CSE 16 7-21-21

Recall: $(P \Rightarrow Q) = (\sim Q \Rightarrow \sim P)$ ✓

contrapositive

also: $(P \Rightarrow Q) \neq (Q \Rightarrow P)$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
0	0	1	1	1	1	1
0	1	1	0	0	1	1
1	0	0	1	1	0	0
1	1	1	1	0	0	1

$=$

By the exercise

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

(1) n even $\Rightarrow n^2$ even

(2) n odd $\Rightarrow n^2$ odd

But converses are also true!

why?

contrapositive of (1) = converse of (2)

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

Restate Thm simply as:

n even $\Leftrightarrow n^2$ even

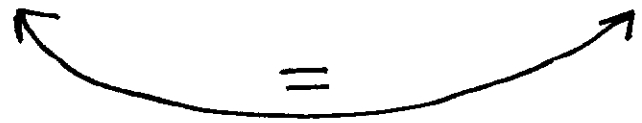
Chapter 5: Contrapositive Proof

Prove $P \Rightarrow Q$ by proving instead its contrapositive $\sim Q \Rightarrow \sim P$

chapter 6: Proof by contradiction

To prove P we can prove $\sim P \Rightarrow F$, (where F is any contradiction, often of the form $R \wedge \sim R$.)

P	$\sim P$	F	$\sim P \Rightarrow F$
0	1	0	0
1	0	0	1



$$\therefore \quad P = (\sim P \Rightarrow F)$$

Theorem

There is no rational number whose square is 2, i.e. $\sqrt{2}$ is *irrational*.

$$\sqrt{2} \in \mathbb{R} - \mathbb{Q}$$

Proof (contradiction)

Assume $\sqrt{2} \in \mathbb{Q}$, i.e. there exist $a, b \in \mathbb{Z}$ $(b \neq 0)$, such that

(*) $$\frac{a}{b} = \sqrt{2} \quad .$$

we may assume (without loss of generality, w.l.o.g.) that a and b have no common factors. (If they do, we may cancel them.)

In Particular:

a and b are not both even

from (*) we have

$$\frac{a^2}{b^2} = 2$$

$\therefore$ $a^2 = 2b^2$

$\therefore$ a^2 even

$\therefore$ a even $\leftarrow$

$\therefore$ $a = 2k$ for some $k \in \mathbb{Z}$

$\therefore$ $(2k)^2 = 2b^2$

$\therefore$ $4k^2 = 2b^2$

$\therefore$ $2k^2 = b^2$

$\therefore$ b^2 even

$\therefore$ b even $\leftarrow$

$\therefore$ <u>both a and b are even</u>

By assuming $\sqrt{2} \in \mathbb{Q}$ we've proved

$R = (a, b \text{ both even})$

and

$\sim R = (a, b \underline{\text{not}} \text{ both even})$

$\therefore R \wedge \sim R$, a contradiction ⚡

Therefore our assumption was false, and $\sqrt{2} \notin \mathbb{Q}$ i.e.

$$\sqrt{2} \in \mathbb{R} - \mathbb{Q}$$

■

Exercise

Prove that $\sqrt{3}$ is irrational.

Follow this outline:

(i) Prove $3 \mid a \Rightarrow 3 \mid a^2$ (direct)

(ii) Prove $3 \mid a^2 \Rightarrow 3 \mid a$ (contrapositive)

i.e. Prove $3 \nmid a \Rightarrow 3 \nmid a^2$.

Do this by cases:

① $a = 3k+1 \Rightarrow 3 \nmid a^2$

② $a = 3k+2 \Rightarrow 3 \nmid a^2$

(iii) by (i) and (ii) $3 \mid a \Leftrightarrow 3 \mid a^2$.

(iv) mimic prev. proof to show

$\sqrt{3} \in \mathbb{Q} \Rightarrow \ldots\ldots \Rightarrow R \wedge \neg R$

(v) Conclude $\sqrt{3} \notin \mathbb{Q}$.

Exercise

Prove that $\sqrt[3]{2}$ is irrational.
(create your own outline, and follow it.)

Def'n

A number $n \in \mathbb{N}$ is called <u>Prime</u> iff it has exactly 2 positive divisors, namely $\{1, n\}$.

If n is not prime, it's called <u>composite</u>.

list:

Prime: 2, 3, 5, 7, 11, 13, ...

Composites: 0, 1, 4, 6, 8, 9, 10, 12, ...
↑ ↑

Note:

- n is composite iff $n = a \cdot b$ where $1 < a \leq b < n$
- 1 is not prime, 0 is not prime.

Theorem

If $n \in \mathbb{N}$ with $n \geq 2$, then n has a prime divisor, i.e. there exist prime p such that

$$p \mid n .$$

Let

$$P = \{ n \in \mathbb{N} \mid n \text{ is prime} \}$$

Thm (Euclid)

P is an infinite set.

Proof (contradiction)

Assume that P is finite, say

$$P = \{ p_1, p_2, p_3, \ldots, p_n \}.$$

define

$$m = (p_1 \cdot p_2 \cdot p_3 \cdots p_n) + 1$$

$\therefore$ $m \geq 2$, so by Prev. thm,

we have

$$\boxed{\exists\, q \in \mathbb{P} : q \mid m}$$

clearly, the remainder of m on division by any p_i $(1 \le i \le n)$ is 1. so

$$\forall\, q \in \mathbb{P} : q \nmid m$$

$$= \boxed{\sim \exists\, q \in \mathbb{P} : q \mid m} \quad \therefore$$

This contradiction shows our assumption was false. $\therefore$ $\mathbb{P}$ is an infinite set.

$\blacksquare$

Thm (fundamental thm. of arithmetic)
Every $n \in \mathbb{Z}^+ = \mathbb{N} - \{0\}$ can be expressed uniquely (up to order) as a product of (zero or more) primes.

note

- 'up to order' means order does not count: $2 \cdot 3 = 6 = 3 \cdot 2$ are not different prime factorizations of 6.
- 'zero or more' extends the meaning of 'product' to include any # of operands
  - Prod. of 0 primes: 1
  - Prod. of 1 prime: that prime $2 = 2$
  - Prod. of 2 primes: $2 \cdot 3 = 6$

Defn

Let $a, b \in \mathbb{Z}$.

- The greatest common divisor of a and b, denoted $\gcd(a,b)$, is the largest integer that divides both a and b. i.e. $d = \gcd(a,b)$ iff
  (i) $d \mid a$ and $d \mid b$
  (ii) if $e \mid a$ and $e \mid b$ then $e \leq d$.
- The least common multiple of a and b, denoted $\operatorname{lcm}(a,b)$, is the smallest (Positive) integer divisible by both a and b.

i.e. $m = \text{lcm}(a,b)$ iff

(i) $a|m$ and $b|m$

(ii) if $a|k$ and $b|k$ then $m \leq k$

Ex. find $\gcd(30, 75)$, $\text{lcm}(30, 75)$

divisors of 30 : 1, 2, 3, 5, 10, 15, 30

" " 75 : 1, 3, 5, 15, 25, 75

common div. of 30, 75 : 1, 3, 5, (15)

$\therefore \gcd(30, 75) = 15$.

Pos. mult. of 30 : 30, 60, 90, 120, (150), 180, ...

" " " 75 : 75, (150), 225, ...

$\therefore \text{lcm}(30, 75) = 150$

notice:

$$30 \cdot 75 = 2250 = 15 \cdot 150$$

Theorem

for any $a, b \in \mathbb{Z}^+$:

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$

Lemma 1:

Let $a, b \in \mathbb{Z}^+$ and let $p_1, p_2, \ldots, p_n$ prime numbers. Suppose

$$a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}$$

for some integers $x_i \geq 0$, $y_i \geq 0$ $(1 \leq i \leq n)$.

Then

$a|b$ iff $x_i \leq y_i$ $(1 \leq i \leq n)$.

Exercise.

try to prove this.

will do next time.