<u>Result</u> Let a, b, k, and n be integers with $n \geq 2$. If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$.

Proof. Suppose a, b, k, and n are integers with $n \geq 2$ and suppose $a \equiv b \pmod{n}$. Then $n \mid (a-b)$, so there exists $c \in \mathbb{Z}$ such that $a - b = c \cdot n$. Then

$$ka - kb = k(a-b) = k(cn) = (kc) \cdot n$$

Since $kc \in \mathbb{Z}$, $n \mid (ka - kb)$. Therefore, $ka \equiv kb \pmod{n}$.

EX: Note that $15 \equiv 7 \pmod{4}$. So we also have

$$30 \equiv 14 \pmod{4}$$
$$45 \equiv 21 \pmod{4}$$
$$-150 \equiv -70 \pmod{4}$$

Result. Let $a, b, c, d, n \in \mathbb{Z}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Aside: $a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \Rightarrow a - b = n \cdot k$. $k \in \mathbb{Z}$

$c \equiv d \pmod{n} \Rightarrow n \mid (c-d) \Rightarrow c - d = n \cdot \ell$ $\ell \in \mathbb{Z}$

We want to show $ac - bd \stackrel{?}{=} n \cdot p$. Try multiplying?

$$(a-b)(c-d) = n \cdot k \cdot n \cdot \ell$$
$$ac - ad - bc + bd = n^2 k \ell$$

Maybe give up

$$\begin{aligned} ac - bd &= n^2 k\ell + bc - 2bd \\ &= n^2 k\ell + bc - bd - bd \\ &= n^2 k\ell + b(c-d) - bd \\ &= n^2 k\ell + b \cdot n\ell - bd \end{aligned}$$

Instead, try $a = b + nk$ and $c = d + n\ell$

Proof. Suppose $a, b, c, d, n \in \mathbb{Z}$ and $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $n \mid (a-b)$ and $n \mid (c-d)$, so

$$a - b = n \cdot k \quad \text{and} \quad c - d = n \cdot \ell$$

for some integers k and ℓ. Thus,

$$a = b + n \cdot k \quad \text{and} \quad c = d + n\ell.$$

So

$$\begin{aligned} ac &= (b + nk)(d + n\ell) \\ &= bd + bn\ell + nkd + n^2 k\ell \\ &= bd + n(b\ell + kd + nk\ell) \end{aligned}$$

Since $ac - bd = n(b\ell + kd + nk\ell)$

where $b\ell + kd + nk\ell \in \mathbb{Z}$

This shows $n \mid (ac - bd)$, so $ac \equiv bd \pmod{n}$.

EX. Note that $15 \equiv 7 \pmod{4}$ and $3 \equiv -5 \pmod{4}$.

Then $45 \equiv -35 \pmod{4}$.

Result(?) $a \equiv b \pmod{n}$ if and only if

a and b have the same remainder when divided by n.

Result. Let $n \in \mathbb{Z}$. If $n^2 \not\equiv n \pmod{3}$, then $n \not\equiv 0 \pmod{3}$ and $n \not\equiv 1 \pmod{3}$.

(C.P. If $n \equiv 0 \pmod{3}$ or $n \equiv 1 \pmod{3}$, then $n^2 \equiv n \pmod{3}$.)

Proof. We will show the contrapositive statement is true.

Suppose $n \in \mathbb{Z}$ with $n \equiv 0 \pmod{3}$ or $n \equiv 1 \pmod{3}$.

Case 1. Suppose $n \equiv 0 \pmod{3}$, so $3 \mid (n-0)$, so we get $n = 3k$ for some integer k. Thus,

$$n^2 - n = (3k)^2 - (3k) = 9k^2 - 3k = 3(3k^2 - k).$$

Since $3k^2 - k \in \mathbb{Z}$, this shows $3 \mid (n^2 - n)$ and so $n^2 \equiv n \pmod{3}$.

Case 2. Suppose $n \equiv 1 \pmod{3}$, so $3 \mid (n-1)$, so we

$n - 1 = 3\ell$ for some integer ℓ. Thus,

$$\begin{aligned} n^2 - n &= (3\ell+1)^2 - (3\ell+1) \\ &= (9\ell^2 + 6\ell + 1) - (3\ell+1) \\ &= 9\ell^2 + 6\ell + 1 - 3\ell - 1 \\ &= 9\ell^2 + 3\ell \\ &= 3(3\ell^2 + \ell) \end{aligned}$$

Since $3\ell^2 + \ell \in \mathbb{Z}$, we get $3 \mid (n^2 - n)$. Hence, $n^2 \equiv n \pmod{3}$.

In both cases, $n^2 \equiv n \pmod 3$.

Note: so if n^2 and n have different remainders when divided by 3, then the remainder of n when divided by 3 isn't 0 and isn't 1 (hence, n has remainder 2 when divided by 3).

4.3 Proofs Involving Real Numbers

We will assume certain basic facts about real numbers as true with proof.

1. For all $a \in \mathbb{R}$ and positive even integers n, $a^n \geq 0$.
2. For all $a \in \mathbb{R}$ with $a < 0$ and positive odd integers n, $a^n < 0$.
3. $ab > 0$ if and only if a and b are both positive or both negative
4. If $a \geq b$ and $c > 0$, then $ac \geq bc$ and $\frac{a}{c} \geq \frac{b}{c}$.
5. If $a \geq b$ and $c < 0$, then $ac \leq bc$ and $\frac{a}{c} \leq \frac{b}{c}$.

Theorem. Let $x, y \in \mathbb{R}$. Then $xy = 0$ if and only if $x = 0$ or $y = 0$.

Proof. (If $xy = 0$, then $x = 0$ or $y = 0$.) Suppose $xy = 0$.

Case 1. If $x = 0$, then $x = 0$ or $y = 0$.

Case 2. If $x \neq 0$, then from $xy = 0$, we get

$$\frac{1}{x}(xy) = \frac{1}{x} \cdot 0$$
$$\left(\frac{1}{x} x\right) y = 0$$
$$1 y = 0$$
$$y = 0$$

So $x = 0$ or $y = 0$.

In both cases, we get $x = 0$ or $y = 0$.

(If $x=0$ or $y=0$, then $xy=0$.)

Suppose $x=0$ or $y=0$.

Case 1. Suppose $x=0$. Then $xy=0y=0$

Case 2. Suppose $y=0$. Then $xy=x\cdot 0=0$.

In both cases, $xy=0$.

Work through 4.3

Do # 4.11, 4.12, 4.16(a,b,c), 4.17

4.2 Proofs Involving Congruences of Integers

Preliminary Idea

$\{x \in \mathbb{Z} : x$ is divided by 3 has a remainder of $0\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$\{x \in \mathbb{Z} : x$ is divided by 3 has a remainder of $1\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$\{x \in \mathbb{Z} : x$ is divided by 3 has remainder of $2\} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

Notice that if we take any two numbers x, y from one of the sets, it appears $3 \mid (x-y)$. So we can "group together" numbers based on whether or not their difference is divisible by 3.

Definition. Suppose a, b, and n are integers with $n \geq 2$. We say <u>a is congruent to b modulo n</u> if $n \mid (a-b)$. In this case we will write $a \equiv b \pmod{n}$.

EX: (a) $15 \equiv 7 \pmod{4}$ since $4 \mid (15-7)$

(b) $5 \equiv -50 \pmod{11}$ since $11 \mid (5-(-50))$

(c) $9 \not\equiv 5 \pmod{3}$ since $3 \nmid (9-5)$