Existence of Prime Factorization

Prime Factorization

Recap

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

Principle of Complete Mathematical Induction (PCMI)

Let $P(n)$ be any statement about n. Suppose we have proved that

$$P(1) \text{ is true} \tag{1}$$

and that

$$\text{for each } n \in \mathbb{N}, \text{ if } P(1), \ldots, P(n) \text{ are all true, then } P(n+1) \text{ is true.} \tag{2}$$

Then we may conclude that for each natural number n, $P(n)$ is true.

Proof by Complete Induction (Template)

- Declaration: Let $P(n)$ be the sentence
  ....
- BASE CASE: $P(1)$ is true because ....
- INDUCTIVE STEP: Let $n \in \mathbb{N}$ such that $P(1), \dots, P(n)$ are all true.
  [NTS $P(n+1)$ is true.]
- Conclusion: Therefore, by complete induction, for each $n \in \mathbb{N}$, $P(n)$ is true.

$S = \{n_0, n_0+1, n_0+2, \dots\}$

(e.g., if $n_0 = 0$, then $S = \omega$.)

To show $(\forall n \in S)\, P(n)$ using complete induction, modify

$P(1) \to P(n_0)$

$n \in \mathbb{N} \to n \in S$

Example: The Existence of Prime Factorization

Theorem 1 (Existence of Prime Factorization)

Each natural number greater than or equal to $\boxed{2}$ either is a product of prime numbers or is itself a prime number.

- We used this result without proof back in Lecture 10; see Remark 4.44.
- It can now be proved using complete induction.
- It is convenient to start from 2. $S = \{2, 3, 4, \cdots\}$

2 : prime ✓

3 : prime ✓

$4 = 2 \cdot 2$ ✓

5 : prime ✓

$6 = 2 \cdot 3$ ✓

$\vdots$

translate

$(\forall n \in S)\, P(n)$ where $P(n)$ stands for "n is a prime or n is a product of primes"

Before We Begin …

Recall the definition of a prime number.

- To say that x is prime means that

$$(x \in \mathbb{N}) \wedge (x \neq 1) \wedge (\forall a, b \in \mathbb{N})[\, x = ab \Rightarrow a=1 \vee b=1 \,]$$

- (S04E15) x is not a prime number iff

$$(x \notin \mathbb{N}) \vee (x=1) \vee (\exists a, b \in \mathbb{N})[\, x = ab \wedge a \neq 1 \wedge b \neq 1 \,]$$

Proof of Theorem 1

Let $S = \{2, 3, 4, \cdots\}$ and let $P(n)$ be the sentence

<u>n is a prime</u> or <u>n is a product of primes</u>.

We shall show that for each $n \in S$, $P(n)$ is true using <u>complete induction</u>.

<u>BASE CASE</u> $P(2)$ is true because 2 is prime.

<u>INDUCTIVE STEP</u> Let $n \in S$ such that $P(2), \cdots, P(n)$ are all true.

We wish to show that $P(n+1)$ is true. That is, we wish to show that $n+1$ is a prime or $n+1$ is a product of primes.

Now either $\underbrace{n+1 \text{ is a prime}}_{\text{Case 1}}$ or $\underbrace{n+1 \text{ is not a prime}}_{\text{Case 2}}$.

Case 1 Suppose that $n+1$ is prime. Then $P(n+1)$ is clearly true.

Case 2 Suppose that $n+1$ is not prime. Then we can pick $a, b \in \mathbb{N}$ such that $n+1 = ab$ and $a \neq 1$ and $b \neq 1$.

S04E15

Since $a > 1$, $n+1 > b$. Likewise, since $b > 1$, $n+1 > a$.

$n+1 = ab$

$> 1 \cdot b = b$

Thus $a, b \in \{2, \dots, n\}$, so by the inductive hypothesis, $P(a)$ and $P(b)$ are both true. In other words, a is a prime or a is a product of primes, and b is a prime or b is a product of primes. Hence, $n+1 = ab$ must be a product of primes. Thus $P(n+1)$ is true.

Thus in either case, $P(n+1)$ is true.

CONCLUSION Therefore, by complete induction, for each $n \in S$, $P(n)$ is true.

$\square$

In Closing

- What would be a challenge had you attempted to prove using induction?

Example Consider the following sequence defined recursively by

$$a_1 = 1, \quad a_2 = 5,$$

$$a_{n+1} = a_n + 2a_{n-1} \quad \text{for } n \geq 2$$

The general formula: $a_n = 2^n + (-1)^n$ for $n \geq 1$.

Proof Let $P(n)$ be the sentence

$$a_n = 2^n + (-1)^n.$$

WTS: for each $n \in \mathbb{N}$, $P(n)$ is true (using complete induction)

BASE CASES $P(1)$ is true because $a_1 = 2^1 + (-1)^1 = 2 - 1 = 1$.

$P(2)$ is true because $a_2 = 2^2 + (-1)^2 = 4 + 1 = 5$.

INDUCTIVE STEP Let $n \in \mathbb{N}$ with $n \geq 2$ such that $P(1), \ldots, P(n)$ are all true. Note, by the definition, that $a_{n+1} = a_n + 2a_{n-1}$ because $n \geq 2$. Thus, by the inductive hypothesis,

$$\begin{aligned} a_{n+1} &= \left[2^n + (-1)^n\right] + 2\left[2^{n-1} + (-1)^{n-1}\right] \\ &= 2^n + (-1)^n + 2^n + 2(-1)^{n-1} \\ &= 2 \cdot 2^n + (-1)^n \left(1 + 2(-1)^{-1}\right) \\ &= 2^{n+1} + (-1)^n (1-2) \\ &= 2^{n+1} + (-1)^n(-1) = 2^{n+1} + (-1)^{n+1}. \end{aligned}$$

This shows that $P(n+1)$ is true.

CONCLUSION Therefore, by complete induction, for each $n \in \mathbb{N}$, $P(n)$ is true. $\square$