Yiddish of the Day

"Dos laygt zikh ofn sayKhel" = דאָס לייגט זיך אויפֿן סייכל

Divisibility of Integers

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

- We write $a \nmid b$ (\nmid) otherwise

ex)
- $2 \mid 6$ and $2 \mid 10$
- $3 \mid 9$ and $3 \mid 27$ and $3 \mid 6$
- $2 \nmid 3$ and $3 \nmid 14$

Lemma: If $a \mid b$ and $b \mid c$ then $a \mid c$

Pf) Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid b$ and $b \mid c$.
Therefore, there exists integers x_1, x_2 such that $b = ax_1$ and $c = bx_2$. Then we can plug in the expression for b to get

$$c = (ax_1)x_2$$
$$= a(x_1 x_2) \quad \text{where } x_1 x_2 \in \mathbb{Z}$$

so $a \mid c$ ☺

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

Experiment / Scratch work

- $a = 4 \quad b = 2 \rightsquigarrow a^2 - b^2 = 16 - 4 = 12$
- $a = 9 \quad b = 5 \rightsquigarrow a^2 - b^2 = 81 - 25 = 56$

Pf) Let $a, b \in \mathbb{Z}$ with the same parity. Then we can consider two cases: when a, b are both odd, and

both even. Lets first consider the case where a, b are even. Then $a = 2k$ and $b = 2l$ for some $k, l \in \mathbb{Z}$

Then

$$a^2 - b^2 = 4k^2 - 4l^2 = 4(k^2 - l^2) \quad \text{where } k^2 - l^2 \in \mathbb{Z}$$

so $4 \mid a^2 - b^2$

Now we must also consider when a, b are odd.

Finish the proof in your own time.

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

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

~> Remember, we showed that $a+b$ is even already (when a, b have same parity)

~> Moreover, have $a - b = \underbrace{a+b}_{\text{even}} - \underbrace{2b}_{\text{even}}$

=> We can write $a+b = 2k$ for $k \in \mathbb{Z}$

$a-b = 2l$ for $l \in \mathbb{Z}$

$\Rightarrow$ We have $a^2 - b^2 = (a+b)(a-b)$

$= (2k)(2l)$

$= 4(kl)$

Congruence of Integers

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

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

a is congruent to b modulo n

and write $a \equiv b \bmod n$ (equiv) iff $n \mid a-b$

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

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

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

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

$3 \mid a-2$

$\Leftrightarrow$ a has remainder of 2 when divided by 3

So, for example $5 \equiv 2 \mod 3$ whereas $4 \equiv 1 \mod 3$

Rmk:

Note that

1) $a \equiv b \mod n \Leftrightarrow n \mid a-b$

$\Leftrightarrow a - b = nK$ for $K \in \mathbb{Z}$

$\Rightarrow (-1) n K = (-1)(a-b)$

$= (-K) n = b - a$ where $(-K) \in \mathbb{Z}$

$\Leftrightarrow n \mid b-a$

$\Leftrightarrow b \equiv a \bmod n$

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

[We call such a property symmetric]

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

[We call such a property reflexive]

(because every # divides 0)

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

$a \equiv c \bmod n$

Pf) We know that we have

(1) $\iff n \mid a-b$, i.e. $nk = a-b$ for $k \in \mathbb{Z}$

(2) $\iff n \mid b-c$, i.e. $nl = b-c$ for $l \in \mathbb{Z}$

We have that

$$a-c = a-b+b-c$$

$$= (a-b)+(b-c)$$

$$= nk + nl = n(k+l) \text{ where } k+l \in \mathbb{Z}$$

Prop: (Arithmetic Properties of Congruence)

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

1) $a+c \equiv b+d \bmod n$

2) $ac \equiv bd \bmod n$

Pf) Let $a, b, c, d \in \mathbb{Z}$. Suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$
Therefore we have $a - b = nk$ and $c - d = nl$ for $k, l \in \mathbb{Z}$
Then

$$(a+c) - (b+d) = a - b + c - d$$
$$= nk + nl = n(k+l) \text{ where } k+l \in \mathbb{Z}$$

Now we will show pt (2).

Then $ac = (b+nk)(d+nl)$

$= bd + bnl + dnk + n^2kl$

We see that

$ac - bd = n(bl + dk + nkl)$

$\in \mathbb{Z}$

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?

- Direct proof (this does work but it will in many cases)
- Contrapositive: If $n \not\equiv 2 \bmod 3$ then $n^2 \equiv n \bmod 3$

Pf) We will prove this by contrapositive. That is, we will assume that $n \not\equiv 2 \bmod 3$ and show that $n^2 \equiv n \bmod 3$. We then have two cases.

Case 1: $n \equiv 0 \bmod 3$

In this case we have that $n = 3k$, $k \in \mathbb{Z}$

Therefore $n^2 - n = 3(3k^2) - 3k$

$= 3(\underbrace{3k^2 - k}_{\in \mathbb{Z}})$

Case 2: $n \equiv 1 \bmod 3$

Then we can use the prop above to get

$n(n) \equiv 1(1) \bmod 3$

Hence $n^2 \equiv 1 \bmod 3$. So $n \equiv 1 \bmod 3$ (hence also $1 \equiv n \bmod 3$) and

$n^2 \equiv 1 \bmod 3$ hence $n^2 \equiv n \bmod 3$

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

Pf) We proved this before using contrapositive

We can give an alternate direct proof using congruence

First note that we are trying to show

$$n \equiv 1 \mod 2$$

Note we have

- $11n - 7 \equiv 0 \mod 2$
- $7 \equiv 7 \mod 2$

So we get that $11n \equiv 7 \mod 2$.

Now we note that $7 \equiv 1 \mod 2$.

so $11n \equiv 1 \mod 2$ (*)

Finally we see that

- $11 \equiv 1 \mod 2$
- $n \equiv n \mod 2$ (bc $2 \mid n-n$ since $2(0) = n-n$)

so $11n \equiv n \mod 2$. (**)

Combining * and ** we see that

$n \equiv 1 \mod 2$ 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) Left as exercise to the reader.

Hint will consider cases.

1) $n \equiv 0 \bmod 3$

2) $n \equiv 1 \bmod 3$

$n \equiv 2 \mod 3$

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

Inequalities of Real #'s

Some basic strategies

1) For every $x \in \mathbb{R}$, $x^2 \geq 0$

2) To show $LHS \geq RHS \iff LHS - RHS \geq 0$

(Show ≥ 0 can sometimes show that $LHS - RHS = (\square)^2$)

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 $\frac{1}{3}x^2 + \frac{3}{4}y^2 - xy \geq 0$

We compute that

$$\frac{1}{3}x^2 + \frac{3}{4}y^2 - xy = \frac{1}{12}\left(4x^2 + 9y^2 - 12xy\right)$$

$$= \frac{1}{12}\left((2x)^2 - 2(2x)(3y) + (3y)^2\right)$$

$$= \frac{1}{12}\left(2x - 3y\right)^2$$

$$\geq 0$$

□

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.

Let $x_1, x_2 \in \mathbb{R}_{\geq 0}$. We want to show that

$$\frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}$$

Let $a = \sqrt{x_1}$ and $b = \sqrt{x_2}$

Then we have

$$\frac{x_1+x_2}{2} - \sqrt{x_1 x_2} = \frac{a^2+b^2}{2} - ab$$

$$= \frac{1}{2}\left(a^2+b^2 - 2ab\right)$$

$$= \frac{1}{2}\left(a^2 - 2ab + b^2\right)$$

$$= \frac{1}{2}(a-b)^2 \geq 0$$

☺

ex) Back to showing the first example

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

Pf) We have

$$\frac{\frac{1}{3}x^2 + \frac{3}{4}y^2}{2} \geq \sqrt{\left(\frac{1}{3}x^2\right)\left(\frac{3}{4}y^2\right)}$$

by the last thm.

So we get

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

So multiplying by 2 gives us

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