CSE 16 7-19-22

Chap. 5: Contrapositive (indirect) Proof.

To Prove $p \to q$, we Prove it contra-Positive $\sim q \to \sim p$. Recall

$$p \to q \equiv \sim q \to \sim p$$

Chap 6: Proof by contradiction

To Prove p, we can Prove $\sim p \to F$ (where F is any contradiction, usually of the form $r \wedge \sim r$.)

note:

p	$\sim p$	F	$\sim p \to F$
0	1	0	0
1	0	0	1

tautology: $p \equiv \sim p \to F$

Theorem

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

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

Proof.

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

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

We may asume (without loss of generality w.l.o.g) that a and b have no common factors, for if they do, we can cancel.

In particular:

a and b are not both even.

$\therefore \quad \left(\frac{a}{b}\right)^2 = 2$

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

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

$\therefore \quad a^2$ is even

$\therefore \quad$ <u>a is even</u>

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

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

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

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

$\therefore \quad b^2$ is even

$\therefore \quad$ <u>b is even</u>

Hence

<u>a and b are both even</u>

By assuming $\sqrt{2} \in \mathbb{Q}$, we have proved

$r =$ (a and b are both even)

and

$\sim r =$ (a and b are not both even)

hence $r \wedge \sim r$, a contradiction. We conclude $\sqrt{2} \notin \mathbb{Q}$, i.e. $\sqrt{2}$ is irrational

$\blacksquare$

<u>Exercise</u>

Prove $\sqrt{3}$ is irrational by following these steps.

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

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

i.e. show $3 \nmid a \Rightarrow 3 \nmid a^2$. Use cases

① $a = 3k+1 \Rightarrow 3 \nmid a^2$

② $a = 3k+2 \Rightarrow 3 \nmid a^2$

(iii) conclude by (i) & (ii) that

$$3 \mid a \Leftrightarrow 3 \mid a^2$$

(iv) mimic previous proof to show

$$\sqrt{3} \in \mathbb{Q} \Rightarrow \cdots\cdots\cdots \Rightarrow r \wedge \sim r$$

(v) conclude $\sqrt{3} \notin \mathbb{Q}$, i.e. $\sqrt{3}$ is irrational.

<u>Exercise</u>

Prove that $\sqrt[3]{2}$ is irrational.

<u>Defn</u>

A number $n \in \mathbb{N}$ is called <u>prime</u> iff it has <u>exactly 2</u> positive divisors, namely 1 and n. If n has <u>more than 2</u> positive divisors, n is called <u>composite</u>.

note

- n is composite iff $n = a \cdot b$ where $1 < a \le b < n$.
- 1 is neither prime nor composite since it has only one pos. divisor, namely 1.

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Composites: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, ...

Theorem

If $n \in \mathbb{N}$ with $n \geq 2$, then n has a prime divisor: $p \mid n$ for some prime p.

Let

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

we use the prev. theorem to show P is infinite.

<u>Proof</u> (contradiction)

Assume P is finite, say

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

define

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

Then $m \geq 2$, so by prev. Thm

$$\exists\, q \in P : q \mid m$$

But clearly the remainder of m upon division by each p_i ($1 \le i \le n$) is 1, so

$$\forall q \in P : q \nmid m$$

$$\therefore \sim \exists q \in P : q \mid m$$

This ※ (contradiction) shows our assumption was false, hence P is infinite. $\blacksquare$

<u>Theorem</u> (fundamental theorem of arithmetic) Every $n \in \mathbb{N}$ can be expressed uniquely (up to order) as a product of (zero or more) primes.

note

- "up to order" means order does not count, i.e. $2 \cdot 3 = 3 \cdot 2$ are not different factorizations of 6.

- "zero or more" extends meaning of "product" to any number of operands.
    - 1 is a product of 0 primes
    - 2 is " " " 1 prime
    - $6 = 2 \cdot 3$ is a product of 2 primes

Defn

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

- The *greatest common divisor* of a and b, denoted $\gcd(a,b)$ is the largest int. that divides both a and b. i.e. $d = \gcd(a,b)$ iff both

(i) $d \mid a$ and $d \mid b$

(ii) if $e \mid a$ and $e \mid b$, then $e \leq d$.

- The <u>least common multiple</u> of a and b, denoted $lcm(a,b)$, is the smallest (positive) int divisible by both a and b.

  i.e. $m = lcm(a,b)$ iff both

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

  (ii) if $a|k$ and $b|k$, then $m \le k$.

<u>Ex.</u> $gcd(30, 75)$ and $lcm(30, 75)$

div. of 30 : 1, 2, 3, 5, 10, 15, 30

div. of 75 : 1, 3, 5, 15, 25, 75

common div : 1, 3, 5, 15

$\therefore gcd(30, 75) = \boxed{15}$

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

" " " 75 : 75, 150, ...

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

observe:

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

Theorem

for any $a, b \in \mathbb{N}$:

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

Lemma 1

let $a, b \in \mathbb{N}$ and let $p_1, p_2, \ldots, p_n$ be 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 $a \mid b$ iff $x_i \leq y_i$ $(1 \leq i \leq n)$.

Proof

observe

$$b = \left(p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}\right) \cdot \left(p_1^{y_1 - x_1} \cdot p_2^{y_2 - x_2} \cdots p_n^{y_n - x_n}\right)$$

$$= a \cdot k$$

where $k = p_1^{y_1 - x_1} p_2^{y_2 - x_2} \cdots p_n^{y_n - x_n}$.

($\Leftarrow$) if $x_i \leq y_i$, then $y_i - x_i \geq 0$ $(1 \leq i \leq n)$, so k is an integer. $\therefore$ $a \mid b$.

($\Rightarrow$) if $a \mid b$, then $b = a \cdot k'$ for some $k' \in \mathbb{Z}$. But also $b = ak$, hence $ak' = ak$, and $k' = k$. Therefore $k \in \mathbb{Z}$. It follows that $y_i - x_i \geq 0$, $\therefore$ $x_i \leq y_i$ (for $1 \leq i \leq n$). ∎

Lemma 2

Let $a, b \in \mathbb{N}$, and let

$$S = \{p_1, p_2, \ldots, p_n\}$$

be all primes that appear either in the prime factorization of a, or of b, or of both. Thus

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

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

where each $x_i \geq 0$, $y_i \geq 0$ $(1 \leq i \leq n)$.

Then

(1) $\gcd(a,b) = p_1^{\min(x_1,y_1)} p_2^{\min(x_2,y_2)} \cdots p_n^{\min(x_n,y_n)}$

and

(2) $\operatorname{lcm}(a,b) = p_1^{\max(x_1,y_1)} p_2^{\max(x_2,y_2)} \cdots p_n^{\max(x_n,y_n)}$