CSE 16 7-14-22

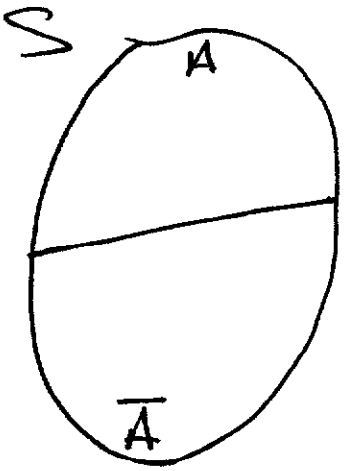
Ex. (P. 109 in Chap. 3)

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

Proof:
Let $|S| = 2n$, and $A \subseteq S$ with $|A| = n$.
obviously RHS is the # of n-element subsets of S:

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

To construct $B \subseteq S$ with $|B| = n$, we perform one of the following $(n+1)$ mutually exclusive subtasks.



K	# elements in A	# elements in $\overline{A}$	# 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	$n-2$	$\binom{n}{2}\cdot\binom{n}{n-2}$
⋮	⋮	⋮	⋮
$n-1$	$n-1$	1	$\binom{n}{n-1}\cdot\binom{n}{1}$
n	n	0	$\binom{n}{n}\cdot\binom{n}{0}$

By the addition principle we have the number of $B \subseteq S$ with $|B| = n$ is:

$$\sum_{K=0}^{n} \binom{n}{K}\cdot\binom{n}{n-K} = \sum_{K=0}^{n} \binom{n}{K}\cdot\binom{n}{K}$$

$$= \sum_{K=0}^{n} \binom{n}{K}^2 = \text{LHS}.$$

$\therefore$ LHS = RHS

Chap. 4 : Direct Proof

many theorems are of the form

$$P \Rightarrow Q .$$

A <u>direct proof</u> of $P \Rightarrow Q$ proceeds by assuming P to be true and showing Q is true as a consequence. we can use

- Previous thms.
- Axioms
- valid inference rules
  (like $(P \wedge (P \to Q)) \to Q$ M.P.)

<u>Defn</u>
let $a, b \in \mathbb{Z}$. we say a <u>divides</u> b iff there exists $k \in \mathbb{Z}$ such that $b = ak$.

<u>notation</u>: $a|b$ read "a divides b"
also say: a is a <u>divisor</u> of b, b is a <u>multiple</u> of a

Rmk:

we did not define $a|b$ to mean

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

although this is equivalent.

Ex.

$2|18$ since $18 = 2 \cdot 6$

$5|75$ since $75 = 5 \cdot 15$

$-5|75$ " $75 = (-5)(-15)$

$5|-75$ " $-75 = 5(-15)$

$-5|-75$ " $-75 = -5(15)$

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

$$\sim\left(\exists k : 19 = 3k\right) = \forall k : 19 \neq 3k$$

Facts

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

Theorem

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

Proof:

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

Then

$$a \mid b \iff b = k_1 a \text{ for some } k_1 \in \mathbb{Z}$$

$$b \mid c \iff c = k_2 b \text{ for some } k_2 \in \mathbb{Z}$$

Therefore

$$c = k_2 b = k_2(k_1 a) = (k_2 k_1)\, a .$$

since $k_2 k_1 \in \mathbb{Z}$, we have

$$a \mid c . \qquad \blacksquare$$

note

we've used some facts:

- equals can be substituted for equals.
- assoc. law for $\mathbb{Z}$.
- closure of $\mathbb{Z}$ under multiplication.

Recall the Axiom

well ordering Prop. of $\mathbb{N}$ (also true for $\mathbb{Z}_{\geq 0}$)

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

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 $q, r \in \mathbb{Z}$

and left as exercise

(2) uniqueness of $q, r \in \mathbb{Z}$.

Proof of (2)

Assume

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

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

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

The 2 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

$$0 < r_2 - r_1 < b$$

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

$$\therefore \quad 0 < q_1 - q_2 < 1$$

Since $q_1 - q_2$ is an int, this is impossible. $\therefore$ $r_1 < r_2$ is impossible.

Similarly $r_2 < r_1$ is also impossible

The only possibility left is $\boxed{r_1 = r_2}$

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

$\Rightarrow \boxed{q_1 = q_2}$.

Ex.

for any $n \in \mathbb{Z}$ there exists a unique k and r s.t.

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

Thus either $r = 0$ or $r = 1$, showing that every int. is one of two forms

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

or

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

Thus

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

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

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

Ex. replace 2 by 3 :
we get a partition of $\mathbb{Z}$ into 3 parts

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

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

We can define an arithmetic on the Parities {Even, Odd} as follows

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

Exercise

Prove that this arithmetic is consistent

For instance: if $a \in O$, $b \in E$ then there exist $k_1, k_2 \in \mathbb{Z}$ s.t.

$$a = 2k_1 + 1$$
$$b = 2k_2$$

Then

$$a+b = (2k_1+1)+2k_2 = 2(k_1+k_2)+1 \in \mathbb{O}$$

and

$$a\cdot b = (2k_1+1)\cdot 2k_2 = 2\left(k_2\cdot(2k_1+1)\right) \in \mathbb{E}$$

Thm

for any $n \in \mathbb{Z}$:

(1) if n is even, then n^2 is even.

and

(2) if n is odd, then n^2 is odd.

Actually the converses of (1), (2) are also true. why

Recall : implication $P \to Q$

converse : $Q \to P$

Contrapositive : $\sim Q \to \sim P$

Recall: $P \to Q = \sim Q \to \sim P$

since $\sim Odd = Even$ and $\sim Even = Odd$

contrapos. of (1) = converse of (2)

" " (2) = " " (1)

simpler form of theorem

Thm

for all $n \in \mathbb{Z}$:

n is even $\iff$ n^2 is even .