TOURNAMENT OF THE TOWNS, 2003–2004

Induction Notes

Suppose you need to find a general formula for the sum of the first \( n \) natural numbers (and you don’t know anything about arithmetic progressions). You might start by seeing if you can see a pattern:

\[
\begin{align*}
1 &= 1 \\
1 + 2 &= 3 \\
1 + 2 + 3 &= 6 \\
1 + 2 + 3 + 4 &= 10 \\
1 + 2 + 3 + 4 + 5 &= 15.
\end{align*}
\]

If you are lucky you might hit on the fact that:

\[1 + 2 + \cdots + n = \frac{n(n + 1)}{2},\]

but how might you show that this is true, for any natural number \( n \). One way (other than learning about how to sum an arithmetic progression) is to use the Principle of Mathematical Induction. The idea is that you start with some statement that depends on a natural number \( n \). (A statement is something that can be either true or false.) Call this statement \( P(n) \). Then the Principle of Mathematical Induction states:

If we can show that both

- \( P(1) \) is true; and
- for a general natural number \( k \),

\[
\text{if } P(k) \text{ is true then } P(k + 1) \text{ is also true;}
\]

then we can conclude that \( P(n) \) is true for all natural numbers \( n \).

This is exactly like proving that we can climb a ladder, in the following way.

- First we show we can get on the first (bottom) rung.
- Then we show we can get from any one rung (i.e. the \( k \)th rung) to the next rung (i.e. the \( k + 1 \)st rung).

It should be clear that we could then get to any rung of the ladder we like (given enough time ... Oh! I forgot to tell you the ladder has an infinite number of rungs!).

Let us prove our simple example above by induction.
Example. First we define

\[ P(n) : \quad 1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \]

Notice, a ‘:’ was used here – by this we mean that \( P(n) \) is short-hand for everything that follows the ‘:’. Use of a symbol like ‘=’ instead of ‘:’ would have been too confusing!

- Show \( P(1) \) is true;

**Proof.** \( P(1) \) is of the form \( \text{LHS} = \text{RHS} \). To show it is true we start with one side and reduce it to the other side. Now the \( \text{LHS of } P(1) \) is just 1 and the \( \text{RHS of } P(1) \) is \( \frac{1.2}{2} \), i.e.

\[
\text{LHS of } P(1) = 1 = \frac{1.2}{2} = \text{RHS of } P(1)
\]

So \( P(1) \) is true. \( \Box \)

- Show, for a general natural number \( k \),

if \( P(k) \) is true then \( P(k+1) \) is also true;

**Proof.** To prove a statement of form:

If hypothesis then conclusion

we assume the hypothesis and deduce from it, the conclusion. Hence, we assume \( P(k) \) is true, i.e. we assume

\[
\text{LHS of } P(k) = \text{RHS of } P(k).
\]

Now we wish to deduce that \( P(k+1) \) is true. Now \( P(k+1) \) is of the form \( \text{LHS} = \text{RHS} \). So to show it is true we start with one side and reduce it to the other side. (Somewhere along the way we expect to use our assumption that \( P(k) \) is true – incidentally, this assumption is called the inductive assumption). Thus, starting with one side . . .

\[
\text{LHS of } P(k+1) = 1 + 2 + \cdots + k + k + 1
\]

\[
= (\text{LHS of } P(k)) + k + 1
\]

\[
= (\text{RHS of } P(k)) + k + 1, \quad \text{(using the inductive assumption)}
\]

\[
= \frac{k(k+1)}{2} + k + 1
\]

\[
= \frac{k(k+1) + 2(k+1)}{2}
\]

\[
= \frac{(k+1)(k+2)}{2}
\]

\[
= \frac{(k+1)((k+1))}{2}
\]

\[
= \text{RHS of } P(k+1)
\]

So, if \( P(k) \) is true then \( P(k+1) \) is true. \( \Box \)

Thus now we may deduce that, by the Principle of Mathematical Induction, \( P(n) \) is true for all natural numbers \( n \).
An example from Number Theory

You may recall doing the following problems.

Exercise. Prove that for every integer $n$:

(i) $2 | n^2 - n$;
(ii) $3 | n^3 - n$;
(iii) $5 | n^5 - n$.

Solution.

(i) $2$ divides exactly one of the consecutive integers $n - 1, n$ and

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

So $2 | n^2 - n$.

(ii) $3$ divides exactly one of the three consecutive integers $n - 1, n, n + 1$ and

$$n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1).$$

So $3 | n^3 - n$.

(iii) $5$ divides exactly one of the five consecutive integers $n - 2, n - 1, n, n + 1, n + 2$. In terms of congruences, exactly one of $n - 2, n - 1, n, n + 1, n + 2$ is congruent to $0$ modulo $5$. Thus:

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n - 1)(n + 1)(n^2 + 1)$$
$$\equiv n(n - 1)(n + 1)(n^2 - 4) \pmod{5}$$
$$\equiv n(n - 1)(n + 1)(n - 2)(n + 2) \pmod{5}$$
$$\equiv 0 \pmod{5}$$

So $5 | n^5 - n$.

The general result suggested by the above is:

**Theorem (Fermat’s Little Theorem).** If $n$ is a natural number and $p$ is a prime then $p | n^p - n$.

One way of proving Fermat’s Little Theorem (in general) involves the following steps, where $p$ is a prime and $n$ is a natural number. You shouldn’t have too much trouble with the first two steps...they are left as an exercise. The third step requires induction and that, after all, is what this set of notes is about.

1. Show $p$ divides $\binom{p}{r}$ for $1 \leq r \leq p - 1$.
2. Deduce $(n + 1)^p \equiv n^p + 1 \pmod{p}$.
3. Using 2. and induction show $n^p \equiv n \pmod{p}$. 

3
Proof.

- The proposition we are trying to prove is
  \[ P(n) : \quad n^p \equiv n \pmod{p}. \]

- We show \( P(1) \) is true:
  
  Now \( 1^p = 1 \) for any prime \( p \). So
  \[ 1^p \equiv 1 \pmod{p} \]
  i.e. \( P(1) \) is true.

- Now we perform the *inductive* step. We will do this two ways. The first is the “…” way. 

  **Inductive Step (first way):**

  \[
  \begin{align*}
  2^p &= (1 + 1)^p \\
  &\equiv 1^p + 1 \pmod{p} \\
  &\equiv 1 + 1 \pmod{p} \\
  &\equiv 2 \pmod{p}
  \\
  3^p &= (2 + 1)^p \\
  &\equiv 2^p + 1 \pmod{p} \\
  &\equiv 2 + 1 \pmod{p} \\
  &\equiv 3 \pmod{p}
  \\
  &\vdots
  \\
  n^p &= (n - 1 + 1)^p \\
  &\equiv (n - 1)^p + 1 \pmod{p} \\
  &\equiv (n - 1) + 1 \pmod{p} \\
  &\equiv n \pmod{p}
  \end{align*}
  \]

  **Inductive Step (second way):** The second way is more formal and abbreviates the first. We show, for a general natural number \( k \),

  \[ \text{if } P(k) \text{ is true then } P(k + 1) \text{ is also true.} \]

  Hence, we assume \( P(k) \) is true, i.e. we assume
  \[ k^p \equiv k \pmod{p}. \]

  Now we wish to deduce that \( P(k + 1) \) is true. Now \( P(k + 1) \) is of the form LHS = RHS.

  So to show it is true we start with one side and *reduce* it to the other side:

  \[
  \begin{align*}
  (k + 1)^p &\equiv k^p + 1 \pmod{p} \\
  &\equiv k + 1 \pmod{p}, \text{by our assumption that } P(k) \text{ is true.}
  \end{align*}
  \]

  So, if \( P(k) \) is true then \( P(k + 1) \) is true.

  Hence, since \( P(1) \) is true, \( P(n) \) is true for all \( n \in \mathbb{N} \).

\[ \square \]