Divisibility of Integers

Def: For $a, b \in \mathbb{Z}$ we say that a _____ b (and we write $a \mid b$)
if $\exists$ _____ such that _____ $= b$

- We write $a \nmid b$ otherwise

ex)

Lemma: If ___ and ___ then

Pf) Let $a, b, c \in \mathbb{Z}$. Suppose

Prop: If $a, b \in \mathbb{Z}$ that have the same parity then $4 \mid a^2 - b^2$

Experiment / Scratch work

.

.

.

Pf) Let $a, b \in \mathbb{Z}$ with the same parity. Then we can consider

Rmk: There are many ways to prove something! Let's sketch another proof of the above.

~> First, note that $a^2 - b^2 = (\quad)(\quad)$

~> Remember, we showed that _____ is even already

~> Moreover, have _____ = _____ − _____

~ ~

=> We can write _____ = _____ for _____ $\in \mathbb{Z}$

_____ = _____ for _____ $\in \mathbb{Z}$

$\Rightarrow$ We have $\_\_\_\_\_ = (\quad)(\quad)$

$= (\quad)(\quad)$

$= \_\_\_\_\_$

Congruence of Integers

Let $n \in \mathbb{Z}$ be such that $n \geq 2$

Def: For $a, b \in \mathbb{Z}$ we say that

and write _____ (equiv) iff _____

⌜ i.e., iff $a-b =$ _____ for some _____ $\in \mathbb{Z}$

iff $a =$ $b +$ _____ for some _____ $\in \mathbb{Z}$

iff a and b have the _____
when divided by n ⌟

ex) Saying that $a \equiv 2 \bmod 3$ means

$3 \mid$ _____

$\Leftrightarrow$ a has _____ when divided by 3

So, for example $\_ \equiv 2 \bmod 3$ whereas $\_ \equiv 1 \bmod 3$

Rmk:

Note that

1) $a \equiv b \bmod n \Leftrightarrow$ _____

$\Leftrightarrow a - b =$ _____ for $k \in \mathbb{Z}$

$\Rightarrow (\ )n\_ = (\ )a - b$

$= \_n =$ _____

$\Rightarrow n \mid$ _____

$\Rightarrow$ _____

Ie, if $a \equiv b \bmod n$ then _____

[We call such a property symmetric]

2) For all $a \in \mathbb{Z}$, $a \equiv$ ____ $\bmod n$

[We call such a property reflexive]

3) If $a \overset{(1)}{\equiv} b \bmod n$ and $b \overset{(2)}{\equiv} c \bmod n$ then

---

Pf) (1) $\Leftrightarrow$

(2) $\Leftrightarrow$

Prop: (Arithmetic Properties of Congruence)

Suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then

1) $\_\_\_\_ \equiv \_\_\_\_ \bmod n$

2) $\_\_\_\_ \equiv \_\_\_\_ \bmod n$

Pf) Let $a, b, c, d \in \mathbb{Z}$. Suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$

Prop: For $n \in \mathbb{Z}$, if $n^2 \not\equiv n \bmod 3$ then $n \equiv 2 \bmod 3$

What method of proof looks promising here?

Pf)

ex) Let $n \in \mathbb{Z}$. If $11n-7$ is even, then n is odd

Pf) We proved this before using _____

We can give an alternate direct proof using congruence

First note that we are trying to show

_____ $\equiv$ _____ mod 2

Note we have

- _____ $\equiv 0 \mod 2$
- _____ $\equiv 7 \mod 2$

So we get that _____ $\equiv$ _____ mod 2.

Now we note that ___ $\equiv 1 \mod 2$.

So ___ $\equiv 1 \mod 2$ (*)

Finally we see that

- ___ $\equiv 1 \mod 2$
- ___ $\equiv$ ___ $\mod 2$

So ___ $\equiv$ ___ $\mod 2$. (**)

Combining * and ** we see that

___ $\equiv$ ___ $\mod 2$ as desired

ex) For all $n \in \mathbb{Z}$ we have $n^3 \equiv n \bmod 3$.

Exp:

n	0	1	2	3	4	5
$n \bmod 3$						
n^3	0	1	8	27	64	125
$n^3 \bmod 3$						

Pf)

Cool general fact: For p a prime #, $n^p \equiv \_\_ \mod p$

Inequalities of Real #'s

Some basic strategies

1) For every $x \in \mathbb{R}$, $x^2 \geq$ ___

2) To show LHS $\geq$ RHS $\Leftrightarrow$ _____ ≥ 0

(Show $\geq$ ___ can sometimes show that

_____ $= (\square)^2$)

ex) For $x, y \in \mathbb{R}$ show that $\frac{1}{3}x^2 + \frac{3}{4}y^2 \geq xy$

Pf) Let $x, y \in \mathbb{R}$. We will show _____ ≥ 0

Prop: (Arithmetic Mean ≥ Geometric Mean)

Given $x_1, x_2, \dots x_n \in \mathbb{R}_{\geq 0}$ (non-neg real #'s) we have

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n}$$

with equality iff $x_1 = x_2 = \cdots = x_n$

Pf) We will prove the $n=2$ case. The more general version can be proved when we learn induction.

ex) Back to showing the first example

$$\frac{1}{3}x^2 + \frac{3}{4}y^2 \geq xy$$

Pf) We have

$$\geq \sqrt{(\quad)(\quad)}$$