Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 4

Principle of Mathematical Induction (POMI)

Axiom: If sequence of statements $P(1)$, $P(2)$, ... satisfy

1. $P(1)$ is true
2. For any $k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is true

then $P(n)$ is true for all $n \in \mathbb{N}$.

Domino Analogy

Example

Example: Prove that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

for all $n \in \mathbb{N}$.

Proof: Let $P(n)$ be the statement that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

holds. We prove $P(n)$ is true for all natural numbers n by the Principle of Mathematical Induction.

Base Case

Base case: When $n = 1$, $P(1)$ is the statement that

$$\sum_{i=1}^{1} i^2 = \frac{(1)((1)+1)(2(1)+1)}{6}.$$

This holds since

$$\frac{(1)((1)+1)(2(1)+1)}{6} = \frac{1(2)(3)}{6} = 1 = \sum_{i=1}^{1} i^2.$$

Inductive Hypothesis

Inductive Hypothesis. Assume that $P(k)$ is true for some $k \in \mathbb{N}$. This means that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

Inductive Step

Inductive Step. We now need to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= \sum_{i=1}^{k} i^2 + (k+1)^2 \overset{IH}{=} \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= (k+1)\left(\frac{k(2k+1)}{6} + k + 1\right) = (k+1)\left(\frac{2k^2+k}{6} + \frac{6k+6}{6}\right) \\ &= (k+1)\left(\frac{2k^2+7k+6}{6}\right) = \frac{(k+1)(k+2)(2k+3)}{6}\end{aligned}$$

Hence, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ is true for all natural numbers n by the Principle of Mathematical Induction.

When Induction Isn't Enough

Let $\{x_n\}$ be a sequence defined by $x_1 = 4$, $x_2 = 68$ and

$$x_m = 2x_{m-1} + 15x_{m-2} \qquad \text{for all } m \geq 3$$

Prove that $x_n = 2(-3)^n + 10 \cdot 5^{n-1}$ for $n \geq 1$.

Solution: By Induction. **Base Case:** For $n = 1$, we have

$$x_1 = 4 = 2(-3)^1 + 10 \cdot 5^0 = 2(-3)^n + 10 \cdot 5^{n-1}.$$

Inductive Hypothesis: Assume that

$$x_k = 2(-3)^k + 10 \cdot 5^{k-1}$$

is true for some $k \in \mathbb{N}$.

Inductive Step: Now, for $k + 1$,

$$\begin{aligned} x_{k+1} &= 2x_k + 15x_{k-1} && \text{Only true if } k \geq 2!!! \\ &= 2(2(-3)^k + 10 \cdot 5^{k-1}) + 15x_{k-1} \\ &= 4(-3)^k + 20 \cdot 5^{k-1} + 15x_{k-1} \\ &= ...? \end{aligned}$$

Principle of Strong Induction

Principle of Strong Induction (POSI)

Axiom: If sequence of statements $P(1)$, $P(2)$, ... satisfy

1. $P(1) \wedge P(2) \wedge ... \wedge P(b)$ are true for some $b \in \mathbb{N}$
2. $P(1) \wedge P(2) \wedge ... \wedge P(k)$ are true implies that $P(k+1)$ is true for all $k \in \mathbb{N}$ $(k \geq b)$

then $P(n)$ is true for all $n \in \mathbb{N}$.

For an example check out the other video.

Fibonacci Sequence

Define the Fibonacci Sequence $\{f_n\}$ as follows. Let $f_1 = 1$ and $f_2 = 1$ and

$$f_m = f_{m-1} + f_{m-2}$$

for all $m \geq 3$. This defines the sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...$$

Euclid's Lemma

Theorem 1 (Euclid's Lemma (Primes and Divisibility PAD)).

Let $a, b \in \mathbb{Z}$ and let p be a prime number. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Corollary 2 (Generalized Euclid's Lemma).

Let $a_1, a_2, ..., a_n \in \mathbb{Z}$ and let p be a prime number. If $p \mid a_1 a_2 ... a_n$ then $p \mid a_i$ for some $1 \leq i \leq n$.

Fundamental Theorem of Arithmetic

Theorem 3 (UFT).

Every integers $n > 1$ *can be factored uniquely into a product of primes*

Note: By convention, primes are said to be a single element product.

Fundamental Theorem of Arithmetic - Existence Proof

Assume towards a contradiction that not all numbers can be factored into a product of primes. By the Well Ordering Principle, there is a smallest such number say n. Then, either n is prime (a contradiction) or n is composite and we write $n = ab$ where $1 < a, b < n$. By the minimality of n, both of a and b must be able to be factored as a product of primes. This implies that $n = ab$ can be factored into a product of primes, contradicting the definition of n. Hence every number can be factored into a product of prime numbers.

Fundamental Theorem of Arithmetic - Informal Uniqueness Proof

Suppose that n can be factored in two distinct ways. Say $n = p_1 p_2 ... p_k = q_1 q_2 ... q_m$. Since

$$p_1 \mid p_1 p_2 ... p_k = q_1 q_2 ... q_m$$

by the Generalized Euclid's Lemma (Generalized Primes and Divisibility), we see that $p_1 \mid q_j$ for some j. By reordering if necessary, we may swap q_1 and q_j in the order so that $p_1 \mid q_1$. Hence, we can divide by p_1 to obtain

$$p_2 ... p_k = q_2 ... q_m.$$

Repeating this process shows that all the factors must match.