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.

Instructor's Comments: What I'm going to do in the future is do existence here and uniqueness leave as a thought experiment: What are we missing?

Theorem: (Unique Factorization Theorem) (UFT) (Fundamental Theorem of Arithmetic)

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

Instructor's Comments: Cannot do uniqueness yet need Euclid's Lemma. If there's time do the definition of GCD.

Instructor's Comments: Ideally you'll get to the definition today. If not you start with it next time.

Greatest Common Divisors

Instructor's Comments: Arguably, this is the toughest portion of the course. These arguments for gcds are often tricky and counter intuitive and take a bit of practice before mastering.

As an exercise, let's list the divisors of 84:

$$\pm1, \pm2, \pm3, \pm4, \pm6, \pm7, \pm12, \pm14, \pm21, \pm28, \pm42, \pm81$$

Divisors of 120:

$$\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm8, \pm10, \pm12, \pm15, \pm20, \pm24, \pm30, \pm40, \pm60, \pm120$$

Hence the greatest common divisors of 84 and 120 is 12.

Definition: The *greatest common divisors* of integers a and b with $a \neq 0$ or $b \neq 0$ is an integer $d > 0$ such that

(i) $d \mid a$ and $d \mid b$

(ii) If $c \mid a$ and $c \mid b$, then $c \leq d$

We write $d = \gcd(a, b)$.

Note:

(i) $\gcd(a, a) = |a| = \gcd(a, 0)$

(ii) Define $\gcd(0, 0) = 0$. Note that $\gcd(a, b) = 0 \Leftrightarrow a = b = 0$

(iii) **Exercise:** $\gcd(a, b) = \gcd(b, a)$