathbb{Z}$. If $p \nmid a$, then*

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

Proof Let p be prime and $a \in \mathbb{Z}$, then $(a, p) = 1$ if and only if $p \nmid a$. Since $\phi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$. ■

Warning 1. *The converse of both of these theorems is false. The easiest example is $1^k \equiv 1 \pmod{m}$ for all positive integers k, m. Also note that $2^{341} \equiv 2 \pmod{341}$. Since $(2, 341) = 1$, there exists an integer a such that $2a \equiv 1 \pmod{341}$. Thus*

$$a2^{341} \equiv (2a)2^{340} \equiv 2^{340} \equiv 2a \equiv 1 \pmod{341}.$$

However, $341 = (11)(31)$.

Proof of Euler's Generalization of Fermat's Little Theorem Let m be a positive integer and let $\{r_1, r_2, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m. If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ is a reduced residue system modulo m by Porism 2.18. Thus, for all $i = 1, 2, \dots, \phi(m)$, then $r_i \equiv ar_j \pmod{m}$ for some $j = 1, 2, \dots, \phi(m)$. Thus

$$r_1 r_2 \cdots r_{\phi(min)} \equiv ar_1 ar_2 \cdots ar_{\phi(min)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $(r_i, m) = 1$, there exists $x_i \in \mathbb{Z}$ such that $r_i x_i \equiv 1 \pmod{m}$. Thus,

$$\begin{aligned} r_1 x_1 r_2 x_2 \cdots r_{\phi(min)} x_{\phi(m)} &\equiv a^{\phi(m)} r_1 x_1 r_2 x_2 \cdots r_{\phi(min)} x_{\phi(m)} \pmod{m} \\ 1 &\equiv a^{\phi(m)} \pmod{m}. \end{aligned}$$

■