Elementary Number Theory

KTW

October 2, 2023

Contents

Contents **2**

1 Preliminaries **3**

1.1 Mathematical Induction 3

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* $a \leq b$ *for all* b*'s belonging to* S.

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

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

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

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

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

□

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 $n \geq 1$.