Recap of last lecture :

- Infinite sets A, B have same cardinality if $\exists$ bijective fn. $f : A \to B$.
  - using Schroder-Bernstein, suffices to show injective fns. $g : A \to B$ and $h : B \to A$.

$$F = \{ S : S \subseteq \mathbb{N}, |S| \text{ is finite} \}$$

- $\mathbb{N}, \mathbb{Z}, \mathbb{N} \times \mathbb{N}, \mathbb{N}^3$, are all of same cardinality.
  - showing injective fn. $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is easy
  - injective fn. $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$?
    - * solution 1 : 'numbering' the $\mathbb{N} \times \mathbb{N}$ grid
    - * solution 2: $h(x,y) = 2^{x-1}(2y-1)$
    - * solution 3: $h(x,y) = 2^x 3^y$
    - * solution 4: $h(x,y) = (x^{th} \text{ prime no})^y$.
    - need to prove that these are injective.

- $\mathbb{N}$ and power set of $\mathbb{N}$ - $P(\mathbb{N})$ have different cardinality. $\exists$ surjective fn. from $P(\mathbb{N}) \to \mathbb{N}$, but $\nexists$ surjective fn. from $\mathbb{N}$ to $P(\mathbb{N})$.

[Cantor] $\nexists$ surjective fn. $f : \mathbb{N} \to P(\mathbb{N})$.

Thm 2.3: $S = \{$set of all infinite bit-strings$\}$.
$\nexists$ surjective fn. $f : \mathbb{N} \to S$.

Find the flaw in this 'proof':

Claim: Let $W = \{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$.
$\nexists$ surjective fn. $f : \mathbb{N} \to W$.

"Proof": PROOF BY CONTRADICTION.
Suppose, on the contrary, $\exists$ surjective fn. $f : \mathbb{N} \to W$.
Let $z = \sum_{i=1}^{\infty} f(i)$.

Claim: $z \in W$, but $\nexists\, j$ s.t. $f(j) = z$.
"Proof": $\forall\, j$, $z > f(j)$.

Hence, contradiction. ∎

Flaws in the above "proof":
$z \notin W$ [z is not well defined] Any natural number should have finite representation, and therefore the sum/product of infinitely many natural numbers is not a natural number.

If sum/product of infinitely many natural nos. is a natural no., then we can also "prove" that $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ have same cardinality

Claim: $\exists$ injective fn. $f: \mathcal{P}(\mathbb{N}) \to \mathbb{N}$.

"**Proof**": Let p_i denote the i^{th} prime no.

For any set S, let $f(S) = \prod_{x \in S} p_x$

↑ not a natural no. if S is infinite.

Fact: Any natural number must have finite representation (and hence, sum/product of infinitely many numbers is not a natural no.)

This follows from the axioms of natural numbers (Peano's axioms).

LECTURE 03: NATURAL NUMBERS

Def. 3.1 A number $n \in \mathbb{N}$ is said to be composite if $\exists\, j, k \in \{2, \dots, n-1\}$ s.t. $n = j \cdot k$. If $n > 1$ and not composite, then we say n is prime.

Thm 3.1: Every natural number $n > 1$ is either a prime, or can be expressed as product of primes.

From the definition of prime/composite numbers, we know that if a number n is not prime, then it can be expressed as a product of two numbers smaller than n. But how do we conclude that it can be expressed as a product of two or more primes? This does not follow from the definition of primes, and we need a new 'axiom'.

Axiom (well ordering Principle):
Every non empty subset of natural numbers has a smallest element.

Pf: PROOF BY CONTRADICTION.

Suppose, on the contrary, there exist composite nos. that cannot be expressed as product of primes.

Let $S = \{ n : n \text{ is composite and cannot be expressed as prod. of primes} \}$

By our assumption, S is non-empty, and $S \subseteq \mathbb{N}$.

Using WOP, $\exists$ a smallest number in S.
Let x be the smallest number in S.

Since x is composite, $x = a \cdot b$ for some a, b s.t. $1 < a < x$, $1 < b < x$.

Since $a < x$, $b < x$, $a \notin S$, $b \notin S$.

Therefore, either a, b are primes, or can be expressed as product of primes.

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_k \qquad b = q_1 \cdot q_2 \cdot \dots \cdot q_l$$

Then $$x = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_l .$$

x is expressed as product of primes, hence we arrive at a contradiction. ∎

In the next lecture, we will prove that the prime factorization is unique (up to reordering)

Thm 3.2 : There exist infinitely many primes.

Proof: PROOF BY CONTRADICTION.

Suppose there exist only finitely many primes. Let $1 < p_1 < p_2 < \dots < p_k$ be the finite set of primes.

Consider the number $N = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

$N > p_k$. If N is prime, then we have a prime larger than p_k, hence contradiction.

If N is composite, then using Thm 3.1, it can be expressed as product of primes, $N = q_1 \cdot q_2 \cdot \dots \cdot q_l$.

But $q_1 \notin \{p_1, p_2, \ldots, p_k\}$, since none of the primes p_i divide N.

Hence we arrive at a contradiction (we assumed $p_1 \ldots p_k$ are the only primes, and we found a new prime $q_1 \notin \{p_1, \ldots, p_k\}$

∎

WELL ORDERED SETS

Def 3.2: A set S is well-ordered if any subset of S has a min. element.

$\mathbb{N}$ is well-ordered. Finite sets are well ordered. What about non-negative rationals?

Exercise 1: $\nexists\ a, b, c \in \mathbb{N}$ s.t.

$$4a^3 + 2b^3 = c^3.$$

Proof: PROOF BY CONTRADICTION.

Suppose, on the contrary, $\exists$ natural nos. a, b, c s.t. $4a^3 + 2b^3 = c^3$.

Let $C = \{ c : \exists\ a, b \text{ s.t. } 4a^3 + 2b^3 = c^3 \}$

Using WOP, $\exists$ smallest element in C, say c_0. By def^n., $\exists\ a_0, b_0$ s.t.
$4a_0^3 + 2b_0^3 = c_0^3$.

Observation: 2 divides $c_0^3 \Rightarrow$ 2 divides c_0.
Let $c_0 = 2c_1$, where $c_1 \in \mathbb{N}$.

Note: This observation also needs a proof. In particular, we are using the fact that 2 is prime, and if a prime divides z^3, then it must divide z.

$$4a_0^3 + 2b_0^3 = 8c_1^3 \Rightarrow 2a_0^3 + b_0^3 = 4c_1^3$$

Observation: 2 divides $b_0^3 \Rightarrow$ 2 divides b_0.
Let $b_0 = 2b_1$, where $b_1 \in \mathbb{N}$.

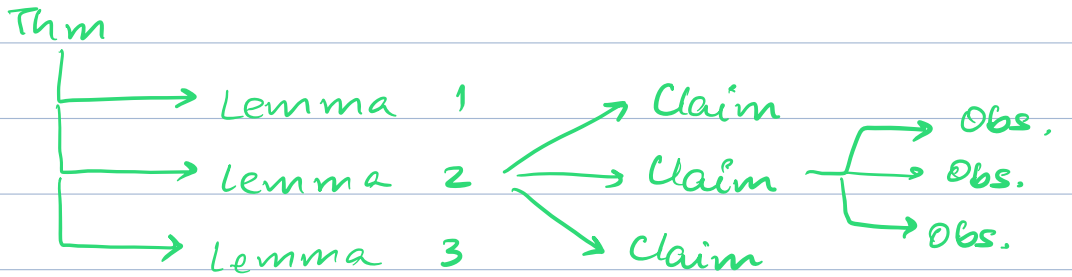
$$4a_0^3 + 16b_1^3 = 8c_1^3 \Rightarrow a_0^3 + 4b_1^3 = 2c_1^3$$

Observation: 2 divides $a_0^3 \Rightarrow$ 2 divides a_0.
Let $a_0 = 2a_1$, where $a_1 \in \mathbb{N}$.

$\Rightarrow 8a_1^3 + 4b_1^3 = 2c_1^3 \Rightarrow 4a_1^3 + 2b_1^3 = c_1^3$.

$\Rightarrow c_1 \in C$ and $c_1 < c_0$. Contradiction since we assumed c_0 is the smallest positive integer in C_0.

PROOF WRITING TIP: Structure long proofs.



No draws - one of the two teams wins.

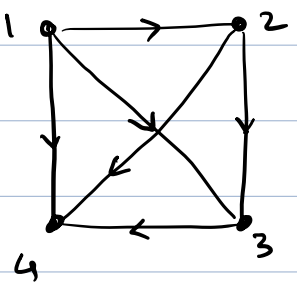
Exercise 2: Tournament with n teams.

Round robin format, every team plays1 every other team exactly once. A cycle in a tournament, of length k, is a sequence of teams $(p_1\ p_2 \dots p_k)$ s.t.

p_1 defeats p_2, p_2 defeats p_3, ..., p_k defeats p_1.

Qn: Does every tournament have a cycle?

No. Counterexample



Claim: If a tournament has a cycle (of some length), then it has a cycle of length 3.

Proof: PROOF BY CONTRADICTION

Suppose ∃ a tournament that has cycles, but no cycle of length 3.

let $S = \{ i : \text{tournament has a cycle of length } i \}$

By WOP, S has a smallest element, say l_0.

Since we assumed that this tournament has no 3-cycle, but it has some cycle, $l_0 > 3$.

∃ team sequence $(P_1, P_2, \ldots, P_{l_0})$ s.t.

P_1 defeated P_2, P_2 defeated P_3, ..., P_{l_0} defeated P_1.

Let us consider the game bet^{n} P_1 and P_3. If P_3 defeated P_1, then we have a 3-cycle (P_1, P_2, P_3).

If P_1 defeated P_3, then consider the sequence $(P_1, P_3, P_4, \cdots, P_{l_0})$.

This sequence has length $l_0 - 1$, and is a cycle. Therefore $l_0 - 1 \in S$.

Contradiction (since we assumed l_0 is the smallest element in S).

□

Summary :

WOP : Let $S \subseteq \mathbb{N}$, $|S| > 0$. Then S has a minimal element.

Proofs using WOP :

Step 1 : State "proof by contradiction"

Step 2 : Define set S. Note that it must be a nonempty subset of $\mathbb{N}$.

Step 3. State "Using WOP, S has a min. element, say l_0.

Step 4 : Arrive at a contradiction.

Bulk the work is in Step 4.