Last time:

- Induction: to prove $\forall n \in \mathbb{N}, P(n)$: prove $P(0)$
  and prove $P(n)$ for an arbitrary $n > 0$, assuming $P(n - 1)$.

- Variant: to prove $\forall$ natural numbers $n \geq a, P(n)$: prove $P(a)$
  and prove $P(n)$ for an arbitrary $n > a$, assuming $P(n - 1)$.

- Variant: to prove $\forall n \in \mathbb{N}, P(n)$: prove $P(0)$
  and prove $P(n + 1)$ for an arbitrary $n \geq 0$, assuming $P(n)$.

Claim: $\forall n \geq 2$, there exists $\ell$ and primes $a_1, a_2, \ldots, a_\ell$ with $n = a_1 \cdot a_2 \cdots a_\ell$

Proof so far: let $P(n)$ be the statement “there exists $\ell$ and primes $a_1, a_2, \ldots, a_\ell$ with $n = a_1 \cdot a_2 \cdots a_\ell$.” We will prove $\forall n \geq 2, P(n)$ by induction. We must show $P(2)$ and $P(n)$ assuming $P(n - 1)$.

To see $P(2)$, choose $\ell = 1$ and $a_1 = 2$. Note that $a_1$ is prime and $n = a_1$.

Now, choose an arbitrary $n \geq 2$, and assume $P(n - 1)$; we want to show $P(n)$, i.e. that $n$ has a prime factorization.
Claim: \( \forall n \geq 2, \text{ there exists } \ell \text{ and primes } a_1, a_2, \ldots, a_\ell \text{ with } n = a_1 \cdot a_2 \cdots a_\ell \)

Claim: \( \forall n \geq 2, \text{ there exists } \ell \text{ and primes } a_1, a_2, \ldots, a_\ell \text{ with } n = \prod_i a_i \) (new notn)

Claim: \( \forall n \geq 2, \text{ there exists primes } (a)_i \text{ with } n = \prod_i a_i \) (new notn)

Weak induction: to prove \( \forall n \in \mathbb{N}, P(n) \): prove \( P(0) \) and prove \( P(n) \) for an arbitrary \( n > 0 \), assuming \( P(n-1) \).

Strong induction: to prove \( \forall n \in \mathbb{N}, P(n) \): prove \( P(0) \) and prove \( P(n) \) for an arbitrary \( n > 0 \), assuming \( P(n-1), P(n-2), \ldots, P(0) \).

(equiv) prove \( P(n) \) for an arbitrary \( n > 0 \), assuming \( \forall k < n, P(k) \).

Claim’: \( \forall n \geq 2, \forall k \leq n, \text{ there exists primes } (a)_i \text{ with } k = \prod_i a_i \)

Can prove claim’ by weak induction, same as proving orig. claim by strong

Claim (Euclidean division): For every \( a \in \mathbb{N}, b \geq 1 \) there exists \( q, r \) with \( a = qb + r \) and \( 0 \leq r < b \).

\( q \) is called the quotient, \( r \) is the remainder

Uniqueness proof required to say “the” quotient or remainder