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 .

Instructor Notes: Paper 1 due

Remark 1. *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 1. *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,* **??** *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 **??**, *all solutions have the from $x = x_0 + \frac{mn}{d}$ 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 $x_0 + \frac{mi}{d}$ and $x_0 + \frac{mj}{d}$ for some integers i and j. Then $x_0 + \frac{mj}{d} \equiv x_0 + \frac{mk}{d} \pmod{m}$ if and only if $m \mid \left(\frac{mi}{d} - \frac{mj}{d}\right)$. That is, if and only if there exists $k \in \mathbb{Z}$ such that $mk = \frac{mi}{d} - \frac{mj}{d}$. Rearranging this equation, we get that $x_0 + \frac{mj}{d} \equiv x_0 + \frac{mk}{d} \pmod{m}$ 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 1. *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:*

Learning outcomes:
Author(s): Claire Merriman

  - $8x \equiv 0 \pmod{12}$. *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*

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

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