Math 300, Lecture 17, Siddhartha Sahi

1 More on induction

1.1 Review of mathematical induction (PMI)

Let $P(n)$ be an open sentence with universe $\mathbb{N}$. Recall that the principle of mathematical induction (PMI) asserts that the following implication

$$P(1) \wedge [\forall k \; P(k) \Rightarrow P(k+1)] \Longrightarrow \forall n P(n)$$

Usually we are interested in proving a theorem of the form $\forall n P(n)$ and we prove this by separately showing $P(1)$ and $\forall k \; P(k) \Rightarrow P(k+1)$.

All proofs by induction look like the following:

Proof. $***$

$\boxed{\text{Therefore } P(1) \text{ is true.}}$

$\boxed{\text{Let } k \text{ be a natural number and suppose } P(k) \text{ is true.}}$

$\circ\circ\circ$

$\boxed{\text{Therefore } P(k+1) \text{ is true.}}$

$\boxed{\text{By PMI, } P(n) \text{ is true for all natural numbers } n.}$ ■

Remark 1 *1. Before starting the proof, you should write down separately the following 4 key sentences: $P(1), P(k), P(k+1), P(n)$. These go into the boxed places in the proof.*

2. The heart of the proof is in the two places marked $***$ and $\circ\circ\circ$. Of these, the $***$ part is usually easy, while the $\circ\circ\circ$ part involves some idea that connects $P(k)$ to $P(k+1)$. Two notes of caution about the $\circ\circ\circ$ part:

(a) You must deduce $P(k+1)$ from $P(k)$ using a correct and complete *argument.*

(b) Do not assume $P(k+1)$ *in $\circ\circ\circ$; you are trying to* prove $P(k+1)$*!*

Here is a proof by induction of a theorem similar to a homework problem.

Theorem 2 *Let $m \in \mathbb{N}$; then for all $n \in \mathbb{N}$, m divides $(m+1)^n - 1$.*

Before starting the proof, we write down the 4 key sentences

$P(1)$	m divides $(m+1)^1 - 1$	$P(k)$	m divides $(m+1)^k - 1$
$P(k+1)$	m divides $(m+1)^{k+1} - 1$	$P(n)$	m divides $(m+1)^n - 1$

Proof. Let m be a natural number, then $(m+1)^1 - 1 = m + 1 - 1 = m$.
$\boxed{\text{Therefore } m \text{ divides } (m+1)^1 - 1.}$
$\boxed{\text{Let } k \text{ be a natural number and suppose that } m \text{ divides } (m+1)^k - 1.}$
Then there exists an integer l such that $(m+1)^k - 1 = lm$.
Therefore $(m+1)^k = lm + 1$, and we get

$$\begin{aligned}(m+1)^{k+1} - 1 &= (m+1)(m+1)^k - 1 = (m+1)(lm+1) - 1 \\ &= lm^2 + lm + m + 1 - 1 = m(lm + l + 1)\end{aligned}$$

Since l, m are integers, $lm + l + 1$ is an integer.
$\boxed{\text{Therefore } m \text{ divides } (m+1)^{k+1} - 1.}$
$\boxed{\text{By PMI } m \text{ divides } (m+1)^n - 1 \text{ for all natural numbers } n.}$ ■

Remark 3 *The boxed sentences are "boiler-plate", i.e. common to all induction proofs. The unboxed parts contain the main ideas. The connection between $P(k)$ and $P(k+1)$ is provided by the arithmetic in the displayed formula.*

1.2 Generalized induction (PGI)

Let $\mathbb{Z}_{\geq l}$ denote the set of integers $\geq l$; thus

$$\mathbb{Z}_{\geq l} = \{x \in \mathbb{Z} \mid x \geq l\} = \{l, l+1, l+2, \cdots\}$$

Let $m = l - 1$, then we have

$$\mathbb{Z}_{\geq l} = \{m+1, m+2, \cdots\} = \{m + n \mid n \in \mathbb{N}\} \tag{1}$$

The principle of generalized induction (PGI) is the following theorem:

Theorem 4 *Suppose $P(n)$ is an open sentence with universe $\mathbb{Z}_{\geq l}$, such that*

1. *$P(l)$ is true*
2. *$\forall k \geq l$ we have $P(k) \Rightarrow P(k+1)$.*

Then $P(n)$ is true for all integers $n \geq l$.

Proof. We leave the proof as an exercise. The main ideas are as follows:

1. Let $m = l - 1$ as in (1) and define a new sentence Q with universe $\mathbb{N}$ as follows
$$Q(n) = P(m+n)$$
2. Prove that $Q(n)$ is true for all $n \in \mathbb{N}$ using PMI.
3. Deduce that $P(n)$ is true for all integers $n \geq l$.

■

1.3 Complete induction (PCI)

The principle of complete induction (PCI) is the following theorem:

Theorem 5 *Suppose $P(n)$ is an open sentence with universe $\mathbb{Z}_{\geq l}$, such that*

1. *$P(l)$ is true*
2. *$\forall k \geq l$ we have $P(l) \wedge P(l+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$.*

Then $P(n)$ is true for all integers $n \geq l$.

Proof. We leave the proof as an exercise. The main idea are as follows:

1. Define a new sentence R with universe $\mathbb{Z}_{\geq l}$ as follows
$$R(n) = P(l) \wedge P(l+1) \wedge \cdots \wedge P(n)$$
2. Prove that $R(n)$ is true for all $n \geq l$ using generalized induction.
3. Deduce that $P(n)$ is true for all integers $n \geq l$.

■

Complete induction is useful when onr cannot easily connect $P(k+1)$ to $P(k)$ alone, but one can relate $P(k+1)$ to $P(j)$ for some other j with $l \leq j \leq k$. Such a situation often arises when one considers questions involving divisibility. As we shall see in the next section.

1.4 Prime factorization

Recall that a natural number n is called a prime if $n \geq 2$ and n is not divisible by any natural numbers other than 1 and n.

Lemma 6 *If $n \geq 2$ and n is not a prime then there are $a, b \in \mathbb{N}$ such that*
$$n = ab, 1 < a < n, 1 < b < n$$

Proof. Let n be a natural number ≥ 2 and suppose n is not a prime. By definition n is divisible by a natural number a that is different from 1 and n. Therefore we can write $n = ab$ for some natural number b. Since a and b divide n we have
$$1 \leq a \leq n, 1 \leq b \leq n \tag{2}$$
By assumption $a \neq 1, n$. Suppose $b = 1$, then since $n = ab$ we get $a = n$, which is a contradiction; therefore we must have $b \neq 1$. Similarly we deduce $b \neq n$. Combining this with (2) we get
$$1 < a < n, 1 < b < n$$
thereby proving the result. ■

For small numbers it is easy to see that we can write them as products of primes. For example
$$2 = 2, 12 = 2.2.3, 25 = 5.5$$

Theorem 7 *Every natural number $n \geq 2$ can be written as a product of primes.*

Proof. Since 2 is a prime number, 2 can be written as product of primes.

Let k be a natural number ≥ 2 and suppose that each of the numbers $2, 3, \cdots, k$ can be written as a product of primes.

We consider two cases for $k+1$. First suppose $k+1$ is prime. Then $k+1$ can be written as a product of primes. Next suppose $k+1$ is not prime, then by the previous lemma, there exist $a, b \in \mathbb{N}$ such that

$$k+1 = ab, 1 < a < k+1,\ 1 < b < k+1$$

Since a and b are integers, they belong to the set $\{2, 3, \cdots, k\}$. By assumption each of a, b can be written as a product of primes. Thus we can write

$$a = p_1 \dots p_r,\ b = q_1 \dots q_s$$

where $p_1, \dots, p_r$ and $q_1, \dots, q_s$ are all prime numbers. Now we have

$$k+1 = ab = p_1 \dots p_r q_1 \dots q_s.$$

Therefore $k+1$ can also be written as a product of primes.

By PCI every natural number $n \geq 2$ can be written as a product of primes.

■

1.5 Exercises

1. Write a *complete and correct* proof of Theorem 4.
2. Write a *complete and correct* proof of Theorem 5.
3. Use PMI to prove that $\frac{1}{2!} + \frac{2}{3!} + \cdots + \frac{n}{(n+1)!} = 1 - \frac{1}{(n+1)!}$ for all $n \in \mathbb{N}$.
4. Use PGI to prove $\left(\frac{2^2-1}{2^2}\right) . \left(\frac{3^2-1}{3^2}\right) \cdots \left(\frac{n^2-1}{n^2}\right) = \frac{n+1}{2n}$ for all $n \geq 2$.