Yiddish of the Day

"Hak mir nisht keyn tchaynik" = קאַק מיר נישט קיין טשײַנעק

HW 4 Due

Glossary 1 Due

~~"What is this Pruing Due"~~

Next week due (on Gradescope)

Back to Sets

We have the following strategies for proving statements involving sets

1) Venn Diagrams

2) Element chasing (element-wise arguments)

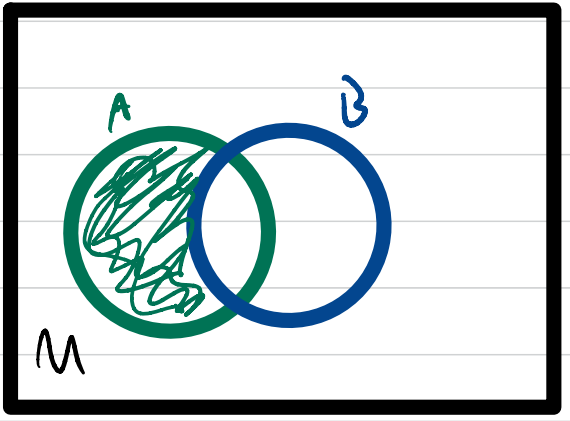
3) Basic Inclusion properties of sets

ex) If $A \subseteq B$ and $B \subseteq C$ then

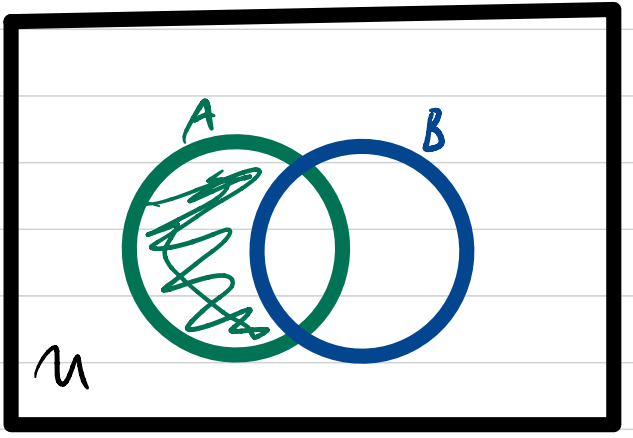
$A \subseteq C$

ex) Show that $A \setminus B = A \cap B^c$

Pf) We'll give a proof by Venn-diagram first



$A \setminus B$



$A \cap B^c$

ex) Show that $A \cup B = A$ iff $B \subseteq A$

⌜ First: this is an "iff" statement. So we have to prove 2 things

a) If $A \cup B = A$ then $B \subseteq A$ and

b) If $B \subseteq A$ then $A \cup B = A$

Also: Remember, showing two sets are equal $X = Y$ requires showing $X \subseteq Y$ and $Y \subseteq X$

⌟

Pf) Let us first assume that $A \cup B = A$. Then we want to show $B \subseteq A$.

Take $x \in B$. Note that $B \subseteq A \cup B$. However, we are assuming that $A \cup B = A$. Therefore $x \in A \cup B = A$

So $x \in A$

Now assume that $B \subseteq A$. We always have that $A \subseteq A \cup B$. So we just need to show that $A \cup B \subseteq A$ in this case.

So let $x \in A \cup B$. Then $x \in A$ or $x \in B$.

If $x \in A$ then nothing to prove. So assume that $x \in B$. Since $B \subseteq A$ we also get that $x \in A$ and hence $A \cup B \subseteq A$ ☺

Prop: (Set-Operation Laws)
Let A, B, C be sets, then

- **Distributive laws:**
  a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- **De-Morgan's Laws:**
  a) $(A \cup B)^c = A^c \cap B^c$
  b) $(A \cap B)^c = A^c \cup B^c$

Pf) Most of these will be left as an exercise to you! Lets prove that

$$(A \cup B)^c = A^c \cap B^c$$

Let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$

Hence $x \in \mathcal{U} \setminus A$ and $x \in \mathcal{U} \setminus B$

So $x \notin A$ and $x \notin B$, hence $x \notin A \cup B$.

Hence $x \in (A \cup B)^c$, so $A^c \cap B^c \subseteq (A \cup B)^c$

Now we will show that $(A \cup B)^c \subseteq A^c \cap B^c$

So let $x \in (A \cup B)^c$. Then $x \in \mathcal{U} \setminus A \cup B$

Hence $x \in \mathcal{U}$ but $x \notin A \cup B$, so $x \notin A$ and $x \notin B$.

So $x \in A^c$ and $x \in B^c$ so $x \in A^c \cap B^c$.

This shows that $(A \cup B)^c \subseteq A^c \cap B^c$

ex) Show that $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$

Pf) We will prove this using already established set operations we know.

We have

$$(A \setminus B) \cap (A \setminus C) = (A \cap B^c) \cap (A \cap C^c) \quad \text{from above}$$
$$= A \cap A \cap B^c \cap C^c \quad \text{commutivity of } \cap$$
$$= A \cap B^c \cap C^c \quad A \cap A = A$$
$$= A \cap (B \cup C)^c \quad \text{last example}$$
$$= A \setminus (B \cup C) \quad \text{from first example}$$

Counterexamples

Consider a universally quantified statement

$\forall x \in S,\ R(x)$

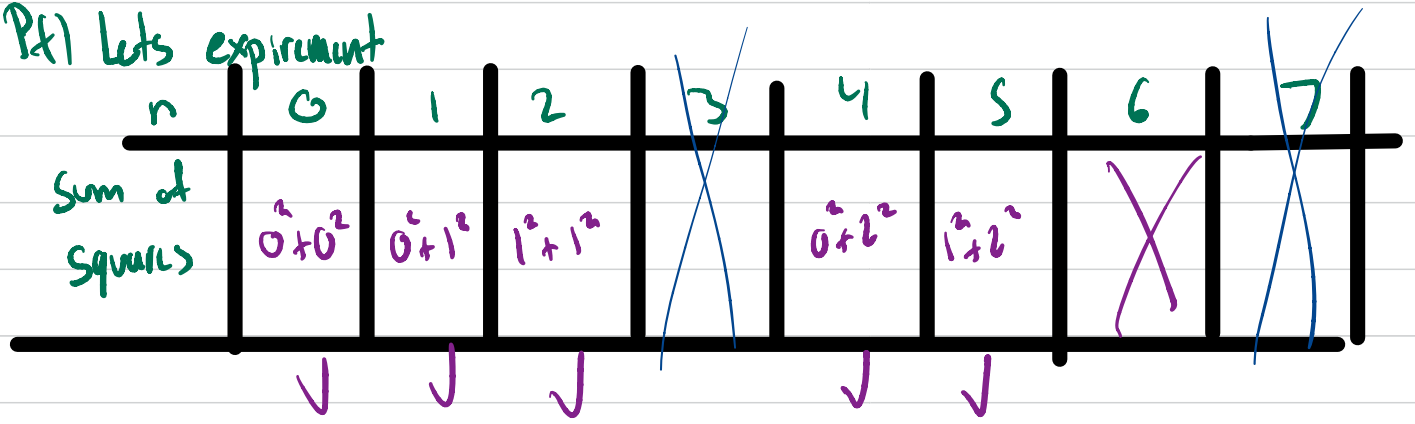
~> Will be either true or false

~> If true, prove it!!!

~> If false, then its negation, $\exists x \in S,\ \neg R(x)$ is true. So to prove original statement is false we have to find (at least one) element $x_0 \in S$ such that $R(x_0)$ is false

~> this element x_0 is called a counterexample

ex) Consider the statement: If $n \equiv 0, 1, 2 \bmod 4$ then n is a sum of two squares ($n = a^2 + b^2$)



Note $6 \equiv 2 \bmod 4$ but 6 is not a sum of 2 squares. So 6 is a counterexample.

ex) Prove or disprove the following. Let $a, b \in \mathbb{R}$ st $a, b \neq 0$

For all $x, y \in \mathbb{R}_{>0}$ $\quad \frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 > xy$

We will try and prove it. If the proof works ☺ ☺ ☺
If not, the reason it didn't may help us find a counterexample

$$\text{LHS} - \text{RHS} = \frac{a^2}{2b^2}x^2 + \frac{b^2}{2a^2}y^2 - xy$$

$$= \frac{1}{2}\left[\left(\frac{ax}{b}\right)^2 + \left(\frac{by}{a}\right)^2 - 2xy\right]$$

$$= \frac{1}{2}\left[\left(\frac{ax}{b}\right)^2 + \left(\frac{by}{a}\right)^2 - 2\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)xy\right]$$

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

$\rightsquigarrow$ LHS − RHS $\geq$ 0

$\rightsquigarrow$ but what about if it $=$ 0

We would have $\frac{a}{b}x = \frac{b}{a}y$

$\rightsquigarrow$ A counterexample can be given by

$x = b^2$ and $y = a^2$

$\Rightarrow$ The statement is false

Proof by Contradiction

Let R be a statement. A proof by contradiction follows the structure

- to show that R is true we show that the negation of R leads to a contradiction

In logical symbols this is $R \equiv (\neg R \Rightarrow \bot)$

Indeed we have the truth table

R	$\neg R$	$\bot$	$\neg R \Rightarrow \bot$

T	F	F	T
F	T	F	F

- In order to show $\neg R \Rightarrow \bot$ is true
  we have $\neg R$ must be false (ie R is true)

Special / Important Case

If the statement R is of the form $P \Rightarrow Q$

then to prove $P \Rightarrow Q$ we can prove

$P \wedge \neg Q \Rightarrow \bot$

recall

$\neg(P \Rightarrow Q)$

$\neg(\neg P \vee Q)$

ex) If $q \in \mathbb{Q}$ and r is an irrational # then $q+r$ is irrational.

Pf) For the sake of contradiction, we will assume that given $q \in \mathbb{Q}$ and r an irrational number that $q+r \in \mathbb{Q}$

Then $q+r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$.

But this implies that $r = \frac{a}{b} - q$. But then $r \in \mathbb{Q}$

which is a contradiction $\rightarrow\leftarrow$

Hence $r+q \notin \mathbb{Q}$ □

ex) Prove that if $n \nmid ab$ then $n \nmid a$ and $n \nmid b$.

Rmk: this will be useful for one of your proof portfolio problems

Pf) For the sake of contradiction, we will assume that $n \nmid ab$ but that $n \mid a$ or $n \mid b$.
WLOG let us say that $n \mid a$. Then $a = n\ell$ for some $\ell \in \mathbb{Z}$.
However, we can then compute
$$ab = n\ell b = n(\ell b) \quad \text{where } \ell b \in \mathbb{Z}.$$
This contradicts the assumption that $n \nmid ab$ ↯

ex) Let $m \in \mathbb{Z}$ st $2 \mid m$ but $4 \nmid m$. Show that there are no integer solutions to the equation $x^2 + 3y^2 = m$ (changed)

Rmk: For non-existance statements, we often will use contradictions.

- Lets do some scratch work before the proof.
  - If $2 \mid m$ but $4 \nmid m$ then
    $m \equiv 2 \pmod 4$

$\rightsquigarrow$ Goal: If $m \equiv 2 \pmod 4$ then $x^2 + 3y^2 = m$ (changed) has no integer solutions

Pf) For the sake of contradiction, let us assume that $m \equiv 2 \bmod 4$ and that $\exists x, y \in \mathbb{Z}$ s.t. $x^2 + 3y^2 = m$

We will first prove a lemma. We claim that, for all $a \in \mathbb{Z}$, $a^2 \equiv 0 \bmod 4$ or $a^2 \equiv 1 \bmod 4$

[Rmk: this lemma will be used in one of your proof portfolio questions....]

Indeed there are 4 options to consider.

1) $a \equiv 0 \bmod 4 \rightsquigarrow a^2 \equiv 0 \bmod 4$
2) $a \equiv 1 \bmod 4 \rightsquigarrow a^2 \equiv 1 \bmod 4$
3) $a \equiv 2 \bmod 4 \rightsquigarrow a^2 \equiv 4 \bmod 4$ so $a^2 \equiv 0 \bmod 4$
4) $a \equiv 3 \bmod 4 \rightsquigarrow a^2 \equiv 9 \bmod 4$ so $a^2 \equiv 1 \bmod 4$

So we will use this fact to produce a contradiction.

Case 1: $x^2 \equiv 0 \bmod 4$ and $y^2 \equiv 1 \bmod 4$

Then $x^2 + 3y^2 \equiv (0 + 3(1)) \bmod 4$

$\equiv 3 \bmod 4$

So this case is not possible

Case 2: $x^2 \equiv 1 \bmod 4$ and $y^2 \equiv 0 \bmod 4$

Then $x^2 + 3y^2 \equiv (1 + 3(0)) \bmod 4$

$\equiv 1 \bmod 4$

So this case is also not possible

Case 3: $x^2 \equiv 0 \bmod 4$ and $y^2 \equiv 0 \bmod 4$

Then $x^2 + 3y^2 \equiv 0 + 3(0) \bmod 4$

$\equiv 0 \bmod 4$ also not allowed

Case 4: $x^2 \equiv 1 \bmod 4$ and $y^2 \equiv 1 \bmod 4$

$$\rightsquigarrow x^2 + 3y^2 \equiv (1 + 3(1)) \bmod 4$$
$$\equiv 4 \bmod 4$$
$$\equiv 0 \bmod 4.$$ also not allowed

But these were all possible cases. Hence it is not possible to have integers x, y such that $x^2 + 3y^2 = m$ in this case