Coffee @ 4 to view class recordings

Defn: a natural number n is prime if it has exactly two positive divisors, 1 and n.

a natural number is composite if it is not prime.

Fact: a natural number $n>1$ is composite if and only if $\exists$ $n=ab$, for $a,b\in\mathbb{N}$, $a<n$ and $b<n$.

Goal: Theorem NT3.2 (Euclid's Theorem) there are infinitely many primes.

Theorem NT3.1 Every natural number $n>1$ is either prime or divisible by a prime.

Proof (contradiction). Suppose there exist natural numbers >1 that are not prime and are not divisible by a prime. Let S be the set of these numbers.

Let n be the smallest element of S.

n is not prime and n is not divisible by a prime, by definition of S.

Since n is not prime, n is composite (by definition of composite).

So $n=ab$, $a,b\in\mathbb{N}$, with $a<n$ and $b<n$, by

the fact stated above.

Note that $a|n$, by the definition of divides.

Consider the number a. There are two cases:

Case 1: a is prime.

then n is divisible by a prime, which is a contradiction.

Case 2: a is not a prime,

thus a is composite, by defn of composite.

Question: is it possible that a is in the set S?

Note a cannot be a member of S, since $a < n$ and n is the smallest member of S.

Since $a \notin S$, either a is prime or a is divisible by a prime. Thus a is divisible by a prime p.

so $p|a$, p is prime.

so $a = px$, $x \in \mathbb{Z}$, by definition of divides.

Since $n = ab$

$$n = (px)b$$

$$n = p(xb)$$

note $xb \in \mathbb{Z}$ since $x \in \mathbb{Z}$, $b \in \mathbb{N}$ and $\mathbb{Z}$ closed under multiplication

thus $p|n$ by definition of divides, so n is divisible by a prime, contradiction $\square$

Theorem there are infinitely many primes.

Proof (contradiction): Suppose there are only finitely many primes. lets call them $p_1, p_2, p_3, \ldots, p_n$

Goal: show there must be a prime not on this list

Consider the number

$$K = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_n + 1$$

for any p_i, note that $p_i \nmid K$ (it has a remainder of 1)

But, by theorem NT 3.1, K is either prime itself, or is divisible by a prime.

In either case, there is a prime not in the list $p_1, p_2, \ldots, p_n$.

Contradiction

$\square$