Monday, February 12: Peer review and introduction to congruences

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

- Prove basic facts about modular arithmetic.
- Understand gaps in argument and writing of proof of Exercise 83. Give classmates useful feedback on their proofs. .

Proposition and examples of $\pmod m$ (30 minutes)

Definition ($a \equiv b \pmod m$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. From Friday, we have the following equivalent definitions of congruence modulo m :

(a) $a \equiv b \pmod m$ if and only if[1] $m \mid b-a$ (standard definition, generalizing even/odd based on divisibility)

(b) $a \equiv b \pmod m$ if and only if a and b have the same remainder with divided by m. That is, That is, there exists unique $q_1, q_2, r \in \mathbb{Z}$ such that $a = mq_1 + r,\ b = mq_2 + r,\ 0 \leq r < m$. (definition generalizing even/odd based on remainder)

(c) $a \equiv b \pmod m$ if and only if a and b differ by a multiple of m. That is, $b = a + mk$ for some $k \in \mathbb{Z}$. (arithmetic progression definition)

Different statements of the definition will be useful in different situations

Proposition 1 (Restatement of Propositions 2.1, 2.4, and 2.5)**.** *Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, then:*

(a) $a \equiv b \pmod m$ *and* $b \equiv c \pmod m$ *implies* $a \equiv c \pmod m$

(b) $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$ *implies* $a + c \equiv b + d \pmod m$

(c) $a \equiv b \pmod m$ *and* $c \equiv d \pmod m$ *implies* $ac \equiv bd \pmod m$.

(d) $a \equiv b \pmod m$ *and* $d \mid m,\ d > 0$ *implies* $a \equiv b \pmod d$

(e) $a \equiv b \pmod m$ *implies* $ac \equiv bc \pmod{mc}$ *for* $c > 0$.

Proof Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$.

(a) Assume $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Then using the second definition of equivalence, there exists $q_1, q_2, q_3, r \in \mathbb{Z}$ such that

$$\begin{aligned} a &= mq_1 + r, & 0 \leq r < m, \\ b &= mq_2 + r, & 0 \leq r < m, \\ c &= mq_3 + r, & 0 \leq r < m. \end{aligned}$$

Thus, a and c have the same remainder when divided by m, so $a \equiv c \pmod m$.

[1] all definitions are if and only if

2/3. Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by the third definition of equivalence, there exists $j, k \in \mathbb{Z}$ such that $b = a + mj$ and $d = c + mk$. Thus,

$$b + d = a + c + m(j + k), \qquad \text{and}$$
$$bd = ac + m(ak + cj + mjk).$$

Thus, $a + c \equiv b + d \pmod{m}$ and $ac = bd \pmod{m}$.

(d) Assume $a \equiv b \pmod{m}$, and $d > 0$ with $d \mid m$. From the first definition of equivalence modulo m, $m \mid b - a$. Since division is transitive, $d \mid b - a$, so $a \equiv b \pmod{d}$.

(e) Assume $a \equiv b \pmod{m}$, and $c > 0$. From the third definition of equivalence modulo m, there exists $k \in \mathbb{Z}$ such that $b = a + mk$. Thus, $bc = ac + mck$, so $ac \equiv bc \pmod{mc}$.

■

Example 1. *Note that* $2 \equiv 5 \pmod{3}$. *Then* $4 \equiv 10 \pmod{3}$ *by Proposition 1 (c), since* $2 \equiv 2 \pmod{3}$. *From part (e),* $4 \equiv 10 \pmod{6}$, *but* $2 \not\equiv 5 \pmod{6}$.

Peer review Chapter 1 Exercise 83 (20 minutes)

Wednesday, February 14: More congruence facts

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

- Prove that $\{0, 1, \ldots, m - 1\}$ is a complete residue system modulo m. .

Basic facts of working modulo m (35 minutes)

Definition (complete residue system)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$. We call the set of all $b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ the *equivalence class of* a. A set of integers such that every integer is congruent modulo m is called a *complete residue system modulo* m.

Proposition (Consequence 2.2, rephrased)**.** *Let* m *be a positive integer. Then equivalence modulo* m *partition the integers. That is, every integer is in exactly one equivalence class modulo* m.

Proof This is an immediate consequence of the fact that equivalence modulo m is an equivalence relation. ■

Notice that this arguments also simplifies the proof the $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proposition (Proposition 2.3)**.** *The set* $\{0, 1, \ldots, m - 1\}$ *is a complete residue system modulo* m.

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$. By the Division Algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $a = qm + r$ with $0 \leq r < m$. In fact, since $0 \leq r < m$, we know $r = 0, 1, \ldots, m - 2$, or $m - 1$. Therefore, every integer is in the equivalence class of $0, 1, \ldots, m - 2$ or $m - 1$ modulo m. Since every integer is in exactly one equivalence class modulo m, and the remainder from the division algorithm is unique, it is not possible for a to be equivalent to any other element of $\{0, 1, \ldots, m - 1\}$. ■

In-class Problem 1 *Practice: addition and multiplication tables modulo* $3, 4, 5, 6, 7$. *I am adding* 9 *to include an odd composite.*

Modulo 3

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$*$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Modulo 4

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$*$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Modulo 5

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[0]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$*$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Modulo 6

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$*$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Modulo 7

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$

$*$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[0]$	$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[0]$	$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[0]$	$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[0]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Modulo 8

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Modulo 9

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[0]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Friday, February 16: Linear congruences in one variable

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

- Prove when a linear congruence in one variable has a solution
- Find all solutions to a linear congruence given a particular solution
- Find the number of incongruent solutions to a linear congruence .

Paper 1 due

Quiz (10 min)

Linear congruences in one variable (40 min)

Remark. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Every row/column of addition modulo m contains $\{0, 1, \ldots, m-1\}$.

We can also say that $a + x \equiv b \pmod{m}$ always has a solution, since $x \equiv b - a \pmod{m}$.

Theorem (Strayer Theorem 2.6 and Porism 2.7)**.** *Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and $d = (a, m)$. The linear congruence in one variable $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$. When $d \mid b$, there are exactly d incongruent solutions modulo m corresponding to the congruence classes*

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \pmod{m}.$$

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and $d = (a, m)$. From the definition of congruence modulo m, $ax \equiv b \pmod{m}$ if and only if $m \mid (ax - b)$. That is, $ax \equiv b \pmod{m}$ if and only if $my = ax - b$ for some $y \in \mathbb{Z}$ from the definition of divisibility. Sine $ax - my = b$ is a linear Diophantine equation, Theorem 6.2 says solutions exist if and only if $(a, -m) = d \mid b$.

In the case that solutions exist, let x_0, y_0 be a particular solution to the linear Diophantine equation. Then x_0 is also a solution to the linear congruence in one variable, since $ax_0 - my_0 = b$, implies $ax_0 \equiv b \pmod{m}$. From Theorem 6.2, all solutions have the from $x = x_0 + \dfrac{mn}{d}$ for all $n \in \mathbb{Z}$. We need to show that these solutions are in exactly d distinct congruence classes modulo m.

Consider the solutions $x_0 + \dfrac{mi}{d}$ and $x_0 + \dfrac{mj}{d}$ for some integers i and j. Then $x_0 + \dfrac{mj}{d} \equiv x_0 + \dfrac{mk}{d} \pmod{m}$ if and only if $m \mid \left(\dfrac{mi}{d} - \dfrac{mj}{d}\right)$. That is, if and only if there exists $k \in \mathbb{Z}$ such that $mk = \dfrac{mi}{d} - \dfrac{mj}{d}$. Rearranging this equation, we get that $x_0 + \dfrac{mj}{d} \equiv x_0 + \dfrac{mk}{d} \pmod{m}$ if and only if $dk = i - j$. Thus, $i \equiv j \pmod{\ }$ by definition of equivalence modulo d. Thus, the incongruent solutions to $ax \equiv b \pmod{m}$ are the congruence classes

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \pmod{m}.$$

■

Example 2. *Let's consider several linear congruences modulo* 12*.*

- *The linear congruence* $2x \equiv 1 \pmod{12}$ *has no solutions, since* $2 \nmid 1$*.*
- *The linear congruence* $8x \equiv b \pmod{12}$ *has a solution if and only if* $4 \mid b$*. Considering the least nonnegative residues, the options for* b *are:*
  - $8x \equiv 0 \pmod{12}$*. The incongruent solutions are* $0, 3, 6, 9 \pmod{12}$*.*
  - $8x \equiv 4 \pmod{12}$*. The incongruent solutions are* $2, 5, 8, 11 \pmod{12}$*. Notice we cannot divide across the equivalence, since* $2x \equiv 1 \pmod{12}$ *has no solutions.*
  - $8x \equiv 8 \pmod{12}$*. The incongruent solutions are* $1, 4, 7, 10 \pmod{12}$*.*
- *The linear congruence* $5x \equiv 1 \pmod{12}$ *has solution* $x \equiv 5 \pmod{12}$*. Since* $(5, 12) = 1$*, the solution is unique.*
- *The linear congruence* $5x \equiv 7 \pmod{12}$ *has solution* $x \equiv -1 \equiv 11 \pmod{12}$*. Since* $(5, 12) = 1$*, the solution is unique. Note that instead of* $12 + 5(-1) = 7$*, we could have done*

$$5(5x) \equiv 5(7) \equiv 11 \pmod{12}.$$