Existence of Prime Factorization

Prime Factorization

Recap

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

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)

$(\forall n \in S)\, P(n)$

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

- Declaration: Let $P(n)$ be the sentence

  ....

- BASE CASE: $P(1)$ is true because ...

  $P(n_0)$

- INDUCTIVE STEP: Let $n \in \mathbb{N}$ such that $P(1), \cdots, P(n)$ are all true.

  (NTS $P(n+1)$ is true.)

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

  $n \in S$

Example: The Existence of Prime Factorization

Theorem 1 (Existence of Prime Factorization)

Each natural number greater than or equal to 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.

$S = \{2, 3, 4, \cdots\}$.

$(\forall n \in S)\ P(n)$ 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

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

$$6 = 2 \cdot 3$$

Proof of Theorem 1

Let $S = \{2, 3, \dots\}$. 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 complete induction.

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

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

We wish to show that $P(n+1)$ is true. In other words, we want 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 $n+1$ is a prime. Then $P(n+1)$ is clearly true.

Case 2: Suppose $n+1$ is not a prime. Then $n+1 = ab$ where $a, b \in \mathbb{N}$, with $a \neq 1$ and $b \neq 1$.

$a > 1$,
$n+1 = ab$
$> 1 \cdot b$
$= b$

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

Then $a, b \in \{2, 3, \ldots, n\}$, so by the inductive hypothesis, $P(a)$ and $P(b)$ are both true.

Thus a is a prime or a product of primes and b is a prime or a product of primes.

Hence $n+1 = ab$ is a product of primes, so $P(n+1)$ 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. In other words, for each natural number $n \geq 2$, n is a prime or a product of primes. $\square$

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

$a_1 = 1$

$a_2 = 5$

$a_3 = 5 + 2 \cdot 1$

$= 7$

$a_4 = 7 + 2 \cdot 5$

$= 17$

$a_5 = 17 + 2 \cdot 7$

$= 31$

$\vdots$

Proof (Complete induction)

Let $P(n)$ be the sentence

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

WTS: For each $n \in \mathbb{N}$, $P(n)$ is true.

BASE CASE

$P(1)$ is true $\quad a_1 = 2^1 + (-1)^1 = 2 - 1 = 1$ and a_1 is defined to be 1.

$P(2)$ is true $\quad a_2 = 2^2 + (-1)^2 = 4 + 1 = 5$ and a_2 is defined to be 5.

INDUCTIVE STEP

Let $n \in \mathbb{N}$ such that $n \geq 2$ and $P(1), \cdots, P(n)$ 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,

$$a_{n+1} = \left[2^n + (-1)^n\right] + 2\left[2^{n-1} + (-1)^{n-1}\right]$$

(Cont' from above)

$$a_{n+1} = \left[2^n + (-1)^n\right] + 2\left[2^{n-1} + (-1)^{n-1}\right]$$

$$= 2^n + (-1)^n + 2^n + 2(-1)^{n-1}$$

$$= 2 \cdot 2^n + (-1)^n\left(1 + 2(-1)^{-1}\right)$$

$$= 2^{n+1} + (-1)^n(1-2)$$

$$= 2^{n+1} + (-1)^n(-1) = 2^{n+1} + (-1)^{n+1}.$$

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

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