CSE 16 2-8-22

- Subsequent class meetings will be

11:25 am to 1:00 pm

Ex. (3.10 #5)

$$\binom{2n}{2} = 2\binom{n}{2} + n^2$$

Proof.

Let $|S| = 2n$, $A \subseteq S$ with $|A| = n$.

Then $\bar{A} = S - A$ also has $|\bar{A}| = n$

The # of 2-subsets of S is obviously

$$\binom{2n}{2}.$$

To count them in a different way, observe the 2-subsets $\{x, y\} \subseteq S$ partition into 2 classes

- $\{x,y\} \subseteq S$ and x, y belong to same half, A or $\bar{A}$. i.e. either $x, y \in A$ or $x, y \in \bar{A}$. To form such a set

  (1) choose which half (A or $\bar{A}$)

  $\#$ ways $= 2$

  (2) choose $\{x,y\} \subseteq A$ (or $\bar{A}$)

  $\#$ ways $= \binom{n}{2}$

  By product rule, there are $2\binom{n}{2}$ ssets of this type.

- $\{x,y\} \subseteq S$ with x, y in different halves, i.e. either $x \in A$, $y \in \bar{A}$ or $x \in \bar{A}$, $y \in A$.

  (1) choose $x \in A$: # ways $= n$
  (2) choose $y \in \bar{A}$: # ways $= n$

  By Prod. rule, # of sets of this type is n^2

By the addition principle the # of 2-ssets of S is

$$2\binom{n}{2} + n^2.$$

This proves

$$\binom{2n}{2} = 2\binom{n}{2} + n^2$$

$\blacksquare$

Exercise (3.10 #6)

show that

$$\binom{3n}{3} = n^3 + 6n\binom{n}{2} + 3\binom{n}{3}$$

Ex. (ex on P. 109)

show

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Proof:
let $A \subseteq S$ with $|S| = 2n$, $|A| = n$, so also $|\bar{A}| = n$. consider

$$\{ B \subseteq S \mid |B| = n \}$$

obviously # elements of this set is $\binom{2n}{n}$.

consider task of constructing $B \subseteq S$. we have $(n+1)$ disjoint types of subsets.

label	# elements in A	# elements in $\bar{A}$	# ways
0	0	n	$\binom{n}{0}\cdot\binom{n}{n}$
1	1	$n-1$	$\binom{n}{1}\cdot\binom{n}{n-1}$
2	2	$n-2$	$\binom{n}{2}\cdot\binom{n}{n-2}$
3	3	$n-3$	$\binom{n}{3}\cdot\binom{n}{n-3}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	$n-1$	1	$\binom{n}{n-1}\cdot\binom{n}{1}$
n	n	0	$\binom{n}{n}\cdot\binom{n}{0}$

Therefore, By the addition principle

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$$

$$= \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k} \qquad \left(\text{since } \binom{n}{n-k} = \binom{n}{k}\right)$$

$$= \sum_{k=0}^{n} \binom{n}{k}^2 .$$

Chap. 4 : Direct Proofs

many theorems are of form

$$P \Rightarrow Q$$

Direct Proof:

Assume P

show as a consequence Q

can use

- previously proved facts
- axioms
- valid inference rules

Number theory: study of $\mathbb{N}, \mathbb{Z}, \mathbb{Q} \dots$

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{\dots, -1, -2, -3, 0, 1, 2, 3 \dots\}$$

$$\mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$$

<u>Defn</u>

let $a, b \in \mathbb{Z}$. we say a <u>divides</u> b iff there exists $k \in \mathbb{Z}$ s.t.

$$b = ka$$

<u>notation</u>: $a \mid b$ (read: "a divides b")

Also say: a is a <u>divisor</u> of b

b is a <u>multiple</u> of a

a is a <u>factor</u> of b.

Remark

we did not define $a|b$ to mean

$$\frac{b}{a} \in \mathbb{Z}$$

(although it's equivalent). This is to keep all expressions in the universe $\mathbb{Z}$ (not $\mathbb{Q}$.)

Ex. $3 \mid 18$ since $18 = 6 \cdot 3$

$5 \mid 75$ " $75 = 15 \cdot 5$

$-5 \mid 75$ " $75 = (-15) \cdot (-5)$

$5 \mid -75$ " $-75 = (-15) \cdot 5$

$-5 \mid -75$ " $-75 = 15 \cdot (-5)$

$3 \nmid 19$ " $19 \neq 3k$ for all $k \in \mathbb{Z}$

Facts

- $1 \mid b$ for all $b \in \mathbb{Z}$ $\quad (k = b)$
- $b \mid b$ for all $b \in \mathbb{Z}$ $\quad (k = 1)$
- $a \mid 0$ for all $a \in \mathbb{Z}$ $\quad (k = 0)$
- $0 \nmid b$ for all $b \neq 0$
- $0 \mid 0$ (with k any integer)

Theorem

For all $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

<u>Proof:</u>

Let $a, b, c \in \mathbb{Z}$. Assume $a|b$ and $b|c$.

Then

$$a|b \Rightarrow b = k_1 a \quad \text{for some } k_1 \in \mathbb{Z}$$

also

$$b|c \Rightarrow c = k_2 b \quad \text{for some } k_2 \in \mathbb{Z}.$$

Hence $c = k_2 b = k_2(k_1 a) = (k_1 k_2) a$.

Since $k_1 \cdot k_2 \in \mathbb{Z}$, we have that

$$a | c$$ ∎

<u>Rmk</u>

we used facts from elem. algebra

- equals can be sub. for equals.
- assoc. law for $\mathbb{Z}$, mult.
- closure of $\mathbb{Z}$ under mult.

Recall

Well ordering Property of $\mathbb{N}$

every non-empty subset of $\mathbb{N}$ contains a least element.

note: also true for $\{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\}$.

Also recall:

Theorem (Division algorithm)

For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b$$

we used W.O.P. to prove:

(1) existence of q, r

exercise: (2) uniqueness of q, r.

Proof of uniqueness

Assume

$$a = q_1 b + r_1 \quad \text{and} \quad 0 \le r_1 < b$$

and

$$a = q_2 b + r_2 \quad \text{and} \quad 0 \le r_2 < b.$$

we must show $r_1 = r_2$ and $q_1 = q_2$.

The eqns. imply

$$q_1 b + r_1 = q_2 b + r_2$$

$$\therefore \quad (q_1 - q_2) b = r_2 - r_1$$

If $r_1 < r_2$, then $0 \le r_1 < r_2 < b$, hence

$$0 < r_2 - r_1 < b$$

$$\therefore \quad 0 < (q_1 - q_2) b < b$$

Since $b > 0$, we can divide through by it

$$0 < q_1 - q_2 < 1,$$

which is impossible. Thus $r_1 \nless r_2$, and therefore $r_1 \geq r_2$. By a similar argument $r_1 \ngtr r_2$, so that $r_1 \leq r_2$. It follows that

$$\boxed{r_1 = r_2}$$

$$\therefore \quad (q_1 - q_2) b = r_2 - r_1 = 0$$

$$\therefore \quad q_1 - q_2 = 0$$

$$\therefore \quad \boxed{q_1 = q_2}$$

$\blacksquare$

Ex.

for any $n \in \mathbb{Z}$, there exist unique k and r such that

$$n = 2k + r \quad \text{and} \quad 0 \leq r < 2$$

Thus either $r = 0$ or $r = 1$. This shows every $n \in \mathbb{Z}$ is one of two forms

- $n = 2k$ (called even)
- $n = 2k + 1$ (called odd)

The uniqueness of r implies no integer is both even and odd.