Script 0

The Natural Numbers and Mathematical Induction

0.1 Responses

10/1: **Exercise 0.2** (PMI Exercise 2)**.** Prove that if $x > -1$, then $(1+x)^n \geq 1+nx$ for any natural number n. (Note that although this script is focused on the natural numbers, your argument should hold for any real number $x > -1$.)

Proof. We induct on n. For the base case $k = 1$, we have $(1+x)^1 = 1+x \geq 1+(1)x$, where the greater than or equal to relation could be strengthened to equality but will be left as such for the sake of the argument. Now suppose inductively that we have proven the claim for some natural number k, i.e., we know that $(1+x)^k \geq 1+kx$ if $x > -1$. We now seek to prove it for $k+1$. To begin, we have

$$(1+x)^{k+1} = (1+x)^k(1+x)$$

by the laws of exponents. By the inductive hypothesis and the fact that $ac \geq bc$ if and only if a, b, c are positive numbers and $a \geq b$ (note that $x > -1$ implies $1+x > 0$ along with $(1+x)^k > 0$), we have that the above is

$$\geq (1+kx)(1+x)$$

Now expand and simplify.

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

Since x^2 must be positive or zero and $k \in \mathbb{N}$ is clearly positive, we have that $kx^2 \geq 0$ so that the above is

$$\geq 1+(k+1)x$$

thus closing the induction. □

Additional Exercises

10/13:

1. Prove that if A is a non-empty subset of $\mathbb{N}$, then A has a least element, i.e., there is some $n_0 \in A$ such that for all $n \in A$, we have $n_0 \leq n$.
2. Prove the following variants of the Principle of Mathematical Induction:
   (a) For each $n \in \mathbb{N}$, let $P(n)$ be a proposition and let n_0 be some natural number. Suppose the following two results:

(A) $P(n_0)$ is true.

(B) If $P(k)$ is true, then $P(k+1)$ is also true.

Then $P(n)$ is true for all natural numbers n such that $n \geq n_0$.

(b) For each $n \in \mathbb{N}$, let $P(n)$ be a proposition. Suppose the following two results:

(A) $P(1)$ is true.

(B) If $P(r)$ is true for all r such that $1 \leq r \leq k$, then $P(k+1)$ is true.

Then $P(n)$ is true for all natural numbers n.

10/8: 7. Let n be a natural number and $k \leq n$ also be a natural number. Define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

where $k! = 1 \times 2 \times \cdots \times k$. Show that

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

for all $n \in \mathbb{N}$.

Proof. We begin with a lemma proving some basic properties of combinations.

Lemma. *Let n be a natural number and $k \leq n$ also be a natural number. Define*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

where $k! = 1 \times 2 \times \cdots \times k$. Then

a) $\binom{n}{0} = 1$ *for all* $n \in \mathbb{N}$*;*

b) $\binom{n}{n} = 1$ *for all* $n \in \mathbb{N}$*;*

c) $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ *for all natural numbers* n *and* $1 \leq k \leq n$*.*

Proof of Lemma 1. We will address each of the three parts of the lemma in turn.

For part (a), we know by the definition of $\binom{n}{k}$ that $\binom{n}{0} = \frac{n!}{0!(n-0)!}$ and by the definition of a factorial that $\frac{n!}{0!(n-0)!} = \frac{1 \cdot n!}{n!} = 1$. Thus, $\binom{n}{0} = 1$, as desired.

For part (b), we proceed in a similar manner to the above: $\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n! \cdot 1} = 1$.

For part (c), we repeatedly apply the definition of $\binom{n}{k}$ and of a factorial in the following algebra. Note that we proceed from the right side of the equality we seek to prove since it makes the algebra flow more logically (via simplification rather than expansion).

$$\begin{aligned}
\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k(k-1)!(n-k)!} \\
&= \frac{n!}{(k-1)!(n-k+1)(n-k)!} + \frac{n!}{k(k-1)!(n-k)!} \\
&= \frac{k \cdot n!}{k(k-1)!(n-k+1)(n-k)!} + \frac{(n-k+1)n!}{k(k-1)!(n-k+1)(n-k)!} \\
&= \frac{k \cdot n! + (n-k+1)n!}{k(k-1)!(n-k+1)(n-k)!}
\end{aligned}$$

$$= \frac{k \cdot n! + (n+1)n! - k \cdot n!}{k!(n-k+1)!}$$
$$= \frac{(n+1)n!}{k!(n+1-k)!}$$
$$= \frac{(n+1)!}{k!((n+1)-k)!}$$
$$= \binom{n+1}{k}$$

□

Now we begin to address the question in earnest by inducting on n. For the base case $n = 1$, begin with the left side of the equality we wish to verify and employ the definition of exponents.

$$(x+y)^1 = x + y$$

Now use a couple of "clever forms of 1," which we can, of course, multiply to the terms in the above equation and still preserve equality.

$$= \frac{1!}{0!(1-0)!}x^1y^0 + \frac{1!}{1!(1-1)!}x^0y^1$$

Now just employ the definition of $\binom{n}{k}$ and use summation notation to simplify the expression.

$$= \binom{1}{0}x^{1-0}y^0 + \binom{1}{1}x^{1-1}y^1$$
$$= \sum_{k=0}^{1}\binom{1}{k}x^{1-k}y^k$$

This proves the base case. Now suppose inductively that we have proven the claim for some natural number n, i.e., we know given the definitions in the question that $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$. We wish to prove the claim for $n+1$, which can be done as follows. Once again, begin with the left side of the equality we wish to prove and employ a rule of exponents.

$$(x+y)^{n+1} = (x+y)^1(x+y)^n$$

Now substitute using the induction hypothesis.

$$= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$

Distribute the summation to each term in $x+y$, and then "distribute" x and y into the general term of the summation.

$$= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k + y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$$
$$= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}$$

Reindex the second summation (instead of iterating from 0 to n, iterate from 1 to $n+1$ [the same number of terms] and subtract 1 from each instance of the index variable k). Note that this does not change the sum at all; it just changes how the sum is written. After the reindexing, algebraically manipulate the exponents into an equivalent form that matches the exponents in the other summation.

$$= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{n-(k-1)}y^{(k-1)+1}$$
$$= \sum_{k=0}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{(n+1)-k}y^k$$

Separate the first term of the left summation and the last term of the right summation from the summation notation.

$$= \binom{n}{0}x^{n+1}y^0 + \sum_{k=1}^{n}\binom{n}{k}x^{(n+1)-k}y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{(n+1)-k}y^k + \binom{n}{n}x^0y^{n+1}$$

Now that the sums are once again indexed alike, combine them and do some algebraic manipulations to set up a substitution.

$$= \binom{n}{0}x^{n+1}y^0 + \sum_{k=1}^{n}\left(\binom{n}{k}x^{(n+1)-k}y^k + \binom{n}{k-1}x^{(n+1)-k}y^k\right) + \binom{n}{n}x^0y^{n+1}$$
$$= \binom{n}{0}x^{n+1}y^0 + \sum_{k=1}^{n}\left(\binom{n}{k} + \binom{n}{k-1}\right)x^{(n+1)-k}y^k + \binom{n}{n}x^0y^{n+1}$$

In the first term, use Lemma 1a to make the substitution $\binom{n}{0} = 1 = \binom{n+1}{0}$. In the last term, use Lemma 1b to make the substitution $\binom{n}{n} = 1 = \binom{n+1}{n+1}$. In the summation, use Lemma 1c to make the substitution $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ (notice how k varies between 1 and n in the summation, just like it is allowed to in the statement of Lemma 1c).

$$= \binom{n+1}{0}x^{n+1}y^0 + \sum_{k=1}^{n}\binom{n+1}{k}x^{(n+1)-k}y^k + \binom{n+1}{n+1}x^0y^{n+1}$$

Expand the limits of the summation to encompass the first and last terms.

$$= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{(n+1)-k}y^k$$

This closes the induction. □

10/15: 8. Let $a, b \in \mathbb{Z}$. We say that b is **divisible** by a if there is an integer m such that $b = ma$. It is easily shown that

i) if both b_1 and b_2 are divisible by a, then so is their sum;

ii) if b is divisible by a, then so is kb for any integer k.

10/8: 9. From Peano's Postulates (below), prove the following claims.

Axioms (Peano's Postulates)**.** *The natural numbers are defined as a set* $\mathbb{N}$ *together with a unary "successor" function* $S : \mathbb{N} \to \mathbb{N}$ *and a special element* $1 \in \mathbb{N}$ *satisfying the following postulates.*

I. $1 \in \mathbb{N}$.

II. If $n \in \mathbb{N}$*, then* $S(n) \in \mathbb{N}$.

III. There is no $n \in \mathbb{N}$ *such that* $S(n) = 1$.

IV. If $n, m \in \mathbb{N}$ *and* $S(n) = S(m)$*, then* $n = m$.

V. If $A \subset \mathbb{N}$ *is a subset satisfying the two properties:*

- $1 \in A$*;*
- *if* $n \in A$*, then* $S(n) \in A$*;*

then $A = \mathbb{N}$.

(a) **Bonus exercise**. Show that

$$\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \cdots\}$$

Proof. We wish to eventually use Axiom V to show that the set on the right side of the above equality (which we shall call A) is equal to $\mathbb{N}$. Thus, we begin by demonstrating that A is a subset of $\mathbb{N}$. To do so, we must verify that every element of A is an element of $\mathbb{N}$. Now A consists of 1 and elements in the codomain of S, so since $1 \in \mathbb{N}$ (Axiom I) and any element of the codomain of S is clearly an element of $\mathbb{N}$ (because the codomain of S *is* $\mathbb{N}$), $A \subset \mathbb{N}$. Moving on, as previously referenced, $1 \in A$, so the first property of Axiom V holds. Additionally, the pattern defining A clearly indicates that for any $a \in A$, $S(a) \in A$, so the second property of Axiom V holds. Therefore, by Axiom V, $A = \mathbb{N}$. □

(b) Prove that the Principle of Mathematical Induction follows from Peano's Postulates.

Proof. We wish to prove, using only Axioms I-V above and set theoretic results, that if $P(n)$ is a proposition pertaining to each natural number n, $P(1)$ is true, and the truth of $P(k)$ implies that $P(S(n))$[1] is also true, then $P(n)$ is true for all natural numbers n. We will do this by defining a set A such that "$P(n)$ is true" is logically equivalent to $n \in A$. Then if we can show that $n \in A$ for all $n \in \mathbb{N}$ (i.e., that $A = \mathbb{N}$), we will have verified that $P(n)$ is true for all $n \in \mathbb{N}$ as desired. Lastly, note that we will show that $A = \mathbb{N}$ by demonstrating that A satisfies the stipulations of Axiom V. Let's begin.

Let $A = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$. Since every element of A is an element of $\mathbb{N}$ by the definition of A, $A \subset \mathbb{N}$. Additionally, since $P(1)$ is true by hypothesis and $1 \in \mathbb{N}$ by Axiom I, we know by the definition of A that $1 \in A$. Now suppose $n \in A$. It follows that $n \in \mathbb{N}$ and $P(n)$ is true. But by hypothesis, the truth of $P(n)$ implies that $P(S(n))$ is true. This, combined with the fact that $S(n) \in \mathbb{N}$ by Axiom II, shows that $S(n) \in A$. Having now proven that $A \subset \mathbb{N}$, $1 \in A$, and $n \in A$ implies $S(n) \in A$, Axiom V tells us that $A = \mathbb{N}$, as desired. □

(c) Define a special element $0 \notin \mathbb{N}$ and define $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Let $s : \mathbb{N}_0 \to \mathbb{N}$ be defined by

$$s(0) = 1$$
$$s(n) = S(n), \text{ for } n \in \mathbb{N}$$

where S is the successor function defined in Peano's Postulates.

Definition. We define addition $x + y$ for $x, y \in \mathbb{N}_0$ inductively on y by

$$x + 0 = x$$
$$x + s(y) = s(x + y)$$

Theorem. *The following facts all hold.*

i. *If $x, y \in \mathbb{N}_0$, then $x + y \in \mathbb{N}_0$.*
ii. *$0 + x = x$, for all $x \in \mathbb{N}_0$.*
iii. *(Commutative Law) $x + y = y + x$ for all $x, y \in \mathbb{N}_0$.*
iv. *(Associative Law) $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{N}_0$.*
v. *Given $x, y, z \in \mathbb{N}_0$, if $x + y = x + z$, then $y = z$.*

Prove that $x+1 = s(x)$ for all $x \in \mathbb{N}_0$ and then prove items (i), (ii), and (iv) in the above theorem.

Proof of first claim. Since $1 = s(0)$ by definition, we know by repeated applications of the various parts of the definition of addition that $x + 1 = x + s(0) = s(x + 0) = s(x)$, as desired. □

Proof of i. We keep x fixed and induct on y. For the base case $y = 0$, we have by the definition of addition that $x + 0 = x$. Since $x \in \mathbb{N}_0$ by assumption, it clearly follows that $x + 0 \in \mathbb{N}_0$, thus proving the base case. Now suppose inductively that we have proven that $x + y \in \mathbb{N}_0$ for some $y \in \mathbb{N}_0$; we now seek to prove that $x + (y + 1) \in \mathbb{N}_0$. By the above argument, $y + 1 = s(y)$, so

$$x + (y + 1) = x + s(y)$$

[1] Addition has not yet been defined. Although we do not yet "know" that $n + 1 = S(n)$ we must assume it for the sake of this proof.

It follows by the definition of addition that the above

$$= s(x + y)$$

Since $s : \mathbb{N}_0 \to \mathbb{N}$ and $x+y \in \mathbb{N}_0$ by hypothesis, $s(x+y) \in \mathbb{N}$. Thus, $x+(y+1) \in \mathbb{N}$. Consequently, $x + (y + 1) \in \mathbb{N} \cup \{0\}$, implying by the definition of $\mathbb{N}_0$ that $x + (y + 1) \in \mathbb{N}_0$. This closes the induction. □

Proof of ii. We induct on x. For the base case $x = 0$, we have by the definition of addition that $0+0 = 0$, thus proving the base case. Now suppose inductively that we have proven that $0+x = x$ for some $x \in \mathbb{N}_0$; we now seek to prove that $0 + (x + 1) = x + 1$. As before, we can write that

$$\begin{aligned} 0 + (x + 1) &= 0 + s(x) \\ &= s(0 + x) \end{aligned}$$

But by the inductive hypothesis and the first claim proven herein, it follows that the above

$$\begin{aligned} &= s(x) \\ &= x + 1 \end{aligned}$$

This closes the induction. □

Proof of iv. We induct on x (keeping y, z fixed). For the base case $x = 0$, we must consider $0 + (y + z)$. By part (i), $y + z \in \mathbb{N}_0$. Thus, part (ii) applies, and implies that

$$0 + (y + z) = y + z$$

Since $y \in \mathbb{N}_0$ by assumption, we can apply part (ii) again in reverse to demonstrate that $y = 0+y$. Thus, the above is

$$= (0 + y) + z$$

This proves the base case. Now suppose inductively that we have proven that $x+(y+z) = (x+y)+z$ for some $x \in \mathbb{N}_0$; we now seek to prove that $(x + 1) + (y + z) = ((x + 1) + y) + z$. As before,

$$(x + 1) + (y + z) = s(x) + (y + z)$$

By part (iii) (which implies that $s(y)+x = s(y+x)$ is also true), the fact that $y+z \in \mathbb{N}_0$ by part (i), and the definition of addition, we thus have that the above

$$= s(x + (y + z))$$

We now apply the inductive hypothesis.

$$= s((x + y) + z)$$

By the fact that $x + y \in \mathbb{N}_0$ (part i) and consecutive applications of the definition of addition, we find that the above

$$\begin{aligned} &= s(x + y) + z \\ &= (s(x) + y) + z \end{aligned}$$

To finish it off, we once again use the first claim proved herein:

$$= ((x + 1) + y) + z$$

This closes the induction. □

(d) **Definition.** We define multiplication $x \cdot y$ for $x, y \in \mathbb{N}_0$ inductively on $\mathbb{N}_0$ by

$$x \cdot 0 = 0$$
$$x \cdot s(y) = x \cdot y + x$$

Prove that $x \cdot 1 = x$ for all $x \in \mathbb{N}_0$.

Proof. Since $s(0) = 1$,

$$x \cdot 1 = x \cdot s(0)$$

By the definition of multiplication, the above is

$$= x \cdot 0 + x$$

From the above, we can use the definition of multiplication to substitute $x \cdot 0 = 0$.

$$= 0 + x$$

Now just apply part (ii) of the Theorem in part (c).

$$= x$$

□

(e) **Definition.** We define $<$ on $\mathbb{N}_0$ by

$$x < y \text{ if and only if } y = x + u \text{ for some } u \in \mathbb{N}.$$

i. Prove that $1 < n$ for all $n \in (\mathbb{N} \setminus \{1\})$.

ii. Prove that if $a, x, y \in \mathbb{N}$ with $x < y$, then $a \cdot x < a \cdot y$.

Proof of i. We induct on n. For the base case $n = 2$, we have $2 = s(1 + 0) = 1 + s(0) = 1 + 1$, so $1 < 2$. Now suppose inductively that $1 < n$ for some $n \in \mathbb{N}$; we wish to prove that $1 < n + 1$. By the induction hypothesis and the definition of $<$, $n = 1 + u$. Thus, $n + 1 = 1 + u + 1$ by the inverse of the cancellation law for addition. Since $u + 1 \in \mathbb{N}$ by part (c) Theorem part (i), we have that $n + 1 = 1 + (u + 1)$, implying that $1 < n + 1$. This closes the induction. □

Proof of ii. We induct on a (keeping x, y fixed). For the base case $a = 1$, we have by part (d) that $x < y$ is equivalent to $1 \cdot x < 1 \cdot y$ since $x = 1 \cdot x$ for all $x \in \mathbb{N}$. Now suppose inductively that we have proven that $a \cdot x < a \cdot y$; we wish to prove that $(a + 1) \cdot x < (a + 1) \cdot y$. Let's start with

$$a \cdot x < a \cdot y$$

By the definition of $<$, we know that this implies

$$a \cdot y = a \cdot x + u$$

By the inverse of the cancellation law for addition, we can add a quantity to both sides, say y.

$$a \cdot y + y = a \cdot x + y + u$$

Since $x < y$ by assumption, $y = x + u'$ for some $u' \in \mathbb{N}$.

$$a \cdot y + y = a \cdot x + x + u' + u$$

Use the definition of multiplication and addition.

$$s(a) \cdot y = s(a) \cdot x + u' + u$$
$$(a + 1) \cdot y = (a + 1) \cdot x + u' + u$$

If we treat $u' + u$ as a single natural number, which we can do because of part (c) Theorem part i, we can employ the definition of $<$ one more time.

$$(a + 1) \cdot x < (a + 1) \cdot y$$

□

10/6: (f) **Definition.** For $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$, we define n^k inductively by

$$n^0 = 1$$
$$n^{k+1} = n \cdot n^k$$

i. Prove that $n < n^2$ for all $n \in \mathbb{N} \setminus \{1\}$.

ii. Prove that $n^k < n^{k+1}$ for all $n \in \mathbb{N} \setminus \{1\}$.