Journal of Innovative Technology and Education, Vol. 11, 2024, no. 1, 1 - 9
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/jite.2024.1157

On Mathematical Induction

Dinamérico P. Pombo Jr.

Instituto de Matemática e Estatística
Universidade Federal Fluminense, Brazil

Abstract

In this note the equivalence among the Well-ordering Principle, the Principle of Finite Induction and certain natural conditions concerning the set of integers is discussed, thereby clarifying facts encountered in the literature.

Mathematics Subject Classification: 97B50, 97C70

Keywords: set of natural numbers, set of integers, Well-ordering Principle, Principle of Finite Induction

1 Introduction

Peano's Postulates for the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of natural numbers [5, p. 35; 7], which may be regarded under the viewpoint of universality [3; 4; 5, Chap. 2], subsume the *Principle of Finite Induction*:

If U is a subset of $\mathbb{N}$ such that $0 \in U$ and $n + 1 \in U$ whenever $n \in U$, then $U = \mathbb{N}$.

The Principle of Finite Induction ensures the validity of the *Well-ordering Principle*, which reads:

Every non-empty subset of $\mathbb{N}$ admits a least element.

This is precisely the statement of Proposition 7, p. 41 of [5], in whose proof one assumes the existence of a non-empty subset V of $\mathbb{N}$ which does not admit a least element and one shows, by induction on n, that "$x \in V$" implies "$x \geq n$", from which one arrives at a contradiction.

On the other hand, the Principle of Finite Induction is a consequence of the Well-ordering Principle, as Theorem 4, p. 10 of [1] guarantees. As a matter of fact, in the proof of the just mentioned result, one takes U as above and assumes that $U \neq \mathbb{N}$, that is, $\mathbb{N}' = \mathbb{N} \setminus U \neq \phi$. If m is the least element of $\mathbb{N}'$, $m - 1 \in U$, and hence $m = (m-1) + 1 \in U$, which cannot occur.

In this note, motivated by results appearing in Chapter I of [1] and Chapter 1 of [6], equivalent conditions to the above-mentioned principles will be discussed. Historical comments concerning *Mathematical Induction* may be found, for example, in [2] and [6].

2 On the Well-ordering Principle and the Principle of Finite Induction

As always, $\mathbb{Z}$ will denote the set of integers.

Firstly we shall prove a result motivated by Exercise 5, p. 11 of [1].

Proposition 2.1. The following conditions are equivalent:

(a) Well-ordering Principle;

(b) every non-empty subset of $\mathbb{Z}$, with an upper bound, possesses a greatest element;

(c) every non-empty subset of $\mathbb{Z}$, with a lower bound, possesses a least element.

Proof. (a) $\Rightarrow$ (b): Let S be a non-empty subset of $\mathbb{Z}$ admitting an upper bound s. Since

$$X = \{s - t\,; t \in S\}$$

is a non-empty subset of $\mathbb{N}$, (a) guarantees the existence of an element u of S so that $s - u \leq s - t$ for all $t \in S$. Thus $t \leq u$ for all $t \in S$, proving (b).

(b) $\Rightarrow$ (c): Let T be a non-empty subset of $\mathbb{Z}$ admitting a lower bound. Then the non-empty subset $-T = \{-t;\, t \in T\}$ of $\mathbb{Z}$ possesses an upper bound. Hence, by (b), there is a $v \in T$ such that $-t \leq -v$ for all $t \in T$, that is, $v \leq t$ for all $t \in T$. Therefore (c) is established.

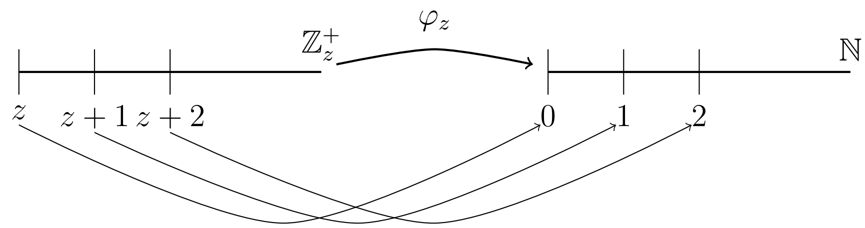
(c) $\Rightarrow$ (a): It suffices to observe that $\mathbb{N}$ has a lower bound.

This completes the proof.

Before proceeding, let us introduce a few notations. Indeed, for each $z \in \mathbb{Z}$ let us write $\mathbb{Z}_z^+ = \{t \in \mathbb{Z}, t \geq z\}$. Obviously, the mapping

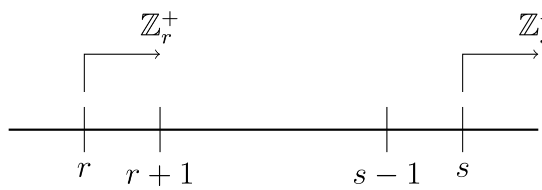
$$\varphi_z \colon t \in \mathbb{Z}_z^+ \longmapsto \varphi_z(t) = t - z \in \mathbb{N}$$

is bijective. Let us also write $\mathbb{Z}_z^- = \{t \in \mathbb{Z};\, t \leq z\}$. Clearly $\mathbb{Z}_z^- = -\left(\mathbb{Z}_{-z}^+\right)$ and z is the least (resp. greatest) element of $\mathbb{Z}_z^+$ (resp. $\mathbb{Z}_z^-$).



Remark 2.2. For all $r, s \in \mathbb{Z}$, with $r < s$, the infinite sets $\mathbb{Z}_r^+$ and $\mathbb{Z}_s^+$ are *quite similar*, in the sense that

$$\mathbb{Z}_r^+ = \mathbb{Z}_s^+ \cup \{r, \ldots, s-1\} \ \left(\mathbb{Z}_r^+ = \mathbb{Z}_s^+ \cup \{r\} \text{ if } s = r+1\right).$$



Evidently we would have a similar remark for the sets $\mathbb{Z}_z^-$.

In the example below we shall furnish an infinite family of infinite subsets of $\mathbb{N}$, each of which does not coincide with a set $\mathbb{Z}_z^+$.

Example 2.3. For each prime natural number p, let us consider the subset

$$X_p = \{p, p^2, \ldots, p^n, p^{n+1}, \ldots\}$$

of $\mathbb{N}$. Since

$$p^{n+1} - p^n = p^n(p-1) \geq p^n \geq 2$$

for every integer $n \geq 1$, X_p is an infinite set whose least element is p and which does not coincide with a set $\mathbb{Z}_z^+$, and the distances between two consecutive elements of X_p may be taken as big as we wish. Moreover, if p, q are arbitrary prime natural numbers, with $p \neq q$, then $X_p \cap X_q = \phi$.

The next result was motivated by Exercise 4, p. 10 of [1] and Theorem 1.3.1, p. 25 of [6].

Proposition 2.4. The following conditions are equivalent:

(a') Principle of Finite Induction;

(b') for each $z \in \mathbb{Z}$, if $R \subset \mathbb{Z}_z^+$, $z \in R$ and $n+1 \in R$ whenever $n \in R$, then $R = \mathbb{Z}_z^+$;

(c') for each $w \in \mathbb{Z}$, if $S \subset \mathbb{Z}_w^-$, $w \in S$ and $n-1 \in S$ whenever $n \in S$, then $S = \mathbb{Z}_w^-$.

Proof. (a') $\Rightarrow$ (b'): Put $L = \varphi_z(R)$; $L \subset \mathbb{N}$ and $0 = \varphi_z(z) \in L$ (since $z \in R$). If $m \in L$ is arbitrary, $m = \varphi_z(n)$ for a (unique) element n of R. By hypothesis, $n+1 \in R$ and

$$\varphi_z(n+1) = (n+1) - z = (n-z) + 1 = \varphi_z(n) + 1 = m + 1,$$

showing that $m+1 \in L$. Thus, by (a'), $L = \mathbb{N}$, which is equivalent to $R = \mathbb{Z}_z^+$. Hence (b') holds.

(b') $\Rightarrow$ (c'): First $-S \subset -(\mathbb{Z}_w^-) = \mathbb{Z}_{-w}^+$ and $-w \in -S$. Moreover, if $n \in S$ is arbitrary and $m = -n$, $m+1 = -n+1 = -(n-1) \in -S$, because $n-1 \in S$ by hypothesis. Therefore, by (b'), $-S = \mathbb{Z}_{-w}^+$, which is equivalent to $S = \mathbb{Z}_w^-$ and proves (c').

(c') $\Rightarrow$ (a'): Let $T \subset \mathbb{N}$ be such that $0 \in T$ and $n+1 \in T$ whenever $n \in T$. Then $0 \in (-T) \subset (-\mathbb{Z}_o^+) = \mathbb{Z}_o^-$ and $n-1 \in (-T)$ if $n \in (-T)$, and (c') yields $-T = \mathbb{Z}_o^-$, which is equivalent to $T = \mathbb{Z}_o^+ = \mathbb{N}$ and proves (a').

This completes the proof.

What we have seen may be summarized in

Corollary 2.5. The conditions (a), (b), (c), (a'), (b') and (c') are equivalent.

3 Examples

Firstly let us mention the following:

Remark 3.1. Let $z \in \mathbb{Z}$ be arbitrary and let us assume that to each $t \in \mathbb{Z}_z^+$ it is associated an assertion $a(t)$ in such a way that $a(z)$ is true and that, for a given $t \in \mathbb{Z}_z^+$, $a(t+1)$ holds whenever $a(t)$ holds. Then $a(t)$ is valid for all $t \in \mathbb{Z}_z^+$.

Indeed, it suffices to consider the subset

$$R = \big\{t \in \mathbb{Z}_z^+ \,;\, a(t) \text{ is valid}\big\}$$

of $\mathbb{Z}_z^+$ and to apply Proposition 2.4 to obtain $R = \mathbb{Z}_z^+$.

Throughout we shall write $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Example 3.2. For all $n \in \mathbb{N}^*$, the number of subsets of the set $\{1, \dots, n\}$ is 2^n.

In fact, since the subsets of $\{1\}$ are $\emptyset$ and $\{1\}$, the assertion holds for $n = 1$. Now, let us assume its validity for a certain $n \in \mathbb{N}^*$. Since

$$\{1, \dots, n, n+1\} = \{1, \dots, n\} \cup \{n+1\} \quad \text{and} \quad \{1, \dots, n\} \cap \{n+1\} = \emptyset,$$

the number of subsets A of $\{1, \dots, n, n+1\}$ for which $n+1 \in A$ coincides with the number of subsets of $\{1, \dots, n\}$, that is, coincides with 2^n. Thus the number of subsets of $\{1, \dots, n, n+1\}$ is $2 \cdot 2^n = 2^{n+1}$, and the assertion is a consequence of Remark 3.1.

Example 3.3. Let p be an arbitrary prime natural number. For all $n \in \mathbb{Z}$, with $n \geq 2$, and for all non-zero integers $a_1, a_2, \dots, a_n$ such that $p | a_1 \cdot a_2 \cdots a_n$, one has $p | a_1$, or $p | a_2, \dots$, or $p | a_n$.

Indeed, the case $n = 2$ corresponds to a fundamental result of Euclides [1, p. 19]. Now let us assume that, for a given $n \in \mathbb{Z}$, with $n \geq 3$, the assertion holds for $n - 1$. Since $p | \big(a_1(a_2 \cdots a_n)\big)$, it follows that $p | a_1$ or $p | (a_2 \cdots a_n)$. If $p | a_1$, we are done. On the other hand, if $p | (a_2 \cdots a_n)$, there would exist a $j \in \{2, \dots, n\}$ for which $p | a_j$. Therefore, by Remark 3.1, our claim is justified.

Example 3.4. For all $n \in \mathbb{Z}$, with $n \geq 4$, one has $2^{n-2} \geq n$.

In fact, since the claim is obvious for $n = 4$, let us suppose $2^{(n-1)-2} = 2^{n-3} \geq n - 1$ for a certain $n > 4$. Then,

$$2^{n-2} = 2^{(n-3)+1} = 2 \cdot 2^{n-3} \geq 2(n-1) = 2n - 2 > n,$$

so that our claim holds for n. Therefore, by Remark 3.1, our claim is justified.

Consequently, $2^n > n$ for all $n \in \mathbb{N}$. Indeed, the claim is obvious if $n \in \{0, 1, 2, 3\}$. And, if $n \geq 4$, what we have just seen gives

$$2^n = 2^2 2^{n-2} \geq 4n > n.$$

Example 3.5. For all $n \in \mathbb{N}^*$,

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

Indeed, since our assertion is obvious for $n = 1$, let us suppose its validity for a given $n \in \mathbb{N}^*$. Then

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

and our assertion is valid for $n+1$. Hence, by Remark 3.1, our claim is justified.

Example 3.6. For all $n \in \mathbb{N}$,

$$9|(10^n + 3{\cdot}4^{n+2} + 5)$$

(that is, 9 is a divisor of $10^n + 3{\cdot}4^{n+2} + 5$).

In fact, since our claim is obvious for $n = 0$, let us assume its validity for a given $n \in \mathbb{N}^*$. Thus, since

$$\begin{aligned} 10^{n+1} + 3{\cdot}4^{(n+1)+2} + 5 &= (9+1)10^n + 12{\cdot}4^{n+2} + 5 \\ &= (10^n + 3{\cdot}4^{n+2} + 5) + 9(10^n + 4^{n+2}), \end{aligned}$$

it follows that $9|(10^{n+1} + 3{\cdot}4^{(n+1)+2} + 5)$, so that our assertion is valid for $n+1$. Hence, by Remark 3.1, our claim holds.

Example 3.7. For all $n \in \mathbb{N}^*$ and for all $x_1, \ldots, x_n$ in the set $\mathbb{R}$ of real numbers,

$$|x_1 + \cdots + x_n| \leq |x_1| + \cdots |x_n|,$$

where $|\cdot|$ denotes the absolute value on $\mathbb{R}$.

Indeed, since the assertion is clear for $n = 1$, let us suppose its validity for a given $n \in \mathbb{N}^*$. Therefore, for $x_1, \ldots, x_n, x_{n+1} \in \mathbb{R}$, the triangle inequality and what we have just assumed give

$$|x_1 + \cdots + x_n + x_{n+1}| \leq |x_1 + \cdots + x_n| + |x_{n+1}| \leq |x_1| + \cdots + |x_n| + |x_{n+1}|,$$

showing the validity of our claim for $n+1$. Thus, by Remark 3.1, our claim is justified.

Example 3.8. For all $x \in \mathbb{R}$, with $x > 0$, one has

$$\lim_{n \to \infty} \sqrt[n]{x} = 1.$$

Firstly let us suppose $x > 1$ and let us show that $(1+x)^n \geq 1 + nx$ for all $n \in \mathbb{N}^*$, which also follows from the binomial formula [1, p. 13].

In fact, since the inequality is clear for $n = 1$, let us assume its validity for a given $n \in \mathbb{N}^*$. Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \geq (1+nx)(1+x) \\ &= 1 + (n+1)x + nx^2 > 1 + (n+1)x \end{aligned}$$

and the inequality holds for $n+1$. Hence Remark 3.1 ensures the validity of the inequality for all $n \in \mathbb{N}^*$. Now, for each $n \in \mathbb{N}^*$ let us write $\sqrt[n]{x} = 1 + h_n$, where $h_n > 0$. Therefore

$$x = \left(\sqrt[n]{x}\right)^n = (1+h_n)^n \geq 1 + nh_n$$

for all $n \in \mathbb{N}^*$, in such a way that

$$0 < h_n \leq \frac{x-1}{n}$$

for all $n \in \mathbb{N}^*$. But, since $\lim_{n\to\infty} \frac{x-1}{n} = 0$ in view of the Archimedean property, one concludes that $\lim_{n\to\infty} h_n = 0$, and consequently $\lim_{n\to\infty} \sqrt[n]{x} = 1$.

On the other hand, if $0 < x < 1$ (if $x = 1$ our claim is obvious), $\frac{1}{x} > 1$, and what we have proved furnishes $\lim_{n\to\infty} \sqrt[n]{\frac{1}{x}} = 1$. Thus $\lim_{n\to\infty} \sqrt[n]{x} = 1$.

By a similar argument [3, p. 35], one justifies:

Example 3.9. $\lim\limits_{n\to\infty} \sqrt[n]{n} = 1$.

Example 3.10. If X is a non-empty set and $f : X \to X$ is an injective (resp. a surjective) function, then the composite function

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}} : X \to X$$

is injective (resp. surjective) for all $n \in \mathbb{N}^*$. In particular, if f is bijective, then f^n is bijective for all $n \in \mathbb{N}^*$.

We shall restrict ourselves to the injectivity. As a matter of fact, assume that f is injective, so that the assertion is obvious for $n = 1$. Suppose that f^n is injective for a given $n \in \mathbb{N}^*$. Then, since

$$f^{n+1} = f^n \circ f,$$

it follows immediately that f^{n+1} is injective. Thus, by Remark 3.1, f^n is injective for all $n \in \mathbb{N}^*$.

Let $a, b \in \mathbb{R}$, with $a < b$. By recalling that the sum $f+g$ and the product fg of two continuous functions $f, g : [a, b] \to \mathbb{R}$ on $[a, b]$ are continuous functions on $[a, b]$, one may apply Remark 3.1 to conclude:

Example 3.11. For all $n \in \mathbb{N}^*$, if $f_1, \ldots, f_n : [a, b] \to \mathbb{R}$ are continuous functions on $[a, b]$, then $f_1 + \cdots + f_n$ and $f_1 \cdots f_n$ are continuous functions on $[a, b]$.

In particular, every polynomial $p(x) = c_0 + c_1 x + \cdots + c_n x^n$ ($c_0, c_1, \ldots, c_n \in \mathbb{R}$) is a continuous function on $\mathbb{R}$.

Example 3.12. Let $\mathbb{Q}$ be the set of rational numbers and $f : \mathbb{Q} \to \mathbb{Q}$ an injective function such that $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in \mathbb{Q}$. Then $f(x) = x$ for all $x \in \mathbb{Q}$.

Initially, we shall show that $f(n) = n$ for all $n \in \mathbb{N}$. Indeed, $f(0) = 0$, since $f(0) = f(0+0) = f(0) + f(0)$. Hence $f(1) \neq 0$, because f is injective, and the equality $f(1) = f(1 \cdot 1) = f(1)f(1) = f(1)^2$ furnishes $f(1) = 1$. Assume $f(n) = n$ for some $n \in \mathbb{N}$. Then $f(n+1) = f(n) + f(1) = n + 1$. Thus, by Remark 3.1, $f(n) = n$ for all $n \in \mathbb{N}$. Consequently, for any $n \in \mathbb{N}^*$,

$$0 = f(0) = f\big(n + (-n)\big) = f(n) + f(-n) = n + f(-n),$$

that is, $f(-n) = -n$. Hence $f(n) = n$ for all $n \in \mathbb{Z}$.

Now, let $m \in \mathbb{Z}$, with $m \neq 0$. Since

$$1 = f(1) = f\left(m \cdot \frac{1}{m}\right) = f(m) f\left(\frac{1}{m}\right) = m f\left(\frac{1}{m}\right),$$

$f\left(\frac{1}{m}\right) = \frac{1}{m}$. Finally, for all $m, n \in \mathbb{Z}$, with $m \neq 0$,

$$f\left(\frac{n}{m}\right) = f\left(n \cdot \frac{1}{m}\right) = f(n) f\left(\frac{1}{m}\right) = \frac{n}{m},$$

as was to be shown.

4 Conclusion

In this note the equivalence among the Well-ordering Principle, the Principle of Finite Induction and certain natural conditions has been established, and a few known examples have been included.

References

[1] G. Birkhoff and S. Mac Lane, *A Survey of Modern Algebra*, Eighth Printing, Macmillan, New York, 1971. https://doi.org/10.1201/9781315275499

[2] F. Cajori, Origin of the Name “Mathematical Induction”, *Amer. Math. Monthly*, **25** (1918), 197-201. https://doi.org/10.1080/00029890.1918.11998417

[3] F.W. Lawvere, An elementary theory of the category of sets, *Proc. Nat. Acad. Sci. U.S.A.*, **52** (1964), 1506-1511. https://doi.org/10.1073/pnas.52.6.1506

[4] F.W. Lawvere, An elementary theory of the category of sets (long version) with commentary, *Reprints in Theory and Applications of Categories*, **11** (2005), 1-35. https://doi.org/10.1007/bfb0080769

[5] S. Mac Lane and G. Birkhoff, *Algebra*, Sixth Printing, Macmillan, New York, 1971.

[6] C.P. Milies and S.P. Coelho, *Números: Uma Introdução à Matemática*, Editora da Universidade de São Paulo, São Paulo, 1998.

[7] G. Peano, *Arithmeticas principia*, novo methodo exposita, Turin, 1889.

Received: October 17, 2024; Published: November 8, 2024