Principles of Induction and Well-ordering

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

We enunciate three principles which essentially state properties enjoyed by the set $\mathbb{N}$ of positive integers. Our aim in this article is to show that $\mathbb{N}$ has one of these properties if and only if it enjoys the other two.

The Induction Principle. Let $A \subset \mathbb{N}$. Assume that (i) $1 \in A$ and that (ii) $n \in A$ implies that $n+1 \in A$. Then $A = \mathbb{N}$.

The Strong Induction Principle. Let $B \subset \mathbb{N}$. Assume that $1 \in B$ and that if $1, 2, \ldots, n \in B$ implies that $n+1 \in B$. Then $B = \mathbb{N}$.

The Well-Ordering Principle. Let $C \subset \mathbb{N}$ be nonempty. Then C has a least element.

Theorem 1. *The above three principles are equivalent.*

Proof. Do you understand what exactly the theorem means? If one of the principle holds true for $\mathbb{N}$, then the other two are also true.

(1) $\implies$ (2): Let B satisfy the hypothesis of the strong induction principle. We wish to show that $B = \mathbb{N}$. We want to use the induction principle. So, we need to devise a set to which the induction principle can be applied. With this in mind, let us define $A := \{n \in \mathbb{N} : \{1, 2, \ldots, n\} \subset B\}$.

Now, $1 \in A$, since by hypothesis on B, $1 \in B$. By the definition of A, it therefore follows that $1 \in A$. Now let $n \in A$. This means that $1, 2, \ldots, n \in B$, by the very definition of A. But by the hypothesis on B, it follows that $n+1 \in B$. Thus $\{1, 2, \ldots, n+1\} \subset B$. By the definition of B, we deduce that $n+1 \in A$. Thus, $A \subset \mathbb{N}$ is such that $1 \in A$ and $n \in \mathcal{A}$ implies that $n+1 \in A$. By the induction principle, we have $A = \mathbb{N}$. In particular, for each $n \in \mathbb{N}$, we have $n \in A$, But then it follows from the definition of A that $1, 2, \ldots, n \in B$, in particular, $n \in B$. Thus for each $n \in \mathcal{B}$, we have shown that $n \in B$. Thus, $\mathbb{N} \subset B$ and hence $B = \mathbb{N}$. That is, we have proved if the induction principle is true for $\mathbb{N}$ then the strong induction principle holds true for $\mathbb{N}$.

(2) $\implies$ (3): Let the strong induction principle is true for $\mathbb{N}$. Let $C \subset \mathbb{N}$ be any nonempty set. We need to show that C has a least element. We prove this by contradiction. More precisely, we wish to show that if $C \subset \mathbb{N}$ has no least element, then C must be $\emptyset$. If it is true, then if we define $A := \mathbb{N} \setminus C$ must be all of $\mathbb{N}$. One way of showing that this what

happens is to show that A is eligible for an application of the strong induction principle. So, let $A := \mathbb{N} \setminus C$.

Now, $1 \in A$. If it were false, then $1 \in C$. But then, clearly, C has a least element! So, we infer that $1 \notin C$ and so, $1 \in A$. Let $1, 2, \ldots, n \in A$. This means that none of them lie in C. We claim that $n+1 \notin C$. If $n+1 \in C$, since $k \notin C$ for all $k = 1, 2, \ldots, n$, it would mean that $n+1$ must be a least element of C. This contradicts our assumption that C has no least element. We therefore conclude that $n+1 \notin C$. Hence, $n+1 \in A$. What we have so far achieved is that A has the properties required by the strong induction principle. Hence, we deduce that $A = \mathbb{N}$ and therefore $C = \emptyset$.

(3) $\implies$ (1): Let us assume that the well-ordering principle holds for $\mathbb{N}$. Let $A \subset \mathbb{N}$ be such that $1 \in A$, and such that whenever $n \in A$, we have $n+1 \in A$. We wish to show that $A = \mathbb{N}$. Suppose this is false. Then the set $C := \mathbb{N} \setminus A$ is nonempty. By the well-ordering principle, C has a least element, say, L. This integer L cannot be 1. For, if it were, $1 \in C$ and hence $1 \notin A$, contradicting our assumption on A. Therefore $L \geq 2$. As a consequence, $L-1$ is a positive integer in $\mathbb{N}$. Since L is the (?) least element of C, we deduce that $k \notin C$ for all $k = 1, 2, \ldots, L-1$. In particular, they all belong to A. But then by the property of A, since $L-1 \in A$, we see that $L \in A$. This is a contradiction since $A \cap C = \emptyset$. This contradiction forces us to conclude that C must be empty, that is, $A = \mathbb{N}$, as desired. □

Remark 2. The condition (i) of the Induction Principle is called the basis for induction awhile (ii) is called the inductive step.

Both these conditions are important can seen from Ex. 10 and Ex. 11.

We illustrate the principle by means of a few examples.

Example 3. For any positive integer n, we have

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

Let $P(n)$ be the statement Eq. 1. We first observe that $P(1)$ is true. Let us now assume that $P(k)$ is true. Thus we have $1 + \cdots + n = n(n+1)/2$. We now add $n+1$ to both sides. We then get

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

The right side of this equation is

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

which is $P(k+1)$. Hence $P(k+1)$ is true. Thus, by principle of induction, we see that Eq. 1 is true for all $n \in \mathbb{N}$. □

Ex. 4. For any positive integer n we have

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Ex. 5. $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$, for all $n \in \mathbb{N}$.

Example 6 (Bernoulli's Inequality)**.** Let $x \in \mathbb{R}$ such that $x > -1$. Then

$$(1+x)^n \geq 1 + nx, x > -1 \text{ and } n \in \mathbb{N}. \tag{2}$$

Let $P(n)$ be the statement Eq. 2.

If $k = 1$, $P(1)$ is clearly true. Assume that $P(k)$ is true. That is, we have $(1+x)^k \geq 1+kx$. Since $1 + x > 0$ we multiply both sides of the inequality by $1 + x$ and get

$$\begin{aligned}(1+x)^{k+1} = (1+x)(1+x)^k &\geq (1+x)(1+kx) \\ &\geq 1 + (k+1) + kx^2 \\ &\geq 1 + (k+1)x.\end{aligned}$$

This shows that $P(k+1)$ holds. Hence, by the principle of induction, Eq. 2 holds true for all $n \in \mathbb{N}$. □

Example 7. If $a_1, a_2, \ldots, a_n$ are positive integers relatively prime to another integer b, then their product $a_1 \cdots a_n$ is relatively prime to b.

Recall that we say two integers r and s are said to be relatively prime if the only positive integral divisor of both is 1. Equivalently, r and s are relatively prime iff there exist integers a and b such that $ar + bs = 1$.

What is $P(n)$ here? We let $P(n)$ be the statement that if we are given n integers whcih are relatively primt to b, so is their product.

$P(1)$ is certainly true by hypothesis. We now prove that $P(2)$ is also true. Let a_1 and a_2 be relatively prime to b. Then there exist integers x_j, y_j, $j = 1, 2$ such that $a_1x_1 + by_1 = 1$ and $a_2x_2 + by_2 = 1$. Multiplying these equations, we get

$$a_1a_2(x_1x_2) + b(a_1x_1y_2 + a_2x_2y_1) = 1.$$

This proves that a_1a_2 is relatively prime to b.

Assume that $P(k)$ is true. Let $a_1, \ldots, a_k, a_{k+1}$ be relatively prime to b. Since $P(k)$ is true, $a_1 \cdots a_k$ is relatively prime to b. Also, by assumption, a_{k+1} is relatively prime to b. By $P(2)$, the 0product $(a_1 \cdots a_k)a_{k+1}$ is relatively prime to b. That is, $P(k+1)$ holds. By induction principle, $P(n)$ holds true for all $n \in \mathbb{N}$. □

Remark 8. The crucial step in the above proof is to show that $P(2)$ holds. To appreciate this, do the next exercise.

Ex. 9. Find the fallacious step in the following argument. We prove by induction that any n things are the same. If $n = 1$ this is clear. Assume that any k things are the same. Let $x_1, x_2, \ldots, x_k, x_{k+1}$ be given. By induction hypothesis (that is another way of saying $P(k)$ is true) applied the the k things $a_1, \ldots, a_k$ we find that $a_1 = a_2 = \cdots = a_k$. Similarly, we conclude that $a_2 = a_3 = \cdots = a_k = a_{k+1}$. Hence $a_1 = a_2 = \cdots = a_k = a_{k+1}$. Hence by induction principle, given any n things, they are always the same.

Ex. 10. Show that the statement $2 + 2 + \cdots + 2n = (n+2)(n-1)$ for all $n \in \mathbb{N}$ satisfies the inductive step but has no basis.

Ex. 11. Show that for some values of n, $n^2 + n + 41$ is a prime number for some it is not, so that there is no inductive step which would show that $n^2 + n + 41$ is a prime number for all n.

Ex. 12. Derive the formula for the sum of first n terms of an arithmetic progression:

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

Ex. 13. Derive the formula for the sum of first n terms of a geometric progression:

$$a + (ar) + (ar^2) + \cdots + (ar^{n-1}) = \frac{a(r^{n-1})}{r - 1}, \qquad r \neq 1.$$

We now give a set of exercises for practice. In all these problems the statement is to be proved for all positive integers by induction.

Ex. 14. If $a \equiv b|m|$, then

$$a^n \equiv b^n|m|.$$

Ex. 15. $4^n \equiv 3n + 1|9|$.

Ex. 16. Fibonacci numbers. We define a sequence of numbers as follows: $f_1 = 1$, $f_2 = 1$ and $f_n = f_{n-2} + f_{n-1}$ for all $n \geq 3$. The number f_n is called the nth Fibonacci number.

Prove that, for each $n \in \mathbb{N}$, the following hold:

$$\begin{aligned} f_2 + f_4 + \cdots + f_{2n} &= f_{2n+1} - 1. \\ f_1 + f_3 + \cdots + f_{2n-1} &= f_{2n}. \\ f_1 + f_2 + \cdots + f_n &= f_{n+2} - 1 \\ f_n &< 2^n. \end{aligned}$$

Ex. 17. If A is the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, then $A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$, for all $n \in \mathbb{N}$.