Elementary Number Theory

KTW

October 3, 2023

Contents

Chapter 1

Preliminaries

1.1 Mathematical Induction

Well-Ordering Principle. *Every nonempty set* S *of nonnegative integers contains a least element; that is, there is some integer* a *in* S *such that* $a \le b$ *for all* b*'s belonging to* S*.*

$$\forall S \subseteq \mathbb{Z}_{>0}, \exists a \in S : \forall b \in S, a \le b$$

Theorem 1.1 (Archimedian Property)**.** *If* a *and* b *are any positive integers, then there exists a positive integer* n *such that* $na \ge b$*.*

$$\forall a, b \in \mathbb{Z}_{>0}, \exists n \in \mathbb{Z}_{>0} : na \ge b$$

Proof. For reductio ad aubsurdum, suppose that the statement of the therorem is false. Then:

$$\begin{aligned}
&\neg(\forall a, b \in \mathbb{Z}_{>0}, \exists n \in \mathbb{Z}_{>0} : na \ge b) \\
\Leftrightarrow\ &\exists a, b \in \mathbb{Z}_{>0} : \forall n \in \mathbb{Z}_{>0}, na < b \\
\Leftrightarrow\ &\exists a, b \in \mathbb{Z}_{>0} : \forall n \in \mathbb{Z}_{>0}, 0 < b - na \\
\Leftrightarrow\ &S = \{b - na \mid n \in \mathbb{Z}_{>0}\} = \mathbb{Z}_{>0} \\
\Rightarrow\ &\exists b - ma \in S : \forall b - na \in S, b - ma \le b - na \quad \text{[by the Well-Ordering Principle]} \\
\Rightarrow\ &\exists b - ma, b - (m+1)a \in S : \forall b - na \in S, b - (m+1)a < b - ma \le b - na \longrightarrow \perp \\
\Rightarrow\ &\forall a, b \in \mathbb{Z}_{>0}, \exists n \in \mathbb{Z}_{>0} : na \ge b
\end{aligned}$$

□

Theorem 1.2 (First Principle of Finite Induction)**.** *Let* S *be a set of positive integers with the following properties:*
(a) $\exists 1 \in S$
(b) $\forall k \in S, \exists k + 1 \in S$
Then S *is the set of all positive integers.*

Proof. Let S be a set of positive integers such that:

$$\exists 1 \in S \ \&\ \forall k \in S, \exists k + 1 \in S$$

For reductio ad absurdum, let T be a nonempty set of all positive integers not in S, that is:

$$T = \{t \in \mathbb{Z}_{>0} \mid t \notin S\}$$

By the Well-Ordering Principle, T has a least element a, and:

$$\begin{aligned}
1 \in S &\Rightarrow 1 < a \in T \\
&\Leftrightarrow 0 < a - 1 \notin T \\
&\Leftrightarrow a - 1 \in S \\
&\Leftrightarrow a \in S \longrightarrow \perp \\
&\Rightarrow T = \varnothing \\
&\Leftrightarrow S = \mathbb{Z}_{>0}
\end{aligned}$$

□

Theorem 1.3 (Second Principle of Finite Induction)**.** *Let* S *be a set of positive integers with the following properties:*
(a) $\exists 1 \in S$
(b) $\exists 1, 2, \ldots, k \in S \Rightarrow \exists k+1 \in S$
Then S *is the set of all positive integers.*

Proof. Let S be a set of positive integers follwing properties above. For reductio ad absurdum, let T be a nonempty set of all positive integers not in S. By the Well-Ordering Principle, T has a least element a, and:

$$\begin{aligned} 1 \in S &\Rightarrow 1 < a \in T \\ &\Leftrightarrow 0 < 1, \ldots, a-1 \notin T \\ &\Leftrightarrow 1, \ldots, a-1 \in S \\ &\Leftrightarrow a \in S \longrightarrow \perp \\ &\Rightarrow T = \varnothing \\ &\Leftrightarrow S = \mathbb{Z}_{>0} \end{aligned}$$

□

Example 1.4 (Lucas sequence)**.**

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

Sequence above may be defined inductively by

$$\begin{cases} a_1 = 1 \\ a_2 = 3 \\ a_n = a_{n-1} + a_{n-2} & \text{for all } n \geq 3 \end{cases}$$

We contend that the inequality

$$a_n < \left(\frac{7}{4}\right)^n$$

holds for every positive integer n. First of all, for $n = 1$ and 2, we have

$$a_1 = 1 < \left(\frac{7}{4}\right)^1 \quad \& \quad a_2 = 3 < \left(\frac{7}{4}\right)^2 = 3\frac{1}{16}$$

and this provides a basis for the induction. For the induction step, choose an integer $k \geq 3$ and assume that the inequality is valid for $n = 1, 2, \ldots, k-1$. Then, in particular:

$$a_{k-1} < \left(\frac{7}{4}\right)^{k-1} \quad \& \quad a_{k-2} < \left(\frac{7}{4}\right)^{k-2}$$

By the way in which the sequence is formed, it follows that:

$$\begin{aligned} a_k = a_{k-1} + a_{k-2} &< \left(\frac{7}{4}\right)^{k-1} + \left(\frac{7}{4}\right)^{k-2} \\ &= \left(\frac{7}{4}\right)^{k-2} \left(\frac{7}{4} + 1\right) \\ &= \left(\frac{7}{4}\right)^{k-2} \left(\frac{11}{7}\right) \\ &< \left(\frac{7}{4}\right)^{k-2} \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^k \end{aligned}$$

Because the inequality is true for $n = k$ whenever it is true for the integers $1, 2, \ldots, k-1$, we conclude by the second induction principle that $a_n < (7/4)^n$ for all $n \geq 1$.

Problems 1.1

1. Establish the formulas below by mathamatical induction:
(a) $1+2+3+\cdots+n=\frac{n(n+1)}{2}$ for all $n\geq 1$.
(b) $1+3+5+\cdots+(2n-1)=n^2$ for all $n\geq 1$.
(c) $1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$ for all $n\geq 1$.
(d) $1^2+3^2+5^2+\cdots+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$ for all $n\geq 1$.
(e) $1^3+2^3+3^3+\cdots+n^3=\left[\frac{n(n+1)}{2}\right]^2$ for all $n\geq 1$.

♯1(a). Let S be a set such that:

$$S=\left\{n\in\mathbb{N}:1+2+3+\cdots+n=\frac{n(n+1)}{2}\right\}$$

$1\in S$ because for $n=1$:

$$1=\frac{1(1+1)}{2}$$

Let any $k\in\mathbb{N}$ be the member of S, that is:

$$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

Then;

$$\begin{aligned}1+2+3+\cdots+k+(k+1)&=\frac{k(k+1)}{2}+(k+1)\\&=\frac{k(k+1)}{2}+\frac{2(k+1)}{2}\\&=\frac{(k+1)(k+2)}{2}\end{aligned}$$

therefore by the First Principle of Finite Induction, $S=\mathbb{N}$. ■

♯1(b). Let S be a set such that:

$$S=\left\{n\in\mathbb{N}:1+3+5+\cdots+(2n-1)=n^2\right\}$$

$1\in S$ because for $n=1$:

$$(2\cdot 1-1)=1=1^2$$

Let any $k\in\mathbb{N}$ be the member of S, that is:

$$1+3+5+\cdots+(2k-1)=k^2$$

Then;

$$\begin{aligned}1+3+\cdots+(2k-1)+[2(k+1)-1]&=k^2+[2(k+1)-1]\\&=k^2+2k+1\\&=(k+1)^2\end{aligned}$$

therefore by the First Principle of Finite Induction, $S=\mathbb{N}$. ■

♯1(c). Let S be a set such that:

$$S=\left\{n\in\mathbb{N}:1\cdot 2+2\cdot 3+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}\right\}$$

$1 \in S$ because for $n = 1$:

$$1(1+1) = 2 = \frac{1(1+1)(1+2)}{3}$$

Let any $k \in \mathbb{N}$ be the member of S, that is:

$$1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$$

Then;

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 3 + \cdots + k(k+1) + (k+1)(k+2) &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= \frac{k(k+1)(k+2)}{3} + \frac{3(k+1)(k+2)}{3} \\ &= \frac{(k+1)(k+2)(k+3)}{3} \end{aligned}$$

therefore by the First Principle of Finite Induction, $S = \mathbb{N}$.

♯1(d). Let S be a set such that:

$$S = \left\{ n \in \mathbb{N} : 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3} \right.$$

$1 \in S$ because for $n = 1$:

$$(2 \cdot 1 - 1)^2 = 1 = \frac{3}{3}$$

Let any $k \in \mathbb{N}$ be the member of S, that is:

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

Then;

$$\begin{aligned} 1^2 + 3^2 + \cdots + (2k-1)^2 + (2k+1)^2 &= \frac{k(2k-1)(2k+1)}{3} + (2k+1)^2 \\ &= \frac{k(2k-1)(2k+1)}{3} + \frac{3(2k+1)^2}{3} \\ &= \frac{(2k+1)[k(2k-1) + 3(2k+1)]}{3} \\ &= \frac{(2k+1)[2k^2 + 5k + 3]}{3} \\ &= \frac{(2k+1)(2k+3)(k+1)}{3} \\ &= \frac{(k+1)(2k+1)(2k+3)}{3} \end{aligned}$$

therefore by the First Principle of Finite Induction, $S = \mathbb{N}$. ■

♯1(e). Let S be a set such that:

$$S = \left\{ n \in \mathbb{N} : 1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 \right\}$$

$1 \in S$ for $n = 1$ beacuase:

$$1^3 = 1 = 1^2$$

Let any $k \in \mathbb{N}$ be the member of S, that is:

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

Then;

$$\begin{aligned}
1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \\
&= \frac{k^2}{4}(k+1)(k+1) + (k+1)(k+1)(k+1) \\
&= (k+1)^2\left(\frac{k^2}{4} + (k+1)\right) \\
&= (k+1)^2\left(\frac{k}{2} + 1\right)^2 \\
&= (k+1)^2\left(\frac{k+2}{2}\right) \\
&= \left[\frac{(k+1)(k+2)}{2}\right]^2
\end{aligned}$$

therefore by the First Principle of Finite Induction, $S = \mathbb{N}$. ■

2. If $r \neq 1$, show that for any positive integer n,

$$a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1}{r - 1}$$

♯2. Let S be a set such that:

$$S = \left\{ n \in \mathbb{N} : a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1} \right.$$

$1 \in S$ for $n = 1$ because:

$$a + ar^1 = a(r+1) = \frac{a(r+1)(r-1)}{r-1} = \frac{a(r^2 - 1)}{r - 1}$$

Let any $k \in \mathbb{N}$ be the member of S, that is:

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

Then;

$$\begin{aligned}
a + ar + \cdots + ar^k + ar^{k+1} &= \frac{a(r^{k+1} - 1)}{r - 1} + ar^{k+1} \\
&= \frac{a(r^{k+1} - 1)}{r - 1} + \frac{(r-1)ar^{k+1}}{r - 1} \\
&= \frac{ar^{k+2} - ar^{k+1} + ar^{k+1} - a}{r - 1} \\
&= \frac{ar^{k+2} - a}{r - 1} \\
&= \frac{a(r^{k+2} - 1)}{r - 1}
\end{aligned}$$

therefore by the First Principle of Finite Induction, $S = \mathbb{N}$. ■

3. Use the Second Principle of Finite Induction to establish that for all $n \geq 1$,

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

[Hint: $a^{n+1} - 1 = (a+1)(a^n - 1) - a(a^{n-1} - 1)$.]

♯3. Let S be a set such that:

$$S = \left\{n \in \mathbb{N} : a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1\right\}$$

$1 \in S$ for $n = 1$ because:

$$a - 1 = (a-1)a^0$$

Let any $k \in \mathbb{N}$ be the member of S, that is:

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$$

Then;

$$\begin{aligned}
(a+1)(a^k - 1) - a(a^{k-1} - 1) &= (a+1)(a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1) - a(a^{k-1} - 1) \\
&= (a-1)(a+1)(a^{k-1} + a^{k-2} + \cdots + a + 1) - a(a^{k-1} - 1) \\
&= (a-1)[a(a^{k-1} + \cdots + a + 1) + (a^{k-1} + \cdots + a + 1)] - a(a^{k-1} - 1) \\
&= (a-1)[a^k + 2(a^{k-1} + \cdots + a) + 1] - a(a^{k-1} - 1) \\
&= (a-1)[a^k + 2(a^{k-1} + \cdots + a) + 1] - a^k + a
\end{aligned}$$

since

$$a^k = (a-1)(a^{k-1} + a^{k-2} + \cdots + a) + a$$

by assumption;

$$\begin{aligned}
(a-1)[a^k + 2(a^{k-1} + \cdots + a) + 1] - a^k + a &= (a-1)(a^k + a^{k-1} + \cdots a + 1) - a + a \\
&= (a-1)(a^k + a^{k-1} + \cdots + a + 1)
\end{aligned}$$

and by the Second Principle of Finite Induction, $S = \mathbb{N}$. ■

4. Prove that the cube of any integer can be written as the difference of two squares. Notice that

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

♯4. By the result of **♯1(e)**, for all $n \in \mathbb{N}$;

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

and since;

$$\begin{aligned}
n^3 &= (1^3 + 2^3 + \cdots + n^3) - (1^3 + 2^3 + \cdots + (n-1)^3) \\
&= \left[\frac{n(n+1)}{2}\right]^2 - \left[\frac{(n-1)(n-2)}{2}\right]^2
\end{aligned}$$

the cube of any integer n can be written as the difference of two squares. ■

5.

(a) Find the values of $n \leq 7$ for which $n! + 1$ is a perfect square.
(b) True or false? For positive integers m and n, $(mn)! = m!n!$ and $(m+n)! = m! + n!$.

♯5.
(a) $n = 4, 5, 7$.
(b) False by counter examples such as $m = 2, n = 3$ where

$$(mn)! = 6! = 6 \cdot 5 \cdot \cdots \cdot 1 = 720 \neq 12 = 2 \cdot 3 \cdot 2 \cdot 1 = m!n!$$

■

1.2 The Binomial Theorem