# Lecture 16

Handout or Document Camera or Class Exercise

A statement $P(n)$ is proved true for all $n \in \mathbb{N}$ by induction.

In this proof, for some natural number $k$, we might:

A) Prove $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

B) Assume $P(1)$. Prove $P(k)$. Prove $P(k+1)$.

C) Prove $P(1)$. Assume $P(k)$. Prove $P(k+1)$.

D) Prove $P(1)$. Assume $P(k)$. Assume $P(k+1)$.

E) Assume $P(1)$. Prove $P(k)$. Assume $P(k+1)$.

**Solution:** Prove $P(1)$. Assume $P(k)$. Prove $P(k+1)$.

**Instructor's Comments: This is the 5 minute mark.**

**Instructor's Comments: This is the last induction example - something slightly different.**

Prove that an $m \times n$ chocolate bar consisting of unit squares can be broken into unit squares using

$$mn - 1$$

breaks.

**Instructor's Comments: Mention below that the base case should be formally proven using induction but that we want. It will help to draw pictures as well. This is the first time that an induction question has two variables.**

**Proof:** Let $m \in \mathbb{N}$ be fixed. We proceed by induction on $n$.

**Base Case:** When $n = 1$, we have an $m \times 1$ chocolate bar. This requires $m - 1$ breaks to get $m$ unit squares (can prove formally by induction).

**Inductive hypothesis:** Assume that an $m \times k$ chocolate bar can be broken into unit squares using $mk - 1$ breaks for some $k \in \mathbb{N}$.

**Inductive step:** For an $m \times (k + 1)$ sized chocolate bar, we see that by breaking off the top row, gives a $m \times 1$ sized chocolate bar and a $m \times k$ sized chocolate bar. The first we know can be broken into unit squares using $m - 1$ breaks (this was the base case) and the latter can be broken into unit squares using $mk - 1$ breaks via the induction hypothesis. Hence, the total is

$$1 + m - 1 + mk - 1 = m(k + 1) - 1$$

as required. Hence, the claim is true for all $n \in \mathbb{N}$ by the Principle of Mathematical Induction.

**Instructor's Comments: Again it helps to draw a picture above. We finish induction with the Fundamental Theorem of Arithmetic. Technically we can't prove it now but I will prove it up to Euclid's Lemma. This basically marks the midterm exam line in Fall2015 and Winter 2016.**

**Instructor's Comments: What you might want to do is do the following proof more informally and then return to it at the end of the term after more mathematical maturity has been developed and then redo this proof.**

**Theorem:** (Euclid's Lemma [PAD - Primes and Divisibility]) Suppose $a, b \in \mathbb{Z}$ and $p$ is a prime number. Show that if $p \mid ab$ then $p \mid a$ or $p \mid b$.

**Corollary:** (Generalized Euclid's Lemma) Suppose $a_1, a_2, ..., a_n \in \mathbb{Z}$ and $p$ is a prime number. Show that if $p \mid a_1a_2...a_n$ then $p \mid a_i$ for some integer $1 \leq i \leq n$.

**Note:** The proof of this lemma will be delayed until after we do some techniques through greatest common divisors. For now we will take this for granted and prove our first major theorem of the course. The generalization follows immediately.

**Theorem:** (Fundamental Theorem of Arithmetic) (UFT)

Every integer $n > 1$ can be factored uniquely as a product of prime numbers, up to reordering.

**Note:** Prime numbers are just the product of a single number.

**Proof: Existence.**

Assume towards a contradiction that not every number can be factored into prime numbers. Let $n$ be the smallest such number (which exists by WOP). Then either $n$ is prime, a contradiction, or $n = ab$ with $1 < a, b < n$. However, since $a, b < n$, the numbers $a$ and $b$ can be written as a product of primes (since $n$ was minimal). Thus $n = ab$ is a product of primes, contradicting the definition of $n$.

**Uniqueness**

Assume towards a contradiction that there exists a natural number $n > 1$ such that

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_m$$

where each $p_i$ and $q_j$ are primes (not necessarily distinct) and further assume that this $n$ is minimal (WOP). By definition, $p_1 \mid n = q_1 q_2 ... q_m$. Hence, by the generalized Euclid's Lemma, we see that $p_1 \mid q_j$ for some $1 \leq j \leq m$. Hence, since $p_1$ and $q_j$ are prime numbers, we have that $p_1 = q_j$. Without loss of generality, we may reorder the primes $q_j$ so that $q_j$ is the first prime, that is, $p_1 = q_1$. Canceling out these primes gives

$$N_0 := p_2 ... p_k = q_2 ... q_m$$

Now $N_0 < n$ and so, the above representations must be equal up to reordering by the minimality of $n$. Hence, $k = m$ and we may reorder so that

$$p_\ell = q_\ell \qquad \text{for all } 2 \leq \ell \leq k$$

Multiplying $N_0$ by $p_1$ shows that the two representations of the factorizations of $n$ are the same up to reordering. This contradicts the existence of $n$ hence all numbers can be written uniquely as a product of primes up to reordering of primes.

**Instructor's Comments: This is a difficult proof. I would advise taking some time and really going through it. If you're lucky this will take you to just the 50 minute mark.**