CSE 16 7-21-20

- no quiz this week
- This Thursday 7-23-20, will have a pre-recorded lecture
- will make up Thursday office hours.

Exercise (3.10 # 6)

Prove

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

Hint count # of $\{x, y, z\} \subseteq S$ where $|S| = 3n$ in two ways. Partition S into 3 sets $A, B, C \subseteq S$ with $|A| = |B| = |C| = n$.

<u>Ex</u> (p. 109 of [ROP].)

show

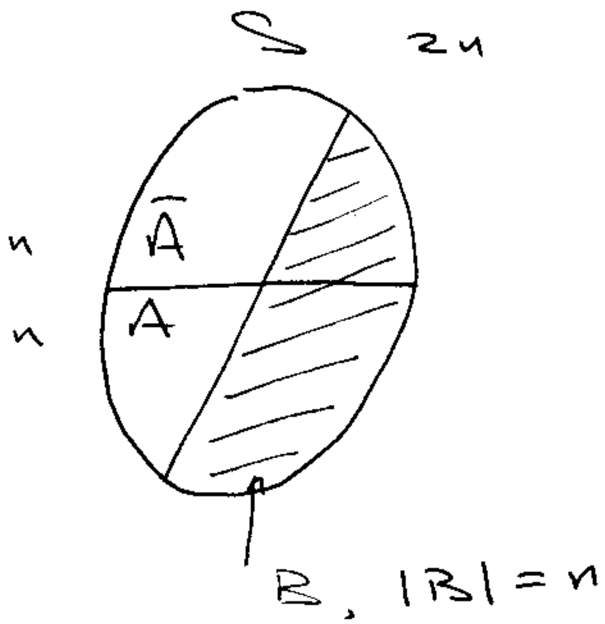
$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

Let $A \subseteq S$ where $|S| = 2n$ and $|A| = n$.
Then $|\bar{A}| = n$ also. consider

(*) $\{B \subseteq S \mid |B| = n\}$

obviously this set has cardinality $\binom{2n}{2}$.
To count this set another way, observe the task of constructing $B \subseteq S$ breaks into $(n+1)$ mutually exclusive subtasks.

i.e. there is a natural partition of (*) into $n+1$ sub-classes.



K	# elements in A	# elements in $\bar{A}$	# ways
0	0	n	$\binom{n}{0}\binom{n}{n}$
1	1	n−1	$\binom{n}{1}\binom{n}{n-1}$
2	2	n−2	$\binom{n}{2}\binom{n}{n-2}$
3	3	n−3	$\binom{n}{3}\binom{n}{n-3}$
⋮	⋮	⋮	⋮
n−1	n−1	1	$\binom{n}{n-1}\binom{n}{1}$
n	n	0	$\binom{n}{n}\binom{n}{0}$

each $B \subseteq S$ with $|B| = n$ belongs to exactly one of the above categories

By the addition Principle

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

But $\binom{n}{n-k} = \binom{n}{k}$ by symmetry;

hence

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

Chapter 4: Direct Proof

Many theorems have the form

$$P \Rightarrow Q$$

i.e. if P, then Q, where P & Q are statements. A *direct proof* proceeds by assuming P is true, then obtain as a consequence Q. *Along* the way we use previously proved facts, axioms, and valid inference rules.

some number theory

Defn
let $a, b \in \mathbb{Z}$. we say a divides b iff there exists $k \in \mathbb{Z}$ such that

$$b = a \cdot k$$

notation: $a \mid b$ (read: "a divides b".)

we also say a is a divisor of b and b is a multiple of a.

Rmk
we didn't define $a \mid b$ to mean that $\frac{a}{b} \in \mathbb{Z}$, although this is clearly equivalent. This is to keep all discussion within the Universe $\mathbb{Z}$ (and not $\mathbb{Q}$.)

Ex.

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

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

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

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

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

$3 \nmid 19$ since $\nexists k \in \mathbb{Z} : 19 = 3k$

i.e. $\forall k \in \mathbb{Z} : 19 \neq 3k$

Facts

- $1 \mid b$ for all $b \in \mathbb{Z}$ $(k = b)$
- $b \mid b$ " " " $(k = 1)$
- $a \mid 0$ " " $a \in \mathbb{Z}$ $(k = 0)$
- $0 \nmid b$ unless $b = 0$

<u>Theorem</u>

for all $a, b, c \in \mathbb{Z}$: if $a|b$ and $b|c$, then $a|c$.

must prove $P \Rightarrow Q$ where

$P = (a|b \text{ and } b|c)$

$Q = (a|c)$

<u>Proof</u>.

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

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

$b|c \Rightarrow c = b k_2$ " " $k_2 \in \mathbb{Z}$.

$\therefore \quad c = b k_2 = (a k_1) k_2 = a(k_1 k_2)$.

Since $k_1 k_2 \in \mathbb{Z}$, we have $a|c$. $\blacksquare$

Recall the Axiom:

<u>Well ordering Property of $\mathbb{N}$</u>

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

<u>note</u> Also true for $\{0\} \cup \mathbb{N}$.

Recall also

<u>Theorem</u> (Division algorithm)
for any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

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

we used W.O.P. to prove

(1) existence of q, r.

left as exercise to prove

(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 two equations 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

$$0 < (r_2 - r_1) < b$$

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

$$\therefore \quad 0 < q_1 - q_2 < 1 \quad (\text{since } b > 0)$$

This is impossible since $q_1 - q_2 \in \mathbb{Z}$ and there is no integer between 0 and 1. Thus $r_1 < r_2$ is false.

$\therefore\ r_1 \geq r_2$. A similar argument shows that $r_2 \geq r_1$. Hence $r_1 = r_2$.

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

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

$$\therefore \quad q_1 = q_2$$

$\blacksquare$

<u>Ex.</u>

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 $r = 0$ or $r = 1$.

Thus every integer is one of two forms

- $n = 2k$ (called <u>even</u>)
- $n = 2k+1$ (called <u>odd</u>)

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

Thus

$$E = \{2k \mid k \in \mathbb{Z}\}$$
$$O = \{2k+1 \mid k \in \mathbb{Z}\}$$

satisfy $E \cap O = \phi$ and $E \cup O = \mathbb{Z}$, i.e. they form a partition of $\mathbb{Z}$.

We could replace 2 by any positive integer.

for instance

- $\{3k \mid k \in \mathbb{Z}\} = [0]_3$
- $\{3k+1 \mid k \in \mathbb{Z}\} = [1]_3$
- $\{3k+2 \mid k \in \mathbb{Z}\} = [2]_3$

Defn

Two integers a, b are said to have the same parity iff they have same remainder on division by 2.

Arithmetic on $\{Even, Odd\}$

a	b	+	×
E	E	E	E
E	O	O	E
O	E	O	E
O	O	E	O