Modular arithmetic

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

- Prove that congruence modulo m is an equivalence relation on $\mathbb{Z}$.
- Define a complete residue system.
- Practice using modular arithmetic. .

Reading Strayer, Section 2.1 through Example 1.

Turn in The book concludes the section with a caution about division. It states that $6a \equiv 6b \pmod 3$ for all integers a and b. Explain why this is true.

Solution: Since $3 \mid 6a - 6b = 3(2a - 2b)$, $6a \equiv 6b \pmod 3$ for all integers a and b.

Definition (divisibility definition of $a \equiv b \pmod m$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is *congruent to b modulo m* and write $a \equiv b \pmod m$ if $m \mid b - a$, and m is said to be the *modulus of the congruence.* The notation $a \not\equiv b \pmod m$ means a is not congruent to b modulo m, or a is *incongruent to b modulo m.*

Definition (remainder definition of $a \equiv b \pmod m$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is congruent to b modulo m if a and b have the same remainder when divided by m.

Be careful with this idea and negative values. Make sure you understand why $-2 \equiv 1 \pmod 3$ or $-10 \equiv 4 \pmod 7$.

Proposition 1 (Definitions of congruence modulo m are equivalent)**.** *These two definitions are equivalent. That is, for $a, b, m \in \mathbb{Z}$ with $m > 0$, $m \mid b - a$ if and only if a and b have the same remainder when divided by m.*

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$. By the **??**, there exists $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$aq_1m + r_1, 0 \leq r_1 < m, \text{ and}$$
$$bq_2m + r_2, 0 \leq r_2 < m.$$

If $m \mid b-a$, then by definition, there exists $k \in \mathbb{Z}$ such that $mk = b-a$. Thus, $mk = q_2m+r_2-q_1m-r_1$. Rearranging, we get $m(k - q_2 + q_1) = r_2 - r_1$ and $m \mid r_2 - r_1$. Since $0 \leq r_1 < m, 0 \leq r_2 < m$, we have $-m < r_2 - r_1 < m$. Thus, $r_2 - r_1 = 0$, so a and b have the same remainder when divided by m.

In the other direction, if $r_1 = r_2$, then $a - b = q_1m - q_2m = m(q_1 - q_2)$. Thus, $m \mid a - b$. ■

Congruences generalize the concept of evenness and oddness. We typically think of even and odd as "divisible by 2" and "not divisible by 2", but a more useful interpretation is even means "there is no remainder when divided by 2" and "there is a remainder of 1 when divided by 2". This interpretation gives us more flexibility when replacing 2 by 3 or larger numbers. Instead of "divisible" or "not divisible" we have several gradations.

There's two major reasons. As we've already seen, calculations get simplified for modular arithmetic. We'll see later that taking MASSIVE powers of MASSIVE numbers is a fairly doable feat in modular arithmetic. The second reason is that by reducing a question from all integers to modular arithmetic, we often have an easier time seeing what is not allowed.

Learning outcomes:
Author(s): Claire Merriman

Example 1. *We will eventually find a function that generates all integers solutions to the equation* $a^2 + b^2 = c^2$ *(this can be done with only divisibility, so feel free to try for yourself after class).*

Modular arithmetic allows us to say a few things about solutions.

First, let's look at $\pmod 2$**.** *Note that* $0^2 \equiv 0 \pmod 2$ *and* $1^2 \equiv 1 \pmod 2$*.*

Case 1: $c^2 \equiv 0 \pmod 2$ *In this case,* $c \equiv 0 \pmod 2$ *and either* $1^2 + 1^2 \equiv 0 \pmod 2$ *or* $0^2 + 0^2 \equiv 0 \pmod 2$*. So, we know* $a \equiv b \pmod 2$. (Note: $\pmod 4$ will eliminate the $a \equiv b \equiv 1 \pmod 2$ case)

Case 2: $c^2 \equiv 1 \pmod 2$ *In this case,* $c \equiv 1 \pmod 2$ *and either* $0^2 + 1^2 \equiv 1 \pmod 2$*. So, we know* $a \not\equiv b \pmod 2$.

Let's start with $\pmod 3$**.** *Note that* $0^2 \equiv 0 \pmod 3$*,* $1^2 \equiv 1 \pmod 3$*, and* $2^2 \equiv 1 \pmod 3$*.*

Case 1: $c^2 \equiv 0 \pmod 3$**.** *In this case,* $c \equiv 0 \pmod 3$ *and* $0^2 + 0^2 \equiv 0 \pmod 3$*. So, we know* $a \equiv b \equiv c \equiv 0 \pmod 3$*.*

Case 2: $c^2 \equiv 1 \pmod 3$**.** *In this case, c could be* 1 *or* 2 *modulo* 3*. We also know* $0^2 + 1^2 \equiv 1 \pmod 3$*, so* $a \not\equiv b \pmod 3$.

Case 3: $c^2 \equiv 2 \pmod 3$ *has no solutions.*

So at least one of a, b, c *is even, and at least one is divisible by* 3*.*

We can use the idea of congruences to simplify divisibility arguments