Weds.
9/18

HW 2

P iff Q
$\neg P$ iff $\neg Q$

④ Let A and B be sets.

Prove: $A \subseteq B$ iff $A - B = \emptyset$

Need to show

$(\Longrightarrow)$ If $A \subseteq B$ then $A - B = \emptyset$

$(\Longleftarrow)$ $\underbrace{\text{If } A - B = \emptyset \text{ then } A \subseteq B}_{\text{If } P\text{, then } Q.}$

Contradiction

If P, then Q.

pf: Assume P.
Show $\neg Q$ leads to a contradiction

Thus, Q is true.

Pr
(⇐
W
L
W
I
B
S
T

proof:

($\Leftarrow$) Assume $A-B=\phi$.

We need to show that $A\subseteq B$.

Let $x\in A$.

Why is $x\in B$ true?

If $x\notin B$, then we would have

$x\in A$ and $x\notin B$, implying $x\in A-B$.

But $A-B=\phi$ by assumption.

So $x\in B$.

Thus $A\subseteq B$.

($\Leftarrow$) (Revised)

Assume $A-B=\phi$. $\leftarrow$ $\boxed{\text{Assume } P}$

By way of contradiction, suppose $A\notin B$. $\leftarrow$ $\boxed{\text{What happens if } \neg Q \text{ is true?}}$

Then there would exist $x\in A$ with $x\notin B$. $\leftarrow$

$A\subseteq B$ means:

$\forall x$(If $x\in A$, then $x\in B$)

$A\nsubseteq B$ means:

$\exists x$ where $x\in A$ and $x\notin B$.

$\forall$ for all

$\exists$ there exists

Then $x\in A-B$.

But that contradicts $A-B=\phi$.

So, $A\subseteq B$. $\leftarrow$ Since $\neg Q$ leads to a contradiction Q must be true

($\Rightarrow$) Suppose $A \subseteq B$. Assume P

We need to show that $A - B = \emptyset$. Need to show Q

By way of contradiction,
suppose $A - B \neq \emptyset$. Assume $\neg Q$

There exists $x \in A - B$.

Then $x \in A$ and $x \notin B$.

But this contradicts that $A \subseteq B$. $\neg Q$ leads to a contradiction.

Thus, $A - B = \emptyset$. Therefore Q

$\square$

Division Alg. continued

Ex: $\boxed{a=5,\ b=17}$ $\boxed{\begin{array}{c} b=aq+r \\ 17=5\cdot 3+2 \\ 0\le r<5 \end{array}}$

Define

$$S=\left\{ b-ax \;\middle|\; \begin{array}{l} x\in\mathbb{Z} \text{ and} \\ b-ax\geq 0 \end{array} \right\}$$

$$=\left\{ b-ax \;\middle|\; \begin{array}{l} x\in\mathbb{Z} \text{ and} \\ 17-5x\geq 0 \end{array} \right\}$$

$$=\{2,7,12,17,22,\dots\}$$

smallest integer in S

x	$b-ax=17-5x$	
$\vdots$	$\vdots$	not in S
5	-8	not in S
4	-3	not in S
3	2	in S
2	7	in S
1	12	in S
0	17	in S
-1	22	in S
$\vdots$	$\vdots$	in S

Division Algorithm Let $a, b \in \mathbb{Z}$ with $a > 0$. Then there exists unique integers q and r with $b = aq + r$ and $0 \leq r < a$.

proof:

(existence) Let

$$S = \left\{ b - ax \,\middle|\, \begin{array}{l} x \in \mathbb{Z} \text{ and} \\ b - ax \geq 0 \end{array} \right\}.$$

Let's show that $S \neq \emptyset$.

Case 1: Suppose $b \geq 0$.

Setting $x = -1$ gives

$$b - ax = b + a > 0$$

(because $b \geq 0$ & $a > 0$).

So, $b + a$ is a positive integer in S.

Case 2: Suppose $b < 0$.

Setting $x = 2b$ gives

$$b - ax = b - a(2b) = b(1 - 2a) > 0$$

(since $b < 0$ and $\underbrace{a \geq 1}_{(a > 0)}$ gives $1 - 2a < 0$)

So, $b-a(2b) \in S$.

By case 1 and case 2, $S \neq \phi$.

Since S is not empty and S is a set of non-negative integers, S must have a smallest element.

Let r be the smallest element in S.

So there exists $q \in \mathbb{Z}$ with

$r = b - aq$ and $r = b - aq \geq 0$.

So, $b = aq + r$ with $0 \leq r$.

We now show $r < a$.

Suppose that $r \geq a$.

Then $r - a \geq 0$.

And,

$$r - a = (b - aq) - a = b - a(q+1).$$

Since $r - a \geq 0$ and $r - a = b - a(q+1)$ we know $r - a \in S$.

But $r - a < r$ since $a > 0$.

But then $r-a$ would be an element of S that is smaller than r.

This contradicts the assumption
that r is the smallest element in S.

So, $r < a$.

Thus, there exists $q, r \in \mathbb{Z}$ with $b = aq + r$ and $0 \leq r < a$.

(uniqueness) Suppose we have $b = aq + r$ and
$b = aq' + r'$ with $q, r, q', r' \in \mathbb{Z}$ and $0 \leq r < a$
and $0 \leq r' < a$.

We will show that $q = q'$ and $r = r'$.

$<a$.

Assume $r' \geq r$.

Then $r'-r \geq 0$.

Since

$$b = aq + r = aq' + r'$$

we have

$$a(q-q') = r'-r.$$

Thus, a divides $r'-r$.

But since $0 \leq r < a$ and $0 \leq r' < a$ and $r'-r \geq 0$ we know that

$$0 \leq r'-r < a.$$

$$\boxed{\begin{array}{l} 0 \leq r' < a \\ 0 \leq r'-r < a-r < a \end{array}}$$

Since $a \mid (r'-r)$ we must have $r'-r = 0$.

So, $r' = r$.

Thus, $a(q-q') = r'-r = 0$.

Since $a > 0$, this gives $q - q' = 0$.

So, $q = q'$ $\blacksquare$