Math 4460
1/27/25

Theorem: Let n be an integer with $n \geq 2$. Then, n can be written as the product of one or more primes

Ex:

$n = 120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$ is the product of five primes

$n = 2$ is the "product" of one prime

proof by strong/complete induction:

Let $S(n)$ be the statement:

"n can be written as the product of one or more primes."

When $n=2$, the statement $S(2)$ is "2 can be written as the product of one or more primes" which is true since $n=2$ is prime.

Let k be an integer with $k>2$.

Assume $S(n)$ is true for all $2 \le n < k$ induction hypothesis

Ex: If $k=5$, we are assuming $S(2), S(3), S(4)$ are true, ie 2, 3, 4 can be factored into primes

Goal: Show $S(k)$ is true, ie k is the product of one or more primes.

Case 1: Suppose k is prime. Then k is the product of one prime and so $S(k)$ is true.

Case 2: Suppose k is not prime.

This implies there is a positive divisor w of k where $w \neq 1$ and $w \neq k$.

So, $2 \leq w < k$.

Then, $k = wz$ for some positive integer z.

If $z = 1$, then $w = k$ which can't happen.

If $z = k$, then $w = 1$ which can't happen.

So, $2 \leq z < k$.

Since $2 \leq w < k$ and $2 \leq z < k$

we know $S(w)$ and $S(z)$ are true.

So, $w = p_1 p_2 \cdots p_r$

and $z = q_1 q_2 \cdots q_s$

where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes.

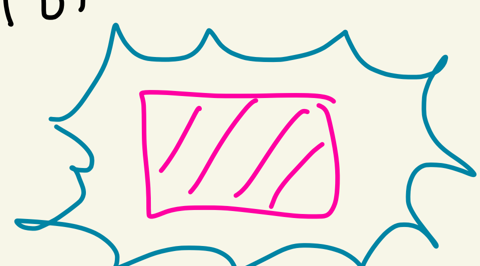
Then

$$k = wz$$
$$= p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

is a product of primes.

So, $S(k)$ is true.

By magical powers of induction $S(n)$ is true for all $n \geq 2$.



Lemma: Let $x, y, z \in \mathbb{Z}$ with $x \neq 0$.
If $x \mid y$ and $x \mid (y+z)$,
then $x \mid z$.

Proof:
Suppose $x \mid y$ and $x \mid (y+z)$.
Since $x \mid y$ we know $y = xk$
where $k \in \mathbb{Z}$.
Since $x \mid (y+z)$ we know
$y + z = xl$ for some $l \in \mathbb{Z}$.

Consequently,
$$z = xl - y = xl - xk$$

$= x(\ell - k).$

Since $\ell, k \in \mathbb{Z}$ we know $\ell - k \in \mathbb{Z}$.

So $z = x(\ell - k)$ implies that $x \mid z$. $\blacksquare$

Theorem (Euclid)

There are infinitely many primes.

proof by contradiction:

Suppose there are finitely many primes $p_1, p_2, \ldots, p_r$.

Let

$$N = p_1 p_2 \cdots p_r + 1$$

Ex: Only 3 primes

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$

$$N = 2 \cdot 3 \cdot 5 + 1 = 31$$

Our previous theorem tells us that N has at least one prime divisor.

So at least one of the $p_1, p_2, \ldots, p_r$ will divide N.

WLOG (without loss of generality) assume $p_1 \mid N$.

So, $p_1 \mid (\underbrace{p_1 p_2 \cdots p_r + 1}_{N})$

But also $p_1 \mid p_1 p_2 \cdots p_r$

The lemma gives then $p_1 \mid 1$.

Then $p_1 = \pm 1$

This can't happen since p_1 is prime.

Contradiction.

So there must be an infinite # of primes.

$\boxed{\boxed{\text{EUCLID}}}$

Calculus method

One can show that

$$\sum_{\substack{2 \le p < n \\ p \text{ prime}}} \frac{1}{p} > \log(\log(n)) - 1$$

Ex: $n=6$

$$\sum_{\substack{2 \le p < 6 \\ p \text{ prime}}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} > \log(\log(6)) - 1$$

Let $n \to \infty$

$$\underbrace{\sum_{p \text{ prime}} \frac{1}{p}}_{\text{this sum diverges}} > \infty$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

So infinite # of primes.