Theorem 1.2 There are infinitely many primes. (I… in Euclid's *Elements*, Book IX, Proposition 20.)

For contradiction suppose there are only a finite number n of primes,

$$p_1, p_2, p_3, \ldots, p_n$$

Let $q = p_1 p_2 p_3 \cdots p_n + 1$.

Claim q is another prime distinct from the $p_1, p_2, \ldots, p_n$.

Clearly $q > p_i$ for every $i = 1, \ldots, n$ so it's distinct.

Is it prime? Why?

Since $q > p_i$ for every $i = 1, \ldots, n$ and by assumption p_i's are the only primes. Then we know q should not be a prime and so it's divisible by one of the p_i's.

Let i be such that $q = m p_i$ for some $m \in \mathbb{Z}$

Thus, p_i divides q.

Thus

$$m p_i = q = \underbrace{p_1 p_2 p_3 \cdots p_n}_{\text{one of those in the product is } p_i} + 1.$$

$$m p_i = q = \left(p_i \prod_{j \neq i} p_j \right) + 1$$

$$p_i \left(m - \prod_{j \neq i} p_j \right) = 1$$

Product of two integers thats equal 1. This can only happen if $p_i = \pm 1$ which can't be, because p_i is a prime.

Proof Suppose there are only finitely many distinct primes, say $p_1, p_2, \ldots, p_n$. Let $M = p_1 p_2 \cdots p_n + 1$. Then M is an integer, and so there exists a prime that divides M. Thus some p_i divides M. But p_i divides $p_1 p_2 \cdots p_n$. Therefore, p_i divides 1, which is a contradiction. ■

Chapter 1.2 Sets

Notation: $x \in A$ means x is an element of the set A

$x \notin A$ means x is not an element of the set A

me → $\boxed{A \subseteq B}$

book → $\boxed{A \subset B}$

$B \supseteq A$

$B \supset A$

mean for every $x \in A$ then $x \in B$.

that is $x \in A \implies x \in B$.

$A = B$ means $A \subseteq B$ and $B \subseteq A$.

$A \subsetneq B$ means A is a proper subset of B

that is $A \subseteq B$ and $A \neq B$.

axiom there is such a thing. → $\emptyset$ is the empty set.

example $\emptyset = \{x \in \mathbb{R} : x^2 < 0\}$.

$A \cup B = \{x : x \in A \text{ or } x \in B\}$

$A \cap B = \{x : x \in A \text{ and } x \in B\}$

$A \setminus B = \{x : x \in A \text{ and } x \notin B\}$

Proposition 1.6 Let A, B, and C be sets. Then

1. $A \cup A = A$ and $A \cap A = A$;
2. $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$;
3. $A \subset A \cup B$ and $A \cap B \subset A$;
4. $A \cup B = B \cup A$ and $A \cap B = B \cap A$ (commutative property);
5. $A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$ (associative property);
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributive property);
7. $A \subset B$ if and only if $A \cup B = B$ and $A \subset B$ if and only if $A \cap B = A$.

Proposition 1.7 Let A, B, and C be sets. Then

1. $A \setminus \emptyset = A$ and $A \setminus A = \emptyset$
2. DeMorgan's Laws:

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$

and

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C).$$

DeMorgan's Laws are generally remembered as stating that the comple-

Let's try DeMorgan's.

Let's show $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

"$\subseteq$" Let $x \in A \setminus (B \cup C)$. Claim $x \in (A \setminus B) \cap (A \setminus C)$.

Thus $x \in A$ and $x \notin B \cup C$

Note $B \cup C = \{z : z \in B \text{ or } z \in C\}$

So $x \notin B \cup C$ means $x \notin B$ and $x \notin C$.

not $x \in B \cup C$ means not $x \in \{z : z \in B \text{ or } z \in C\}$

means $x \in \{z : \text{not}(z \in B \text{ or } z \in C)\}$

(de Morgans for Logic)

means $x \in \{z : \text{not } z \in B \text{ and not } z \in C\}$

$x \in \{z : z \notin B \text{ and } z \notin C\}$

Thus $x \notin B$ and $x \notin C$.

Therefore $x \in A$ and $x \notin B$ and $x \notin C$.

So $(x \in A \text{ and } x \notin B)$ and $(x \in A \text{ and } x \notin C)$

So $x \in A \setminus B$ and $x \in A \setminus C$

Finally... $x \in (A \setminus B) \cap (A \setminus C)$

☑ Claim $\boxed{x \in (A \setminus B) \cap (A \setminus C)}$

"$\supseteq$" Let $x \in (A \setminus B) \cap (A \setminus C)$ Claim $x \in A \setminus (B \cup C)$..

For next time:

1. finish this proof
2. read the DeMorgan's law for arbitrary intersections and unions.