CSE 16 7-22-20

- no quiz this week
- show work on quiz problems
- Recorded lecture tomorrow.

Exercise:

show arithmetic on Parities is consistent.

for instance

$$O + E = O \quad \text{and} \quad O \cdot E = E$$

let

$$a = 2k_1 + 1$$

$$b = 2k_2$$

for some $k_1, k_2 \in \mathbb{Z}$

Then

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

$$a \cdot b = (2k_1+1)(2k_2) = 2k_2(2k_1+1) \in E$$

all of this follows from uniqueness of r in Division Algorithm.

Exercise

discover the arithmetic on residue classes mod 3:

$$\{3k \mid k \in \mathbb{Z}\} = [0]$$

$$\{3k+1 \mid k \in \mathbb{Z}\} = [1]$$

$$\{3k+2 \mid k \in \mathbb{Z}\} = [2]$$

The arithmetic on $\{E, O\}$ gives us:

Theorem

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.

Recall: given $P \Rightarrow Q$

- converse: $Q \Rightarrow P$
- contrapositive: $\neg Q \Rightarrow \neg P$

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

so $(P \Rightarrow Q) \neq (Q \Rightarrow P)$

but $(P \Rightarrow Q) = (\sim Q \Rightarrow \sim P)$.

since $\sim \text{Odd} = \text{Even}$ and $\sim \text{Even} = \text{Odd}$

$\therefore$ contrapositive of (1) = converse of (2)

" " (2) = " " (1)

Theorem

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

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

Chapter 5: Contrapositive Proof (indirect Proof)

we can prove $P \Rightarrow Q$ by Proving $\sim Q \Rightarrow \sim P$.

inference rule: modus tollens

$$\frac{P \Rightarrow Q \quad \sim Q}{\therefore \sim P}$$

chapter 6: Proof by contradiction

To Prove P Prove $\sim P \Rightarrow F$ where F is a contradiction (usually: $R \wedge \sim R$)

Tautology:
$(\sim P \Rightarrow F) \Leftrightarrow P$

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

inference rule: contradiction

$$\frac{\sim P \Rightarrow F}{\therefore P}$$

Theorem

There is a 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

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

we may assume (without loss of generality W.L.O.G) that a, b have no common factors, since if they do, we can cancel.

In Particular we assume $*$ holds and

a and b are not both even

squaring both sides of *:

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

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

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

$$\therefore \quad a^2 \text{ is even}$$

$$\therefore \quad a \text{ is even} \quad \text{(Prev. thm)}$$

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

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

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

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

$$\therefore \quad b^2 \text{ is even}$$

$$\therefore \quad b \text{ is even} \quad \text{(Prev. thm)}$$

Hence

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

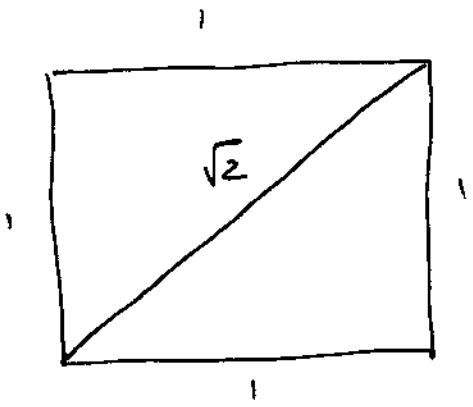
By assuming $\sqrt{2} \in \mathbb{Q}$ we have proved

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

and

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

which yields $R \wedge \sim R$, a contradiction. we conclude $\sqrt{2} \notin \mathbb{Q}$, i.e $\sqrt{2}$ is irrational. ∎



Exercise

Prove $\sqrt{3}$ is irrational.

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

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

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

have 2 cases:

① $a = 3k+1 \Rightarrow 3 \nmid a^2$

② $a = 3k+2 \Rightarrow 3 \nmid a^2$

(iii) conclude by (i) & (ii) $3|a \Leftrightarrow 3|a^2$

(iv) mimic Prev. Proof to show

$\sqrt{3} \in \mathbb{Q} \Rightarrow \ldots\ldots \Rightarrow 2 \wedge 2$ ✗

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

Exercise

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

Defn $\in \mathbb{N}$

A number n is called Prime if it has exactly 2 Positive divisors, namely 1 and n. If n has more than 2 Positive divisors, n is called composite.

note

- n is composite iff $n = a \cdot b$ where $1 < a \leq b < n$.
- 1 is neither Prime nor composite since it has only 1 Positive 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 (divisibility by primes)
If $n \in \mathbb{N}$ with $n \geq 2$, then n has a prime divisor: $p \mid n$.

we can't prove this yet.
we'll do it in chapter 10.

Let

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

Theorem
The set $\mathbb{P} \subseteq \mathbb{N}$ is infinite.

Proof. (contradiction)
Assume $\mathbb{P}$ is finite, say $|\mathbb{P}| = n$

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

define

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

Then $m \geq 2$, so by thm on divisibility by primes we have

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

But clearly remainder of m on division by each p_i $(1 \leq i \leq n)$ is 1. So

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

$$= \sim \exists\, q \in \mathbb{P} : \; q \mid m$$

This contradiction shows our assumption was false, so $\mathbb{P}$ is infinite. ∎