# Lecture 13: variations on induction

**Claim:** For every $n \in \mathbb{N}$, if $n \geq 2$ then $n$ can be written as a product of primes $n = p_1 \cdot p_2 \cdots p_k$

**Proof attempt:** Let $P(n)$ be the statement "there exists a sequence of one or more primes $p_1, \ldots p_k$ with $n = p_1 \cdot p_2 \cdots p_k$." We will show $P(2)$ and $P(n+1)$ assuming $P(n)$.

To see $P(2)$ (i.e. that we can factor 2), choose $p_1 = 2$; we see that $p_1$ is prime, and $2 = p_1$, so $p_1$ is a prime factorization of 2.

To see $P(n+1)$, assume $P(n)$, $P(n-1)$, $P(n-2)$ ..., $P(2)$ — proof by "strong" induction.

We want to show that $n+1$ can be written as a product of primes. There are two cases. If $n+1$ is prime, then we can choose $p_1 := n+1$, and we are done.

don't know that $k, \ell$ can be factored!

If $n+1$ is not prime, then we know that $n+1 = k \cdot \ell$ for some $k \geq 2$ and $\ell \geq 2$. We write $k = p'_1 \cdot p'_2 \cdots p'_i$ and $\ell = p''_1 \cdot p''_2 \cdots p''_j$ where $p'_1, \ldots, p'_i$ are the prime factors of $k$ and $p''_1, \ldots, p''_j$ are the prime factors of $\ell$. Then $n+1 = p'_1 \cdot p'_2 \cdots p'_i \cdot p''_1 \cdot p''_2 \ldots p''_j$ is a prime factorization of $n+1$, as required.

Since $k \leq n$ and $\ell \leq n$, so we've assumed $P(k)$ and $P(\ell)$.

If I knew $P(k)$ and $P(\ell)$, then ok...

A. Looks good ~~B.~~ Bug in inductive hypothesis ~~C.~~ Bug in base case $\boxed{\text{D.}}$ Bug in inductive step

Strong induction:

to prove $\forall n \in \mathbb{N}, P(n)$,

(1) prove $P(0)$

(2) prove $P(n+1)$, assuming $P(n), P(n-1), \ldots, P(0)$

## Fixing the proof without strong induction

Let $P(n)$ be the statement "there exists a sequence of one or more primes $p_1, \dots p_k$ with $n = p_1 \cdot p_2 \cdots p_k$.".

On the previous slide, we proved

1. $P(2)$
2. $P(n+1)$ assuming $P(n), P(n-1), P(n-2), \dots, P(2)$

$\forall k$ with $2 \le k \le n$

Can we prove $\forall n \geq 2, P(n)$ using only weak induction?

Let $Q(n)$ be the stmt "$\forall k \in [2 \dots n]$, $P(k)$"

i.e. $Q(n)$ is "$P(2)$ and $P(3)$ and ... $P(n)$"

Strengthening the Ind. Hyp.

$Q(2)$: WTS $\forall k \in [2 \dots 2]$, $P(k)$.

well, the only $k \in [2 \dots 2]$ is $k = 2$, we've proved $P(2)$

$Q(n+1)$, assuming $Q(n)$:

WTS $\forall k \in [2 \dots n+1]$, $P(k)$. Choose arb. $k \in [2 \dots n+1]$.

if $k \in [2 \dots n]$, then by $Q(n)$, we know $P(k)$.

the only remaining case is when $k = n+1$,

So we need to show $P(n+1)$.

we've already proved $P(n+1)$ using $P(2) \dots P(n)$,

we know $P(2) \dots P(n)$ by $Q(n)$.

## Variations on induction

Here is the only "induction principle" you need:

- To prove "$\forall n \in \mathbb{N}, P(n)$" by induction:
  [1] prove $P(0)$, and [2] prove $P(n+1)$ assuming $P(n)$, for an arbitrary $n \in \mathbb{N}$

Here are some alternate versions that are often useful:

- To prove "$\forall n \in \mathbb{N}$, $\overbrace{\text{if } n \geq k \text{ then } P(n)}^{Q(n)}$" by induction:
  [1] prove $P(k)$, and [2] prove $P(n+1)$ assuming $P(n)$, for an arbitrary $n \geq k$
- To prove "$\forall n \in \mathbb{N}, P(n)$" by induction:
  [1] prove $P(0)$, and [2] prove $P(n)$ assuming $P(n-1)$, for an arbitrary $n > 0$
  (change of variables let $m = n-1$)
- To prove "$\forall n \in \mathbb{N}, P(n)$" by strong induction:
  [1] prove $P(0)$, and [2] prove $P(n)$ assuming $P(n-1), P(n-2), \ldots, P(0)$

$k > 0$

let $Q(n) =$ "if $n \geq k$ then $P(n)$".

I will prove $Q(0)$ and $Q(n+1)$, assuming $Q(n)$.

$\boxed{Q(0)}$: WTS if $0 \geq k$ then $P(0)$. well $0 \not\geq k$, so this is vacuously true.

$\boxed{Q(n+1) \text{ assuming } Q(n)}$:

WTS if $n+1 \geq k$ then $P(n+1)$.

3 cases: $n+1 < k$, $n+1 = k$ or $n+1 > k$.

if $n+1 < k$, $Q(n+1)$ is vacuously true,

if $n+1 = k$, we have a proof of $P(k)$, so we're done. 1

if $n+1 > k$, then $n \geq k$, so we can use 2

## Euclidean division

For the next few weeks, we'll be interested in the natural numbers and integers (not the rationals or reals). For this reason:

- Avoid writing $\frac{a}{b} = c$

instead: $a = b \cdot c$

so you don't have to check that it is an integer.

$(*)\ \frac{a}{b} = q + \frac{r}{b}$

if $\boxed{a = qb + r}$

and $0 \leq r < b$

then $q$ is a quotient of $a$ over $b$

$r$ is a remainder of $a$ over $b$.

let $quot(a,b)$ is $q$

$rem(a,b)$ is $r$

$\Big\}$ need to justify that quot. & rem. are functions:

need (total): every pair has a quot. & rem.

(unambig.): quotient & remainder are unique

(next time)