8

THE PRINCIPLE OF MATHEMATICAL INDUCTION

8.1 The Principle

Recall that we might use the following line of reasoning in the middle of a proof:

$$\vdots$$

We know $P \Rightarrow Q$ (is true).
We know P (is true).
So, we conclude Q (is true).

$$\vdots$$

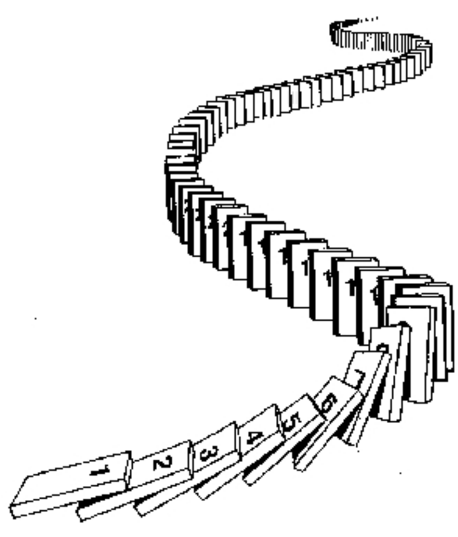
This is because we have adopted the following Rule:

$$\begin{array}{l} P \Rightarrow Q \\ P \\ \hline \therefore\ Q \end{array}$$

This rule was adopted based on our intended meaning of the conditional connective and its associated truth table. So, if $P \Rightarrow Q$ holds and so does P, then Q must hold. (Remember that if P is false, then $P \Rightarrow Q$ is taken as true.)

We are about to adopt another *reasonable* rule based on what seems logical to us.

An Analogy. Suppose we have dominoes which are numbered thus: $1, 2, 3, \cdots$. Suppose all dominoes are sequentially arranged standing on their smallest side.
<u>If</u> we know
(1) domino 1 falls ; and
(2) for all k, the fall of the k^{th} domino will cause the fall of the $k + 1^{st}$,
<u>then</u> we would conclude *all dominoes fall*.



This propels us to adopt the following scheme as a tool for reasoning.

The Stage. $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

The Principle of Mathematical Induction (PMI).
If (1) $P(1)$, and
(2) $\forall k[P(k) \Rightarrow P(k+1)]$,
then $\forall n P(n)$.

Application of PMI.
Suppose $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

Then, if we are in the beginning or middle of a proof and wish to show $\forall n P(n)$, we may unravel the target as follows.

$$\vdots$$

Show $\forall n P(n)$.

(1) Show $P(1)$. (Complete this task.)	(2) Show $\forall k[P(k) \Rightarrow P(k+1)]$. Imagine arbitrary k. Show $P(k) \Rightarrow P(k+1)$. Assume $P(k)$. $(*)$ (Call this 'the star witness.') Show $P(k+1)$. (Complete this task.)

After having completed both tasks, we would reason that since we have shown the required conditional clauses of PMI, we may appeal to the principle (PMI) and conclude: Hence we have shown $\forall n P(n)$ is true.

In this process, task (1) is generally straight forward to establish. To complete task (2), we use the assumption of

$P(k)$ and any other known relevant facts (in the Bank) to demonstrate that $P(k+1)$ holds.

We should note that while our universe is $\mathbb{N}^+$, PMI is clearly applicable if the universe is $\mathbb{N}$ (it includes 0), or is $\{3, 4, \cdots\}$, for example. In the last two cases, we would simply adjust the first clause of PMI to be $P(0)$ or $P(3)$, respectively. Also, often we might encounter *fractions* of natural numbers in our open sentences. In such cases, we should imagine that both sides of equalities or inequalities can be multiplied by the denominators to yield assertions entirely about the universe $\mathbb{N}^+$ (or the others described above). Furthermore, if we are in a universe larger than $\mathbb{N}^+$, where a particular variable of a closed sentence is ranging over $\mathbb{N}^+$, we may apply PMI to that particular variable.

Example 8.1. Recall that we proved, for the universe $\mathbb{R}$, $\forall a \forall b(0 < a < b \Rightarrow a^2 < b^2)$. We then used that to prove $\forall a \forall b(0 < a < b \Rightarrow a^3 < b^3)$. Which in turn was useable to prove
$\forall a \forall b(0 < a < b \Rightarrow a^4 < b^4)$ ...

It is natural then to imagine that we could prove $\forall a \forall b(0 < a < b \Rightarrow a^{341} < b^{341})$. But it also would seem that we need to establish a similar result with 341 replaced by 340, which in turn suggests that we need a similar result for 339, and so on.

But what if we employed PMI?

Claim 8.2. $\forall a \forall b[0 < a < b \Rightarrow (\forall n \in \mathbb{N}^+)(a^n < b^n)]$.

Proof. Show $\forall a \forall b[0 < a < b \Rightarrow (\forall n \in \mathbb{N}^+)(a^n < b^n)]$.
Imagine arbitrary a and b(in $\mathbb{R}$).
Assume $0 < a < b$. $\quad (*)$
Show $(\forall n \in \mathbb{N}^+)(a^n < b^n)$.

At this stage, we will use PMI.
(1) Show $a^1 < b^1$.
But this is given.
(2) Show $\forall k \in \mathbb{N}^+[(a^k < b^k) \Rightarrow (a^{k+1} < b^{k+1})]$.
Imagine arbitrary $k \in \mathbb{N}^+$.
Show $(a^k < b^k) \Rightarrow (a^{k+1} < b^{k+1})$.
Assume $a^k < b^k$. $\qquad (**)$
Show $a^{k+1} < b^{k+1}$.
But then $(*)$, $(**)$ and Theorem 7.38 give $a^{k+1} < b^{k+1}$.

So (1), (2) and PMI yield $(\forall n \in \mathbb{N}^+)(a^n < b^n)$. $\square$

Example 8.3. Suppose $U = \mathbb{N}^+$. Note that
$1 = 1 + \frac{1(1+1)}{2}$,
$1 + 2 = 3 = \frac{2(2+1)}{2}$,
$1 + 2 + 3 = 6 = \frac{3(3+1)}{2}$,
$1 + 2 + 3 + 4 = 10 = \frac{4(4+1)}{2}$,
$\vdots$
Thus we might be tempted to suspect that, for any n,
$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Claim 8.4. $\forall n[1 + 2 + \cdots + n = \frac{n(n+1)}{2}]$.

Proof. Show $\forall n[1 + 2 + \cdots + n = \frac{n(n+1)}{2}]$.
We will use PMI.
(1) Show $1 = \frac{1(1+1)}{2}$.
Show $1 = \frac{2}{2}$.
Show $1 = 1$. This is verifiable in $\mathbb{N}^+$.
(2) Show
$\forall k[1 + 2 + \cdots + k = \frac{k(k+1)}{2} \implies 1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+1+1)}{2}]$.
Imagine arbitrary k.

Assume $1 + 2 + \cdots + k = \frac{k(k+1)}{2} \qquad (*)$.
Show $1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}$.
Note

$$\begin{aligned}
1 + 2 + 3 + \cdots + (k+1) &= [1 + 2 + 3 + \cdots + k] + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \qquad \text{(By } (*)\text{.)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}.
\end{aligned}$$

So (1) , (2) and PMI give us

$$\forall n[1 + 2 + \cdots + n = \frac{n(n+1)}{2}].$$

□

Example 8.5. Suppose $U = \mathbb{N}^+$. Note that
$1^2 = 1 = \frac{1(1+1)(2(1)+1)}{6}$
$1^2 + 2^2 = 5 = \frac{2(2+1)(2(2)+1)}{6}$
$1^2 + 2^2 + 3^2 = 14 = \frac{3(3+1)(2(3)+1)}{6}$
$\vdots$
Thus we might be tempted to suspect that, for any n,
$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Claim 8.6. $\forall n[1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}]$

Proof. Show $\forall n[1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}]$.
We will use PMI.
(1) Show $1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$.
Show $1 = \frac{1\cdot 2\cdot 3}{6}$. Show $1 = 1$. This is clearly true.
(2) Show $\forall k[1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6} \Rightarrow$
$1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+2)+(2k+3)}{6}]$.
Imagine arbitrary k.
Assume $1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$. $\quad (*)$
Show $1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$.
Note

$$
\begin{aligned}
1^2 + 2^2 + ... + (k+1)^2 &= [1^2 + 2^2 + \cdots + k^2] + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \text{ by } (*) \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}.
\end{aligned}
$$

Thus, by PMI, $\forall n[1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}]$. □

Claim 8.7. $\forall n(1^3 + \cdots + n^3 = [\frac{n(n+1)}{2}]^2)$.

Proof. Show $\forall n(1^3 + \cdots n^3 = \left[\frac{n(n+1)}{2}\right]^2)$. We will use PMI,
(1) Show $1^3 = \left[\frac{1(1+1)}{2}\right]^2$. Show $1 = (\frac{1(2)}{2})^2$. Show $1 = 1^2$.
This is directly verifiable.
(2) Show

$$\forall k\big(1^3 + \cdots + k^3 = \left[\frac{k(k+1)}{2}\right]^2 \implies 1^3 + \cdots + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2}\right]^2\big).$$

Imagine arbitrary k. Assume $1^3 + \cdots + k^3 = \left[\frac{k(k+1)}{2}\right]^2$ $(*)$.
Show $1^3 + \cdots + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2}\right]^2$.

Note: $1^3 + \cdots + (k+1)^3 = 1^3 + \cdots + k^3 + (k+1)^3$

$$= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \quad \text{by } (*).$$

$$= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}.$$

$$= \frac{(k+1)^2(k^2 + 4k + 4)}{4}.$$

$$= \left[\frac{(k+1)(k+2)}{2}\right]^2.$$

So, by PMI, $\forall n(1^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2)$. □

Claim 8.8.
$\forall n[1^2 + 4^2 + 7^2 + \cdots + (3n-2)^2 = \frac{1}{2}n(6n^2 - 3n - 1)]$.

Proof. Show
$\forall n[1^2 + 4^2 + 7^2 + \cdots + (3n-2)^2 = \frac{1}{2}n(6n^2 - 3n - 1)]$.
We will use PMI.
(1) Show $(3(1) - 2)^2 = \frac{1}{2}(1)(6(1)^2 - 3(1) - 1)$.
Show $1^2 = \frac{2}{2}$. But this is true by simple verification in the universe.
(2) Show $\forall k[(1^2+4^2+\cdots+(3k-2)^2 = \frac{1}{2}k(6k^2-3k-1)) \implies (1^2 + 4^2 + \cdots + (3(k+1)-2)^2 = \frac{1}{2}(k+1)(6(k+1)^2 - 3(k+1) - 1))]$.
Imagine arbitrary k.
Assume $1^2 + 4^2 + \cdots + (3k-2)^2 = \frac{1}{2}k(6k^2 - 3k - 1)$. $\quad (*)$
Show $1^2 + 4^2 + \cdots + (3(k+1)-2)^2 = \frac{1}{2}(k+1)(6(k+1)^2 - 3(k+1) - 1)$.

We now demonstrate the desired equality:
$1^2 + \cdots + (3(k+1)-2)^2$

$$= 1^2 + \cdots + (3k-2)^2 + (3(k+1)-2)^2$$

$$= [1^2 + \cdots + (3k-2)^2] + (3k+3-2)^2$$

$$= \frac{1}{2}k(6k^2 - 3k - 1) + (3k+1)^2 \quad \text{by } (*)$$

$$= \frac{1}{2}[k(6k^2 - 3k - 1) + 2(3k+1)^2]$$

$$= \frac{1}{2}[6k^3 - 3k^2 - k + 18k^2 + 12k + 2]$$

$$= \frac{1}{2}[6k^3 + 15k^2 + 11k + 2]$$

$$= \frac{1}{2}[(6k^3 + 9k^2 + 2k) + (6k^2 + 9k + 2)]$$

$$= \frac{1}{2}[k(6k^2 + 9k + 2) + (6k^2 + 9k + 2)]$$

$$= \frac{1}{2}[(k + 1)(6k^2 + 9k + 2)]$$

$$= \frac{1}{2}[(k + 1)(6k^2 + 12k + 6 - 3k - 3 - 1)]$$

$$= \frac{1}{2}(k + 1)(6(k + 1)^2 - 3(k + 1) - 1).$$

So, by PMI:

$$\forall n[1^2 + \cdots + (3n-2)^2 = \tfrac{1}{2}n(6n^2-3n-1)]. \quad \square$$

Arithmetic and geometric progressions

Recall that a sequences such as $2, 5, 8, 11, \cdots$ and $1, 2, 4, 8, \cdots$ are *progressions*. We use PMI to find the sum of a desired number of terms of a progression.

Definition 8.9. A sequence of numbers of the form $a, (a + d), (a + 2d), (a + 3d), , (a + 4d) \cdots$, where a and d are in $\mathbb{R}$, is an *arithmetic progression*.

A sequence of numbers of the form $a, ar, ar^2, ar^3, , ar^4 \cdots$, where a and r are in $\mathbb{R}$, is a *geometric progression*.

The next theorem establishes a formula when we add the first $n+1$ terms of an arithmetic progression.

Theorem 8.10.
$\forall a \forall d \forall n \big[a+(a+d)+(a+2d)+\cdots+(a+nd) = \frac{n+1}{2}(2a+nd)\big]$.

Proof. Show
$\forall a \forall d \forall n \big[a+(a+d)+\cdots+(a+nd) = \frac{n+1}{2}(2a+nd)\big]$.
Imagine arbitrary a and d.
Show $\forall n \big[a+(a+d)+\cdots+(a+nd) = \frac{n+1}{2}(2a+nd)\big]$.
We will use PMI (on n).
(1) Show $a+(a+d) = \frac{1+1}{2}(2a+d)$.
Show $2a+d = 2a+d$.
This is clearly true.
(2) Show $\forall k[a+(a+d)+\cdots+(a+kd) = \frac{k+1}{2}(2a+kd) \Rightarrow a+(a+d)+\cdots+(a+(k+1)d) = \frac{(k+1)+1}{2}(2a+(k+1)d)]$.
Imagine arbitrary k.
Assume $a+(a+d)+\cdots+(a+kd) = \frac{k+1}{2}(2a+kd)$. $(*)$
Show $a+(a+d)+\cdots+(a+(k+1)d) = \frac{(k+1)+1}{2}(2a+(k+1)d)$.

Note: $a+(a+d)+\cdots+(a+(k+1)d)$

$$= a+(a+d)+\cdots+(a+kd)+(a+(k+1)d)$$

$$= \frac{k+1}{2}(2a+kd)+(a+(k+1)d) \quad \text{by } (*)$$

$$= \frac{k+1}{2}(2a+kd)+\frac{2a+2(k+1)d}{2}$$

$$= \frac{k+1}{2}(2a+kd)+\frac{(k+1)d}{2}+\frac{2a+(k+1)d}{2}$$

$$= \Big[\frac{k+1}{2}(2a+kd) + \frac{(k+1)d}{2}\Big] + \frac{2a+(k+1)d}{2}$$

$$= \frac{k+1}{2}(2a+kd+d) + \frac{2a+(k+1)d}{2}$$

$$= \frac{k+1}{2}(2a+(k+1)d) + \frac{1}{2}(2a+(k+1)d)$$

$$= \frac{k+2}{2}(2a+(k+1)d)$$

So (1), (2) and PMI establish
$\forall n\big[a+(a+d)+\cdots+(a+nd) = \frac{n+1}{2}(2a+nd)\big]$. □

The next theorem establishes a formula when we add the first $n+1$ terms of a geometric progression.

Theorem 8.11. *Let* $r \neq 1$. $\forall n[1+r+\cdots+r^n = \frac{1-r^{n+1}}{1-r}]$.

Proof. Assume $r \neq 1$.
Show $\forall n[1+r+r^2+\cdots+r^n = \frac{1-r^{n+1}}{1-r}]$.
We will use PMI (on the variable n).

(1) Show $1+r = \frac{1-r^2}{1-r}$.
Show $1+r = \frac{(1-r)(1+r)}{1-r}$.
Show $1+r = 1+r$.
This is true.

(2) Show $\forall k[(1+r+\cdots+r^k = \frac{1-r^{k+1}}{1-r}) \Rightarrow$
$(1+r+\cdots+r^{(k+1)} = \frac{1-r^{(k+1)+1}}{1-r})]$.
Imagine arbitrary k.

Assume $1 + r + \cdots + r^k = \frac{1-r^{k+1}}{1-r}$. $(*)$
Show $1 + r + r^2 + \cdots + r^{(k+1)} = \frac{1-r^{(k+1)+1}}{1-r}$.

Note: $1 + r + \cdots + r^{(k+1)} = 1 + r + r^2 + \cdots + r^k + r^{(k+1)}$

$$= \frac{1 - r^{k+1}}{1 - r} + r^{(k+1)} \quad \text{by } (*)$$

$$= \frac{1 - r^{k+1} + (1-r)r^{(k+1)}}{1 - r}$$

$$= \frac{1 - r^{k+1} + r^{(k+1)} - r^{(k+1)+1}}{1 - r}$$

$$= \frac{1 - r^{(k+1)+1}}{1 - r}.$$

So (1), (2) and PMI establish
$\forall n[1 + r + r^2 + \cdots + r^n = \frac{1-r^{n+1}}{1-r}]$. $\square$

8.2 A Slight Variation of PMI

It should be clear that the following variation (improvement) of PMI is also valid.

The Stage. $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

The Principle of Mathematical Induction (PMI).

Let j_0 be a fixed element of $\mathbb{N}^+$ (so j_0 could be 1 or bigger).

If (1) $P(j_0)$, and

(2) $\forall k[P(k) \Rightarrow P(k+1)]$,

then $\forall n[n \geq j_0 \Rightarrow P(n)]$.

This asserts that if some property holds for a number j_0, and whenever it holds for a number k, it also holds for $k+1$, then it holds for *all numbers bigger than or equal to* j_0.

Hence an application of this version of PMI would be the following.

Application of PMI.

Suppose $U = \mathbb{N}^+$, $P(n)$: an open sentence about n, and $j_0 \in \mathbb{N}^+$.

Then, if we are in the beginning or middle of a proof, have identified j_0, and wish to show $\forall n[n \geq j_0 \Rightarrow P(n)]$, we may unravel the target as follows.

$\vdots$

Show $\forall n[n \geq j_0 \Rightarrow P(n)]$.

(1) Show $P(j_0)$. (Complete this task.)	(2) Show $\forall k[P(k) \Rightarrow P(k+1)]$. Imagine arbitrary k. Show $P(k) \Rightarrow P(k+1)$. Assume $P(k)$. $(*)$ (Call this assumption 'the star witness.') Show $P(k+1)$. (Complete this task.)

After having completed both tasks, we would reason that since we have shown the required conditional clauses of PMI, we may appeal to the principle (PMI) and conclude: Hence we have shown $\forall n[n \geq j_0 \Rightarrow P(n)]$ is true.

Example 8.12. Notice that $\forall n[3^n > 5n]$ is false when $n = 1$ and $n = 2$, but it seems to hold for $n = 3, 4, \cdots$.
So, we **Claim:** $\forall n[n \geq 3 \Rightarrow 3^n > 5n]$, and see if we can prove it.

Proof. Show $\forall n[n \geq 3 \Rightarrow 3^n > 5n]$.
We will use PMI.
(1) Show $3^3 > 5 \cdot 3$.
Show $27 > 15$.
This is clear.
(2) Show $\forall[3^k > 5k \Rightarrow 3^{k+1} > 5(k+1)]$.
Assume $3^k > 5k$. $(*)$
Show $3^{k+1} > 5(k+1)$.
Note:

$$\begin{aligned}
3^{k+1} &= 3 \cdot 3^k \\
&> 3 \cdot 5k \qquad [\text{by } (*)] \\
&= 1 \cdot 5k + 2 \cdot 5k = 5k + 10k \\
&\geq 5k + 10 \\
&> 5k + 5 \\
&= 5(k+1).
\end{aligned}$$

So (1), (2), and PMI establish $\forall n[n > 2 \Rightarrow 3^n > 5n]$. $\square$

Exercises 8.2

1. Show $\forall n[1 + 3 + 5 + \cdots + 2n - 1 = n^2]$.

2. Show $\forall n[1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)]$.

3. Show $\forall n[1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2]$.

4. Show
   $\forall n[1^2 + 4^2 + 7^2 + \cdots + (3n-2)^2 = \frac{1}{2}n(6n^2 - 3n - 1)]$.

5. Show
   $\forall n[2^2 + 5^2 + 8^2 + \cdots + (3n-1)^2 = \frac{1}{2}n(6n^2 + 3n - 1)]$.

6. Show $\forall n(3^n > 2^n)$.

7. Show $\forall n(2^n > n)$.

8. Show $\forall n(2^n \geq 2n)$.

9. True or false: $\forall n(2^n > 2n + 1)$?
   (True in a smaller universe than $\mathbb{N}^+$?)

10. Show the sentence $\forall n(2^n > n^2)$ is false.

11. Show $\forall n(2^n > n^2)$.
    (In a smaller universe than $\mathbb{N}^+$.)

12. True or false: $\forall n(2^n > n^3)$?
    (True in a smaller universe than $\mathbb{N}^+$?)

13. Show $\forall n(2^n \leq (n+1)!)$.

14. Show $\forall n[(n \geq 5) \Rightarrow (2^n > n^2)]$.

15. Show $\forall n(3^n \geq 3n)$.

16. Show $\forall n(3^n > n^2)$.

17. Show $\forall n(3^n > n^3)$.

18. Show $\forall n(3|2^{2n-1} + 1)$.

19. Show $\forall n(3|4^n - 1)$.

20. Show $\forall n(4|5^n - 1)$.

21. Show $\forall j[\forall n(j|(j+1)^n - 1)]$.

22. Show $\forall n(6|n^3 - n)$.

23. Show $\forall n(4 \mid 3^{2n-1} + 1)$.

24. Recall $e > 2$. Show $\forall n(e^n > n)$.

25. Show $\forall n[\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}]$.

26. Show $\forall n[\frac{1}{(n+1)^2} < \frac{1}{n(n+1)}]$.
(For this problem, you do not need to use induction.)

27. Show $\forall n[\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < 2]$.
(Hint: Use Problems 25 and 26 above.)

28. Show $\forall n(8 \mid n^5 - n^3)$. (Challenging.)

8.3 On the Notation $\sum$ and $\prod$

We should recall that using the notations $\sum$ and $\prod$ is most expedient.

Notation. For a sequence of numbers, $c_1, c_2, \cdots, c_n \cdots$, we use:

$$\sum_{j=1}^{k} c_j = c_1 + c_2 + \cdots + c_k$$

$$\prod_{j=1}^{k} c_j = c_1 c_2 \cdots c_k$$

Exercises 8.3

1. Let $U = \mathbb{N}$. (n must be in $\mathbb{N}$; a and b are in $\mathbb{R}$.) Show $\forall a \forall b \forall n [a^{n+1} - b^{n+1} = (a-b) \sum_{j=0}^{n} a^{(n-j)} b^j]$.

2. Let $U = \mathbb{N}$. (n must be in $\mathbb{N}$; a and b are in $\mathbb{R}$.) Show $\forall a \forall b \forall n [a^{n+1} + b^{n+1} = (a+b) \sum_{j=0}^{n} (-1)^j a^{(n-j)} b^j]$.

3. Find a formula for $\prod_{j=1}^{n} e^j$.

4. Rewrite the proof of Theorem 8.10 using the $\sum$ notation.

5. Rewrite the proof of Theorem 8.11 using the $\sum$ notation.

8.4 The Principle of Strong Mathematical Induction

Recall that PMI allows us to establish the truth of $\forall n P(n)$, where $P(n)$ is an open sentence about n and the universe is $\mathbb{N}^+$, by establishing $P(1)$ and by proving $P(k) \implies P(k+1)$. The second step, the inductive step, should be seen as the truth of $P(k)$, alone, leading to the truth of $P(k+1)$.

It is the case that in many situations, not only we need the truth of $P(k)$ but also the truth of $P(k-1)$, $P(k-2)$, $P(k-3)$, *possibly* all the way to the truth of $P(1)$ to establish the truth of $P(k+1)$.

So it seems that we need a 'stronger' principle to step in and help. Such a principle is indeed possible to formulate and is actually equivalent to PMI. Hence if we adopt PMI because it is intuitively convincing, we get the new principle for free.

In this section, we state the new principle and defer showing its equivalence to PMI to a future section.

The Stage. $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

The Principle of Strong Mathematical Induction (PSMI).
If
(1) $P(1)$, and
(2) $\forall k[P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \wedge P(k) \implies P(k+1)]$,
then $\forall n P(n)$.

Application of PSMI.

Suppose $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

Then, if we are in the middle of a proof and wish to show $\forall n P(n)$, we may unravel the target as follows.

$$\vdots$$

Show $\forall n P(n)$.

(1) Show $P(1)$. (Complete this task.)	(2) Show $\forall k[P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \wedge P(k) \implies P(k+1)]$. Imagine arbitrary k. Show $P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \wedge P(k) \implies P(k+1)$. Assume $P(1) \wedge \cdots \wedge P(k-1) \wedge P(k)$. $(*)$ (Call this 'the star witnesses.') Show $P(k+1)$. (Complete this task.)

After having completed both tasks, we would reason that since we have shown the required conditional clauses of PSMI, we may appeal to the principle (PSMI) and conclude: Hence we have shown $\forall n P(n)$ is true.

Exercises 8.4

1. Let $U = \mathbb{N}^+$. Show that, for all n, $7^n - 2^n$ is divisible by 5.

2. Let $U = \mathbb{N}^+$. Let $a_1 = 3$ and $a_{n+1} = 2\sum_{i=1}^{n} a_i + 3$, for each n.
   Show $\forall n(a_n = 3^n)$.

3. For $U = \mathbb{N}^+$, let a sequence $a_1, a_2, a_3, \ldots$ be defined as follows:
   $a_1 = 3$, and from then on by $a_{n+1} = a_n(a_n+2)$. First, calculate a_3, a_4 and a_5.

   Find a formula for the n^{th} term of this sequence and prove your claim.

4. For$U = \mathbb{N}^+$, let a sequence $a_1, a_2, a_3, \ldots$ be defined as follows:
   $a_1 = 3$, $a_2 = 9$, and from then on by $a_{n+2} = 5a_{n+1} - 6a_n$. First, calculate a_3, a_4 and a_5.

   Find a formula for the n^{th} term of this sequence and prove your claim.

5. For $U = \mathbb{N}^+$, let a sequence $a_1, a_2, a_3, \ldots$ be defined as follows:
   $a_1 = 4$, $a_2 = 24$, and from then on by $a_{n+1} = 6a_n - 5a_{n-1}$. First, calculate a_3, a_4 and a_5.

   Find a formula for the n^{th} term of this sequence and prove your claim.

8.5 The Principle of Existence of the Least Natural Number

In Chapter 5, we reasoned that if we consider all natural numbers with a certain property where there is one or more such numbers, then there is the least such number holding that property. Here we describe that and its application more formally, and in the next section we show that it is equivalent to PMI.

The Stage. $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

The Principle of Existence of the Least Natural Number – or – The Well Ordering Principle (WOP[1]). If $\forall n P(n)$ is false, which means $P(n)$ is false for at least one $n \in \mathbb{N}^+$, then there is ℓ such that $P(\ell)$ is false and $P(x)$ is true for all x with $x < \ell$, if any $x < \ell$ (as ℓ could be equal to 1).

Formally, we can write WOP as

$$\neg\forall n P(n) \Rightarrow \big[\neg P(1) \vee \exists \ell [P(1) \wedge \cdots \wedge P(\ell - 1) \wedge \neg P(\ell)]\big]$$

Application of WOP.

Suppose $U = \mathbb{N}^+$, $P(n)$: an open sentence about n.

Then, if we are in the beginning or middle of a proof and wish to show $\forall n P(n)$, we may try to show this indirectly.

$$\vdots$$

Show $\forall n P(n)$.

!! Presume $\neg\forall n P(n)$.

Applying WOP to this, we conclude

[1] We will use WOP to refer to the principle as it is better known under that name.

$\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$.
That is, there is a least number for which $P(\ell)$ is false.
Next we would work to show that indeed
'$P(1)$ is true', and
'the least $\ell > 1$ exists with $P(\ell)$ false'
lead to
'$P(\ell')$ for some $\ell' < \ell$ is false'.
That is a contradiction !!
Thus $\forall n P(n)$ is never false. Thus $\forall n P(n)$ is true.

The similarity of this principle to PMI should be clear.

An example follows.

Claim 8.13. *Let the universe be $\mathbb{N}$ (which includes 0).*
$\forall n[n \geq 8 \Rightarrow \exists a \exists b(n = 3a + 5b)]$.

Proof. Show $\forall n[n \geq 8 \Rightarrow \exists a \exists b(n = 3a + 5b)]$.
We will use WOP in an indirect proof.
!! Presume $\neg \forall n[n \geq 8 \Rightarrow \exists a \exists b(n = 3a + 5b)]$.
So, for some least $\ell \geq 8$, $\ell \neq 3a + 5b$, for any a and b $\quad(*)$.
Note that $9 = 3(3) + 5(0)$ and $10 = 3(0) + 5(2)$, thus ℓ has to be larger or equal to 11.
But then $\ell - 3$, which is bigger than or equal to 8 and less than ℓ cannot be written as $3x + 5y$ for any x and y because if $\ell - 3 = 3x + 5y$, then $\ell = 3(x+1) + 5y$, contrary to our $(*)$ statement.
This contradicts the choice of ℓ (which was assumed to be *the least* such number). !!
So our presumption was wrong and we are done. (Notice that this proof contains a proof by contradiction within a proof by contradiction!)

$\square$

Next, we prove a needed fact and a theorem introduced as an axiom in Chapter 4 and give its proof.

Theorem 8.14. *For any p, a, and b, if p is a prime and p divides ab, then either p divides a or p divides b.*

Proof. !! Presume our assertion is false. So there are p (a prime), a and b such that $p \mid ab$ but $p \nmid a$ and $p \nmid b$. Using WOP, let a be the least such number and b be the least such number for the prime p.

Since $p \mid ab$, we have $pm = ab$ for some m. Now we must have p smaller than either a or b. Without loss of generality, let's assume $p < a$; then it follows that $b < m$. So $a - p > 0$ and $m - b > 0$. Also note that as $p \nmid a$, we have $p \nmid (a - p)$.

Next, using $pm = ab$, we get $pm - pb = ab - pb$. This gives $p(m - b) = b(a - p)$. This last equation offers the following:
The prime p divides the product of $a - p$ and b but p does not divide either $a - p$ or b.

Comparing this with our choice of a and b, we have a contradiction as $a - p < a$. !!

So our presumption is false and we have our theorem.

□

Theorem 8.15. ***The Fundamental Theorem of Arithmetic.*** *For any $n \in \mathbb{N}^+$, $n > 1$,*
(1) a prime factorization of n ***exists****; and*
(2) that prime factorization is ***unique****.*

Proof. We prove (1) by using PSMI.
(1.1) Note that $n = 2$ is expressed as a product of primes.
(1.2) Assume that for any n with $2 \leq n \leq k$, n may be written as a product of primes. $\quad (*)$
We are now to show that $k+1$ may be written as a product of primes.

There are two cases. If $k+1$ is a prime, we are done. If $k+1$ is a composite, then $k+1 = ij$ with $i, j < k+1$. Hence, by our induction hypothesis $(*)$, each i and j may be written as product of primes. So $k+1$ is the product of those two products and we are done.

So (1.1), (1.2) and PSMI yield our claim (1).

We prove (2) by using WOP.

!! Presume the assertion of interest, (2), is false.

Then there is one or more n such that each has at least two distinct prime factorization. By WOP, choose the least such n.

Of course that n cannot be a prime and is a composite. So we have $n = ps$ and $n = qt$, two factorizations of n, where we make sure p is a prime in the $n = ps$ factorization and q is a prime in the $n = qt$ factorization. (Also s and t are the rest of each factorization, each possibly the product of a bunch of primes). As n is the least such number, p and q are different primes and p and q do not appear in t and s, respectively. (Otherwise we would have divided n by one that appears in both sides to get a smaller counterexample to the assertion in the theorem. Note that we are trying to prove it is impossible for a prime to 'appear' in one factorization and therefore divide the other factorization but 'not appear' in the second factorization.)

As prime p divides n, p divides qt but p does not divide q. So by Theorem 8.14, p divides t; so $t = pr$ for some r.

Hence we have $n = ps = qpr$. But this equation yields $s = qr$. Since s does not have a copy of q, we have two distinct factorizations of s. As $s < n$, we have a contradiction to the choice of n. !!

So our presumption is false and we have our theorem.

$\square$

Exercises 8.5

1. Show any integer is either even or odd.
2. Show that, for any $n \in \mathbb{N}^+$, the sum of n even integers is an even integer.
3. Show that, for any $n \in \mathbb{N}^+$, the sum of $2n$ odd integers is an even integer.
4. Show that, for any $n \in \mathbb{N}^+$, the sum of $2n + 1$ odd integers is an odd integer.
5. Show that, for any $n \in \mathbb{N}^+$, the product of n even integers is an even integer.
6. Show that, for any $n \in \mathbb{N}^+$, the product of n integers where at least one of them is even is an even integer.
7. Show that, for any $n \in \mathbb{N}^+$, the product of n odd integers is an odd integer.

8.6 Equivalence of PMI, PSMI and WOP

In this section, we show that adopting any one of the PMI, PSMI or WOP allows us to gain the other two principles as invokable ones.

Theorem 8.16. *PMI, PSMI and WOP are equivalent.*

Proof. We must show that

$$\text{PMI} \iff \text{PSMI} \iff \text{WOP}.$$

To that end, we will complete the following:

1. Show PMI $\Rightarrow$ PSMI.
2. Show PSMI $\Rightarrow$ WOP.
3. Show WOP $\Rightarrow$ PMI.

(1) Show PMI $\Rightarrow$ PSMI.
Assume PMI is invokable.
Show PSMI is invokable.
Let $P(n)$ be an open sentence about n.
Show if $P(1) \wedge \forall k[P(1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)]$, then $\forall n P(n)$.
Assume $P(1) \wedge \forall k[P(1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)]$. $\quad (*)$
Show $\forall n P(n)$.
Let $Q(j) \equiv \forall k[k \leq j \Rightarrow P(k)]$.
(Note that $Q(j) \equiv P(1) \wedge \cdots \wedge P(j)$.)
We will next show $\forall j Q(j)$, which is equivalent to $\forall j P(j)$, holds by PMI.
(1.1) We have that $Q(1)$, which is the same as $P(1)$, is true by $(*)$.
(1.2) Show $\forall j[Q(j) \Rightarrow Q(j+1)]$.

Imagine arbitrary j.
Assume $Q(j)$. So we have $P(1) \wedge \cdots \wedge P(j)$. $\quad (**)$
Show $Q(j+1)$.
That is show $P(1) \wedge \cdots \wedge P(j+1)$.
We note that $(**)$ and $(*)$ give $P(j+1)$.
The last line and $(**)$ yield $P(1) \wedge \cdots \wedge P(j+1)$.
So $Q(j+1)$.
Now, using (1.1) and (1.2) and invoking PMI to the sentnce $Q(n)$ establishes $\forall j Q(j)$.
That is we have $\forall j \forall k[k \leq j \Rightarrow P(k)]$.
Letting $k = j$, we get $\forall j[j \leq j \Rightarrow P(j)]$.
Since $j \leq j$, we have $\forall j[P(j)]$.
So PSMI is invokable. $\bullet$

(2) Show PSMI $\Rightarrow$ WOP.
Assume PSMI is invokable.
Show WOP is invokable.
Let $P(n)$ be an open sentence about n.
Show $\neg \forall n P(n) \Rightarrow \big[\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]\big]$.
Assume $\neg \forall n P(n)$. $\quad (*)$
Show $\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$.
!! Presume $\neg\big[\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]\big]$.
So $P(1) \wedge \neg \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$.
So $P(1) \wedge \forall \ell \neg[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$.
So $P(1) \wedge \forall l\big[\neg[P(1) \wedge \cdots \wedge P(\ell-1)] \vee P(\ell)\big]$.
So $\forall \ell\big[\neg[P(1) \wedge \cdots \wedge P(\ell-1)] \vee P(\ell)\big]$.
So $\forall \ell\big[[P(1) \wedge \cdots \wedge P(\ell-1)] \Rightarrow P(\ell)\big]$. $\quad (**)$
Now invoking PSMI for the same open sentence $P(n)$, and noting $P(1)$ and $(**)$ hold, we would conclude
$\forall n P(n)$.
But this contradicts $(*)$. !!
Hence $\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$ holds.
So WOP is invokable. $\bullet$

(3) Show WOP $\Rightarrow$ PMI.
Assume WOP is invokable.
Show PMI is invokable.
Let $P(n)$ be an open sentence about n.
Show if $P(1) \wedge \forall k[P(k) \Rightarrow P(k+1)]$, then $\forall n P(n)$.
Assume $P(1) \wedge \forall k[P(k) \Rightarrow P(k+1)]$. $\quad (*)$
Show $\forall n P(n)$.
!! Presume $\neg \forall n P(n)$.
By stating WOP for the same open sentence $P(n)$, we have $\neg \forall n P(n) \Rightarrow \big[\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]\big]$ holds.
Our presumption gives:
$\neg P(1) \vee \exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$.
Since, by $(*)$, $P(1)$ is true, we must have $\exists \ell[P(1) \wedge \cdots \wedge P(\ell-1) \wedge \neg P(\ell)]$. That is $\ell > 1$ is the smallest element of $\mathbb{N}^+$ with $\neg P(\ell)$. $\quad (**)$
But $(*)$ also gives us, when we let $k = \ell$, $P(\ell-1) \Rightarrow P(\ell)$, or, equivalently, $\neg P(\ell) \Rightarrow \neg P(\ell-1)$.
So this and $(**)$ give us $\neg P(\ell-1)$.
But this contradicts that $P(\ell-1)$, as given in $(**)$. !!
Hence our presumption is false.
Hence $\forall n P(n)$.
So PMI is invokable. $\bullet$

$\square$

Exercises 8.6

1. Directly show PSMI $\Rightarrow$ PMI.
2. Directly show WOP $\Rightarrow$ PSMI.
3. Directly show PMI $\Rightarrow$ WOP.
4. Rewrite the given schematic proof of Theorem 8.16.1 in prose.
5. Rewrite the given schematic proof of Theorem 8.16.2 in prose.
6. Rewrite the given schematic proof of Theorem 8.16.3 in prose.