Lecture 14: Strong Induction

- Find & fix bug in proof of existence of prime factors

- New technique: strong induction
  - motivation
  - using str. ind.
  - it's not actually stronger

- Euclidean division

Applications:
- in 2800: lots
- elsewhere: analyzing "divide and conquer" algorithms, which can be much faster than others.
willing to accept proofs \( P(0) \)
\[ P(n) \] assuming \( P(n-1) \).

- Can prove

\[ \forall n \in \mathbb{N}, \text{if } n \geq 3 \text{ then } P(n) \].

\( P(0) \) "vacuously true" because \( 0 \neq 3 \)

\( P(1) \) "vacuously true"

\( P(n) \), assuming \( P(n-1) \).

Choose \( n \in \mathbb{N} \). If \( n < 3 \) then "if \( n \geq 3 \) then \( P(n) \)" is vacuously true.

- If \( n = 3 \)
  - (proof of \( P(3) \), \( P(n-1) \) says nothing)

- If \( n > 3 \)
  - (proof of \( P(n) \), using \( P(n-1) \))
know \( n-1 \) has a prime factorization.

wrg: \( n \) has a prime factorization (case analysis)

1. if \( n \) is prime, then let \( \ell=1 \), let \( a_1=n \).
   then \( a_1 \) is prime, and \( n=a_1 \).

2. if \( n \) is composite (i.e. \( n=x \cdot y \) for some \( x,y \in \mathbb{N} \))

   can't factorize

   \[ x \equiv 1 \pmod{2} \] because we can only factorize \( n-1 \).

\[ P(2): \text{2 is prime } \checkmark \]

\[ P(3): \text{3 is prime } \checkmark \]

\[ P(4): 4 = 2 \cdot 2 \]

\[ P(11): \]

\[ P(12): 12 = 3 \cdot 4 \]
Claim: \( \forall n \geq 2 \exists \text{ primes } (\alpha)_i \text{ with } n = \prod a_i \)

Proof: We'll prove this using strong induction. Let \( P(n) \) be the statement that we will show \( P(2) \), and \( P(n) \) assuming \( P(k) \) holds for \( 2 \leq k < n \).

\( P(2) \): Same as before.

\( P(n) \): Assume \( P(k) \) for \( 2 \leq k < n \).

We show \( P(n) \), i.e., \( n \) has a prime factorization.

- If \( n \) is prime, let \( a_i = n \).
- If \( n \) is composite, \( n = x \cdot y \) for some \( x, y > 2 \). Note \( x < n \) and \( y < n \).
- Otherwise, \( n = x \cdot y > n \).

By \( P(x) \), \( \exists \text{ primes } (\alpha)_i \text{ with } x = \prod a_i \).

By \( P(y) \), \( \exists \text{ primes } (\beta)_i \text{ with } y = \prod b_i \).

Then \( n = x \cdot y = \left( \prod a_i \right) \left( \prod b_i \right) = \prod (\alpha_i \beta_i) \).

Let \( (\alpha)_i \) be \( (\alpha)_i \) followed by \( (\beta)_i \).
WTS: \( \forall n \geq 2, \forall 1 \leq k \leq n, \text{ } k \text{ has a prime factorization} \)

Prove by weak induction. Let \( Q(n) \):

\( Q(2) \): \( \forall 2 \leq k \leq 2, \text{ } k \text{ has prime factorization} \)

prove \( P(2) \)

\( Q(n) \): Assume \( \forall 2 \leq k \leq n-1, \text{ } k \text{ has factorization} \)

WTS \( \forall 2 \leq k \leq n, \text{ } k \text{ has factors} \)

need to show \( n \) has factors
\[
\frac{a}{b} \text{ might not be } \in \mathbb{Z}. \text{ Avoid division!}
\]

like to divide with remainder.

**Claim:** \( \forall a \in \mathbb{N}, b \geq 1, \exists q, r \text{ with } a = qb + r \)

with \( 0 \leq r < b \).

(Euclidean division algorithm)

**Proof:** we WTS \( \forall a \in \mathbb{N}, b \geq 1, \exists q, r \text{ as above} \).

we'll prove this by \textit{pm}. Let \( P(a) = \exists q, r \text{ as above} \).

let \( P(b) = \exists q, r \text{ as above} \).

we WTS \( P(0) \) and \( P(n) \) assuming \( P(n) \).

\( P(0) \): WTS \( \forall b \geq 1, \exists q, r \) with \( 0 = qb + r \) and \( 0 \leq r < b \).

choose \( q = 0 \) \( r = 0 \).

Then \( qb + r = 0b + 0 = 0 = a \).

\( P(a) \): assume \( P(a-1) \).

choose \( q \) \( b \geq 1 \).

then by \( P(a-1) \), \( \exists q', r' \) with \( a-1 = q'b + r' \).

WTS \( \exists q, r \) with \( a = qb + r \) and \( 0 \leq r < b \).

let \( q = q' \) \( r = r' + 1 \)

then \( (a-1)+1 = q'b + r' + 1 \) \( 0 \leq r' < b \)

\[
= qb + r
\]

need \( 0 \leq r < b \)

i.e. \( 0 \leq r' + 1 \).

if \( r' < b-1 \), let \( q = q' \) \( r = r' + 1 \)

\[
\text{ know: } a-1 = q'b + r' \quad r' = b-1
\]

want: \( a = qb + r \)

\[
\text{ try: } a-1 = b-4 \quad \text{ if } r = b-1 \text{ let } q = r = \quad 2
\]

know: \( a-1 = q'b + r' \quad r' = b-1 \)