Continuing ...

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

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

existence (div. alg.) $\Rightarrow$ $E \cup O = \mathbb{Z}$

uniqueness $\Rightarrow$ $E \cap O = \emptyset$.

$\therefore$ $\{E, O\}$ form a Partition of $\mathbb{Z}$.

Ex. We can divided any $n \in \mathbb{Z}$ by 3, we get a Partition

$$\{3k \mid k \in \mathbb{Z}\} = [0]_3$$

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

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

We say $a, b \in \mathbb{Z}$ have the same Parity iff they have same remainder on by 2.

Arithmetic on $\{E, O\}$:

	a	b	+	x
	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, suppose $a \in O$, $b \in E$.

Then there exist k_1, k_2 st.

$$a = 2k_1 + 1$$

$$b = 2k_2$$

Then

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

and

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

special case:

Theorem

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

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

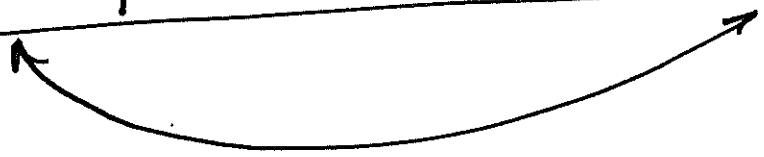
and

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

Actually converses are true. ✓

Recall contrapositive of $P \to Q$

P	Q	$P \to Q$	$Q \to P$	$\sim Q$	$\sim P$	$\sim Q \to \sim P$
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



$\therefore P \to Q \equiv \sim Q \to \sim P$.

note $\sim$ Odd = Even, $\sim$ Even = Odd

contrapositive of (1) = converse of (2)

contrapositive of (2) = converse of (1)

more efficient statement:

<u>Theorem</u> for all $n \in \mathbb{Z}$

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

Chap 5 : Contrapositive Proof

We can Prove $P \Rightarrow Q$ by Proving its contrapositive $\sim Q \Rightarrow \sim P$, which is logically equivalent.

Chap 6 : Proof by contradiction

To Prove a statement P, we can Prove $\sim P \Rightarrow F$ (where F is a contradiction, usually of the form $R \wedge \sim R$.) observe

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

∴ Tautology : $P = (\sim P \Rightarrow F)$

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 $a, b \in \mathbb{Z}$ such that

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

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

In Particular, (*) holds, and

a and b are not both even

Then

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

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

$$\therefore \quad a^2 = 2b^2 \longleftarrow (**)$$

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

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

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

$$\therefore \quad (2k)^2 = 2b^2 \quad \text{by } (**)$$

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

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

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

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

Hence

a and b are both even

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

$R =$ "a and b are both even"

and

$\sim R =$ "a and b are not both even"

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

we conclude that $\sqrt{2} \notin \mathbb{Q}$,

i.e. $\sqrt{2}$ is irrational. ∎

Exercise

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

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

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

by proving its contrapositive: $3 \nmid a \Rightarrow 3 \nmid a^2$.

Do this by cases.

① $a = 3k+1 \Rightarrow 3 \nmid a^2$

② $a = 3k+2 \Rightarrow 3 \nmid a^2$

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

$3|a \Leftrightarrow 3|a^2$

(iv) mimic previous proof to show

$\sqrt{3} \in \mathbb{Q} \Rightarrow \ldots\ldots\ldots\ldots \Rightarrow 1 \sim 1$

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

Exercise

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

Defn

A number $n \in \mathbb{N}$ is called Prime if it has exactly 2 positive divisors, namely 1 and n. If n has more than 2 positive divisors, then n is called composite.

Rmk

- 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.

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

Composites: 4, 6, 8, 9, 10, 12, 14, 15, 16, 20, 21, ...

Theorem

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

(Proof later)

Let

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

we will show P is infinite.

Thm P is infinite

Proof (contradiction)

Assume $\mathbb{P}$ is finite, say

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

define

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

Then $m \geq 2$, and by previous thm

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

But clearly the remainder of m on division by p_i $(1 \leq i \leq n)$ is 1, so

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

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

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

The theorem on divisibility by primes has another consequence

Theorem (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 doesn't count, i.e. $2 \cdot 3 = 3 \cdot 2$ are not different prime factorizations of 6.

- 'zero or more' extends the meaning of 'product' to include any number of operands.
  - 1 is a product of 0 primes
  - 2 " " " " 1 prime
  - 6 " " " " 2 primes
  - 30 " " " " 3 "

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 $\operatorname{lcm}(a,b)$, is the smallest (positive) int. divisible by both a and b.

i.e. $m = \operatorname{lcm}(a,b)$ if both

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

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