¡¡¡¡¡¡¡ Updated upstream ======= ¿¿¿¿¿¿¿ Stashed changes

Modular arithmetic facts

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

- Prove basic facts about modular arithmetic. .

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 $m \mid b - a$ (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. 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

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

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

??/?? 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,

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

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 $a \equiv b \pmod{d}$.

Learning outcomes:
Author(s): Claire Merriman
all definitions are if and only if

(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 **????**, since $2 \equiv 2 \pmod{3}$. From part **??**, $4 \equiv 10 \pmod{6}$, but $2 \not\equiv 5 \pmod{6}$.