Induction

To prove \( \forall n \in \mathbb{N}, P(n) \):

- Prove \( P(0) \), and
- Prove \( P(n+1) \), assuming \( P(n) \) (for an arbitrary \( n > 0 \))

Claim: every natural number \( n \geq 2 \) can be written as a product of one or more primes

- Defn: \( n \) is composite if \( n = k \cdot \ell \) for some natural numbers \( k \geq 2 \) and \( \ell \geq 2 \).
- Defn: \( n \) is prime if it is not composite

Proof by induction.

Let \( P(n) \) be the statement

\[
\text{\( n \) can be written as a product of primes.}
\]

Base case: \( P(2) \) states \( 2 \) can be written as a product of one or more primes.

\[ 2 = 2 \quad \text{let} \quad p_1 = 2, \text{note} \quad 2 \text{ is prime.} \]

Inductive step: Assume \( P(n) \) holds for some \( n \in \mathbb{N} \).

If \( n+1 \) is prime, we're done.

\[ \text{let} \quad p_1 = n+1, \quad p_1 \text{ is prime, } n+1 = p_1. \]

If \( n+1 \) is not prime,

\[ n+1 = k \cdot l \quad \text{for some } k \geq 2 \text{ and } l \geq 2. \]

Like: by \( P(k) \), \( k = p_1 \cdot p_2 \cdots p_i \), \( i < m \).

Then \[ n+1 = k \cdot l = p_1 \cdot p_2 \cdots p_i \cdot q_1 \cdot q_2 \cdots q_j \]

all primes.
Strong induction

To prove \( \forall n \in \mathbb{N}, P(n) \) by strong induction:
- prove \( P(0) \)
- prove \( P(n+1) \), assuming \( P(n), P(n-1), \ldots, P(0) \).

Claim: \( \forall n \geq 2, \ n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \) for some sequence of primes \( p_i \).

i.e., \( n \) can be written as a product of primes.

Proof by induction:

let \( P(n) : = \forall k \leq n \text{ if } k \geq 2. Q(k) \)

\( P(2) \): same as before, only be with \( 2 \leq k \leq 2 \) is 2.

\( P(n+1) \) assuming \( P(n) \): WTS \( \forall k \leq n+1, Q(k) \)

by \( P(n) \) if \( k \leq n \), then we know \( Q(k) \).

So only need to consider \( k = n+1 \). (same as before)
Euclidean division

want to divide $a$ by $b$.

$$\frac{a}{b} = q + \frac{r}{b}$$

avoid using $\frac{a}{b}$ notation.

$a = qb + r$

is the relationship between

num. denon. quotient, remainder

num. quot. den rem.

$0 \leq r < b.$
Euclidean division

Claim: For all $a$ and all $b > 0$, there exists $q$ and $r$ satisfying
1. $a = qb + r$, and
2. $0 \leq r < b$

Proof:

By induction on $a$.

Let $P(a) := \forall b > 0, \exists q, r \text{ s.t. } a = qb + r$.

We'll show $P(0)$ and $P(a+1)$ assuming $P(n)$.

**$P(0)$**

Let $b > 0$, $\exists q, r \text{ s.t. } 0 = qb + r$

$s.t.$ $0 \leq r < b$.

Let $q = r = 0$ then indeed, $0 = qb + r$

$= 0b + 0 = 0 \checkmark$

**$P(a+1)$ assuming $P(n)$**

Know: $\exists q', r'$ with $a = q'b + r'$ \hspace{1cm} (P(n))

Want: $\exists q, r$ with $a + 1 = qb + r$ \hspace{1cm} (P(a+1))