

NATURAL NUMBERS

We are ready for the *official* introduction of the natural numbers. I ask you to *suspend belief* in the truth of the things you already know about the natural numbers, but not to lose one bit of your knowledge — just stop taking things for granted. “The Natural Numbers” now becomes a name only, to be used in the following list of mathematical statements, each of which you are asked to regard as true.

This is where the course “really” starts; what came before was “preliminaries,” and we still have some preliminary stuff to do — more about sets and topology. But the natural numbers will literally be the foundation on which we will build the ordinary integers, the rational numbers, and then the real and the complex numbers, which in turn form the “floor” for Calculus.

(5.01) The Peano Postulates (or Axioms)

Here are the Peano Postulates, phrased in a way that lets you use what you have learned so far:

We assume that the four following mathematical statements are true.

(5.01A) There exists a non-empty set \mathbf{N} , whose elements we will call **natural numbers**.

(5.01B) There exists a one-to-one function $s : \mathbf{N} \rightarrow \mathbf{N}$, that we will call the **successor function**.

(5.01C) There exists an element $0 \in \mathbf{N}$ such that 0 is not in the image, $s(\mathbf{N})$, of s .

(5.01D) For all subsets S of \mathbf{N} , if S contains 0 , and $s(S) \subseteq S$, then $S = \mathbf{N}$.

Here is a restatement of these axioms, in a less dense form:

(5.02-1) There exists a non-empty set \mathbf{N} , called the set of natural numbers, and a function s on \mathbf{N} , called the successor function, whose value, $s(n)$, at any n in \mathbf{N} , is called the **successor of n** , such that

(5.02-2) Different elements of \mathbf{N} have different successors (s is one-to-one),

(5.02-3) There is an element, 0 , of \mathbf{N} that is not the successor of any element of \mathbf{N} (0 is not in the image of s),

(5.02-4) Every subset of \mathbf{N} that contains 0 and also contains the successor of each of its elements must be equal to \mathbf{N} (if S contains 0 , and $s(S) \subseteq S$, then $S = \mathbf{N}$).

According to the Encyclopedia Britannica, 15th edition,¹ the five Peano postulates are:

1. 0 is a number.
2. The successor of any number is also a number.
3. No two distinct numbers have the same successor.
4. 0 is not the successor of any number.
5. If any property is possessed by 0 and also by the successor of any number having that property, then all numbers have that property.

Postulate 5 is different than (5.01D), and is different than (5.02-4).

But all three versions amount to the same thing, when expressed in terms of set-selector notation.

For, “property” has to refer to a mathematical statement $P(n)$ about elements n of \mathbf{N} .

Thus, $\{ n \in \mathbf{N} : P(n) \text{ is true } \}$ is the set of all elements of \mathbf{N} that possess the property $P(n)$.

If the “property” satisfies the conditions of postulate 5, then $0 \in \{ n \in \mathbf{N} : P(n) \text{ is true } \}$, and $s(\{ n \in \mathbf{N} : P(n) \text{ is true } \}) \subseteq \{ n \in \mathbf{N} : P(n) \text{ is true } \}$, so $\{ n \in \mathbf{N} : P(n) \text{ is true } \} = \mathbf{N}$.

On the other hand, let S be a subset of \mathbf{N} .

Then we define the “property (of n)” to be that n belongs to S .

That is, $P(n)$ is the statement “ $n \in S$.” This “property” is then covered by postulate 5.

Postulate 5 is about *sets* of natural numbers. You probably did not bring this postulate with you to this course, at least not explicitly. And yet, it will seem natural to you shortly, I hope. Here are the three versions of Postulate 5, collected in one place:

For all subsets P of \mathbf{N} , if P contains 0, and $s(P) \subseteq P$, then $P = \mathbf{N}$;

Every subset of \mathbf{N} that contains 0 and also contains the successor of each of its elements must be equal to \mathbf{N} ;

If any property is possessed by 0 and also by the successor of any number having that property, then all numbers have that property.

This Postulate is called **The Principle of Mathematical Induction**.

The Principle of Mathematical Induction is our principal source of “mathematical energy!”

¹Volume 23, page 275

We usually don't make axioms in a vacuum — there is usually some thought behind them. But that thought can be hidden! So here is an “explanation” of the axioms. First, let's imagine that we go into the “back room,” where we don't have to prove anything — just work on ideas! We “know” the integers exist, positive, zero and negative. The natural numbers are going to be our model of the non-negative integers. The successor function is “really” the function whose value at n , $n \geq 0$, is $n + 1$: $s(n) = n + 1$. Different non-negative integers “should” have different successors. This is what “ s is one-one” means. This is an *assumption* about the successor function! Saying 0 is not the successor of any non-negative integer means that $0 \neq n + 1$ for any *non-negative* integer n . The postulate about **sets** of non-negative integers is not something we usually take for granted. But the idea makes sense: if a set S contains 0 , and contains the successor of each of its elements, then it also contains 1 , and 2 , and 3 , and so on. So it ought to contain every non-negative integer, namely $S = \mathbf{N}$.

In your experience, perhaps \mathbf{N} starts with 1 , not 0 . There is an equivalent version of these axioms for that version of \mathbf{N} . We simply replace each “ 0 ” in the first version with “ 1 ,” and call the new set \mathbf{P} , for positive integers. We will want to use induction “starting with 1 .” But, instead of making another set of axioms, we will give the name 1 to $s(0)$, and then we can *deduce* the proposed axioms, from the Peano Postulates, so they become a theorem: a set of true mathematical statements whose truth is logically deduced from axioms, instead of being *assumed*.

(5.03) Theorem and Definition and Notation: There is a non-empty set \mathbf{P} , whose elements we will call **positive integers**, a one-to-one function $s: \mathbf{P} \rightarrow \mathbf{P}$, that we will call the **successor function**, and an element $1 \in \mathbf{P}$ such that 1 is not in the image, $s(\mathbf{P})$, of s . In addition, for all subsets E of \mathbf{P} , if E contains 1 , and $s(E) \subseteq E$, then $E = \mathbf{P}$.

The idea of the proof is to remove 0 from \mathbf{N} to construct \mathbf{P} . Then we have to check that each of the postulates can be re-interpreted in the new set. The Induction property will be deduced by temporarily putting 0 back, then taking it out after applying the Principle of Mathematical Induction for \mathbf{N} .

Proof: Let $\mathbf{P} := \mathbf{N} \sim \{0\}$. We now construct $s: \mathbf{P} \rightarrow \mathbf{P}$ by $s(n) = s(n)$ for every n in \mathbf{P} . Does this make sense? Yes; \mathbf{P} is a subset of \mathbf{N} , so $s(n)$ is defined for all n in \mathbf{P} . The problem is, is every value of s in \mathbf{P} , or at least are all the values that s takes on, for n in \mathbf{P} , in \mathbf{P} ? The answer is “yes,” because the only element of \mathbf{N} that is not in \mathbf{P} is 0 , and 0 is not in $s(\mathbf{N})$, by axiom (5.02-3), hence 0 is also not in $s(\mathbf{P})$. The new function s , new because its domain is different (smaller), is still one-to-one. Now 1 is not in the image of the new s , because 1 is the

image of 0, by definition, and 0 has been removed, and s is one-one, so 1 is not the image of any other element of \mathbf{N} , much less \mathbf{P} . Therefore, 1 is not $s(n)$ for any n in \mathbf{P} .

Since $1 = s(0)$, and 0 is not in \mathbf{P} , and s is 1-1, $s(n) = 1$ means $s(n) = s(0)$, so $n = 0$ if $s(n) = 1$. But 0 is not in \mathbf{P} . The idea of this proof could be applied to the set of all natural numbers starting with 10, or 17, or any other, instead of 1, like \mathbf{P} .

To prove that the Principle of Mathematical Induction is true for \mathbf{P} , suppose that E is a subset of \mathbf{P} , E contains 1, and $s(E) \subseteq E$.

We have to show that $E = \mathbf{P}$. We will work in \mathbf{N} !

Construct a subset F of \mathbf{N} by assignment: $F := E \cup \{0\}$.

We're back in \mathbf{N} now!

Now **0 is in F** , by construction, and

$$\begin{aligned} s(F) &= s(E \cup \{0\}) = s(E) \cup s(\{0\}) \quad (\text{by (4.26b)}) \\ &= s(E) \cup \{s(0)\} = s(E) \cup \{1\} \subseteq E \cup \{1\} = E \quad (\text{because } 1 \in E) \\ &\subseteq F \quad (\text{by construction}). \end{aligned}$$

By transitivity of set inclusion, $s(F) \subseteq F$.

By the Principle of Mathematical Induction, $F = \mathbf{N}$.

Now $F = E \cup \{0\}$ and $\mathbf{N} = \mathbf{P} \cup \{0\}$.

Also, $E \cap \{0\} = \emptyset$ and $\mathbf{P} \cap \{0\} = \emptyset$.

Therefore, $E = F \sim \{0\} = \mathbf{N} \sim \{0\} = \mathbf{P}$ (why?).

Thus $E = \mathbf{P}$, as desired.

You have probably seen Mathematical Induction before, but it looked a little different then.

Example: Use Mathematical Induction (school version) to show that for all positive integers n , $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$. In this Example, we will use your prior knowledge about \mathbf{P} .

The procedure is this: 1. Let $P(n)$ denote the statement to be proved: $P(n)$ must have n as its only free variable.

2. Verify that $P(1)$ is true.

3. Show that, by *assuming* $P(n)$ is true, you can deduce that $P(n+1)$ must be true.

That is, prove the *quantified* mathematical statement "For all n in \mathbf{N} , $P(n) \Rightarrow P(n+1)$."

Then Mathematical Induction assures us that $P(n)$ is true for all n .

Let's do it, for review.

Step 1. Let $P(n)$ denote the statement " $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$."

Step 2. $P(1)$ is the statement " $1 = \frac{1(1+1)}{2}$." This is true, by a very quick computation.

Step 3. Assume that $P(n)$ is true for some n . Then $P(n+1)$ is the statement " $1 + 2 + 3 + \dots + (n+1) = \frac{(n+1)(n+2)}{2}$."

We have $1 + 2 + 3 + \dots + (n+1) = 1 + 2 + 3 + \dots + n + (n+1) = (1 + 2 + 3 + \dots + n) + (n+1) = \frac{n(n+1)}{2} + 2 \frac{n+1}{2} = \frac{(n+1)(n+2)}{2}$, by a few basic algebraic manipulations. The equality of the first and last expressions in this chain of equalities is $P(n+1)$, shown to be true under the assumption that $P(n)$ is true. The truth of $P(n)$ for all n is now established, by **Mathematical Induction**. Note that, were $P(n)$ false, the statement $P(n) \Rightarrow P(n+1)$ would be true vacuously.

The way we will often "do" Mathematical Induction differs only a little from this (and you may certainly use the old way in your papers in this class). The set-theoretic version of this argument goes something like this:

Let $E := \{ n \in \mathbf{P} : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} \}$. Then we show $1 \in E$ (as we did), and that $n \in E$ implies $n+1 \in E$ (as we did). Then $E = \mathbf{P}$ by **Mathematical Induction**.

You will need to learn new ways to use (the Principle of) Mathematical Induction. You are probably familiar with Mathematical Induction as a tool for verifying formulas. We will need to use Mathematical Induction for other purposes. For example, we will need to know whether certain kinds of functions from \mathbf{N} to \mathbf{N} exist, and there may be one function for each n , or maybe our statement will be that there is NO such function, for ANY n . We will then construct a set

$$S := \{ n \in \mathbf{N} : \text{a function } f_n : \mathbf{N} \rightarrow \mathbf{N} \text{ exists such that "thus and so" is true about } f_n \}.$$

Then we will follow the "same" pattern as school induction:

Step 0: Show that 0 is in S. The way we show that 0 is in S will of course depend on what the criterion is for membership in S . But the *objective* of Step 0 is always the same.

Step 1: Let someone choose an *arbitrary* element n of \mathbf{N} , and then **show that** the statement

$$"n \in S \Rightarrow s(n) \in S" \text{ is true.}$$

This is the objective of Step 1, then: show that $(\forall n \in \mathbf{N})(n \in S \Rightarrow s(n) \in S)$ is true.

Since this is a statement with a universal quantifier, we have to be able to show that every one of the statements $(n \in S \Rightarrow s(n) \in S)$ is true. We know by now that there is one easy way for this statement to be true: in case $(n \in S)$ is false! We usually don't mention this possibility; we just assume that $(n \in S)$ is true. Then we try to use the truth of $(n \in S)$ to deduce the truth of

$(s(n) \in S)$. *But we can't always work that way!* Sometimes we have to use the *contrapositive* of $(n \in S \Rightarrow s(n) \in S)$, namely $(s(n) \notin S \Rightarrow n \notin S)$. That is, we assume that $(s(n) \notin S)$ is true. Then we try to use the truth of $(s(n) \notin S)$ to deduce the truth of $(n \notin S)$. This second approach is logically equivalent to the first way, but it not *psychologically* the same! Step 1 is the “heart” of an induction proof. But Step 0 is essential!

Step 3: We apply the Principle of Mathematical Induction by noting that the $S = \mathbf{N}$. This step is one you sort of do automatically; it's like a coda in a piece of music...

(5.04) Example: Let's prove that $s(\mathbf{N}) = \mathbf{P}$.

That is, let's show that every n in \mathbf{P} is $s(m)$ for some m in \mathbf{N} .

We have already seen, in the proof of Theorem (5.03), that $s(\mathbf{N}) \subseteq \mathbf{P}$.

To show equality, it remains to show that $\mathbf{P} \subseteq s(\mathbf{N})$.

We do already know of one element of \mathbf{P} that is in $s(\mathbf{N})$, namely $1 = s(0)$.

Thus $1 \in \{ n \in \mathbf{P} : \text{there exists } m \in \mathbf{N} \text{ such that } n = s(m) \} =: E$.

We will use induction for \mathbf{P} instead of \mathbf{N} . We already did Step 0 (or ought it be Step 1, for \mathbf{P} ?)!

We need to show that, for all n in \mathbf{P} , “ $n \in E \Rightarrow s(n) \in E$ ” is true.

Well, “ $n \in E \Rightarrow s(n) \in E$ ” is true if “ $n \in E$ ” is false.

Since “ $n \in E$ ” has to be true or false, we have to see what happens if “ $n \in E$ ” is true.

So, next suppose that “ $n \in E$ ” is true.

Now, “ $n \in E$ ” means that there exists $m \in \mathbf{N}$ such that $n = s(m)$.

But then, $s(n) = s(s(m))$, by the Substitution Rule.

The Substitution Rule is tricky. We have to set up the “right” statement. Let's make $P(x) :=$ “ $s(x) = s(s(m))$.” Then, putting $x := s(m)$ yields: $P(s(m))$ is true. NOW we can apply the Substitution Rule: since $n = s(m)$, $P(n)$ is true. And $P(n)$ is “ $s(n) = s(s(m))$,” as desired.

Thus, $s(n) \in E$.

Then, by Mathematical Induction (*set* version, for \mathbf{P}), $E = \mathbf{P}$. In other words, every n in \mathbf{P} is the successor of some m in \mathbf{N} , as desired.

If you have time, I recommend that you read *Foundations of Analysis*, by Edmund Landau, Chelsea Publishing Co., New York, 1951. Despite the author's request, *do* read the preface for the teacher. Read the preface for the student too, and the book too, a little bit at a time. What Landau does is to carefully develop the properties of the positive integers from the axioms (the version for \mathbf{P}). Here are some exercises, adapted from theorems in that book. In these exercises, do not use your prior knowledge, just use the axioms.

(5.05) Exercise: Show that, for all n in \mathbf{N} , and for all m in \mathbf{N} , if $n < m$ then

$s(n) = s(m)$.

(5.06) Problem: Show that, for all n in \mathbf{N} , $s(n) = n$. You will need induction!

(5.07) Exercise: Show that, for all n in \mathbf{N} , if $n > 0$ then there exists exactly one m in \mathbf{N} such that $n = s(m)$. You may need induction!

(5.08) Notation: If $n \in \mathbf{N}$ and $n > 0$ we let $n-1$ denote the unique m in \mathbf{N} (provided by (5.07)) such that $n = s(m)$. That is, $n = s(n-1)$.

An important point: $n-1$ does not exist for all n in \mathbf{N} ; $n-1$ exists only for $n > 0$. This is not subtraction! The meaning of $n-1$ is “predecessor of n .”

Theorem 4 in Landau’s book is also a definition, that of addition, defined in terms of the successor function. This theorem is mentioned as part of an interesting “confession” in the preface to the teacher. The proof is hard to follow. Here it is, paraphrased to fit \mathbf{N} instead of \mathbf{P} :²

(5.09) Theorem and Definition (of) and notation (for) (on addition): There exists one and only one function $p: \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ with the following properties (p is for “plus”):

(A) for all n in \mathbf{N} , $p(n, 0) = n$,

(B) for all n in \mathbf{N} , and for all m in \mathbf{N} , $s(p(n, m)) = p(n, s(m))$.

We call finding the value of $p(n, m)$ **addition of n and m** , and we call the value of $p(n, m)$ **the sum of n and m** . We use the notation $n + m := p(n, m)$.

The ordered pairs that comprise the function p have first members that are themselves ordered pairs! For example, $((1, 0), 1)$ and $((1, 1), 2)$ are in p .

Landau proves this Theorem in two main steps. First, he shows that there is at most one function that has properties **(A)** and **(B)**. This is the “only one” part of the proof; this may strike you as odd, because we don’t know yet whether there is any such function! The point is that we *assume* there are two such functions, and then show they must be equal functions! This is the standard way to approach a proof of uniqueness: assume there are two objects with all the properties under study, and then show that the two objects must be equal to each other.

²Thm 4, page 4.

Proof:

Uniqueness part: Suppose that p and q are two functions that satisfy **(A)** and **(B)**.

We will show that, for each n_0 in \mathbf{N} , given and *fixed*, $p(n_0, m) = q(n_0, m)$ for all m in \mathbf{N} .

I'm often going to write "for all m " as a short version of "for all m in \mathbf{N} ."

We will use Mathematical Induction (the *set* version).

We'll define a set S that consists of all the m 's such that $p(n_0, m) = q(n_0, m)$.

Then we'll set out to show, using Mathematical Induction, that $S = \mathbf{N}$.

This will show that $p(n_0, m) = q(n_0, m)$ for all m .

But then, since n_0 was *arbitrary*, it'll also be true that for all n , $p(n, m) = q(n, m)$ for all m .

This is what we mean by equality of functions of two variables. Now, let's do the proof!

Let S denote the set of all m such that $p(n_0, m) = q(n_0, m)$. In set selector notation,

$$S := \{ m \in \mathbf{N} : p(n_0, m) = q(n_0, m) \}.$$

Let us show that 0 is in S .

By **(A)**, $p(n, 0) = n$ for all n , and by **(A)**, $q(n, 0) = n$ for all n .

Thus, for our fixed n , namely n_0 , we have $p(n_0, 0) = q(n_0, 0)$.

This means that 0 is in S .

Now suppose that m is in S (that is, m is the name of an element in S . We don't know which m).

This means that $p(n_0, m) = q(n_0, m)$.

We want to show that $s(m)$ is in S . This means we have to show that

$$p(n_0, s(m)) = q(n_0, s(m)).$$

Since $p(n_0, m) = q(n_0, m)$, $s(p(n_0, m)) = s(q(n_0, m))$, using (3.3), Rule 9: Substitution.

The substitution Rule is tricky. We have to set up the "right" statement. Let's make $P(x) := "s(p(n_0, m)) = s(x)." Then, putting $x := p(n_0, m)$ yields: $P(p(n_0, m))$ is true. NOW we can apply the Substitution Rule: since $P(p(n_0, m))$ is true, and $q(n_0, m) = p(n_0, m)$, $P(q(n_0, m))$ is true. And $P(q(n_0, m))$ is " $s(p(n_0, m)) = s(q(n_0, m))$," as desired.$

By **(B)** (used twice), $s(p(n_0, m)) = p(n_0, s(m))$ and $s(q(n_0, m)) = q(n_0, s(m))$.

We choose, as the values of the variables n and m in **(B)**, n_0 and the *particular* m that we supposed was in S . Notice how we keep using the same letter, here m , but in different ways!

Therefore, by the transitivity of equality, $p(n_0, s(m)) = q(n_0, s(m))$.

By the definition of S , $s(m)$ thus belongs to S if m does.

Hence $S = \mathbf{N}$, by the Principle of Mathematical Induction (an axiom).

This means that for n_0 , $p(n_0, m) = q(n_0, m)$ for all m . But our fixed n , n_0 , was any n_0 at all.

That is, for all n , $p(n, m) = q(n, m)$ for all m . This is the condition for equality of functions

with two variables: for all n and m , $p(n, m) = q(n, m)$. That is, $p = q$.

The uniqueness part is done: if there *is* a function that works, there is only one!

Existence part: This is where we show that yes, there IS a function that works!

Let E denote the set of all n for which we can construct (meaning: show that there exists) a function $p_n: \mathbf{N} \rightarrow \mathbf{N}$ such that: $p_n(0) = n$, and for all m in \mathbf{N} , $s(p_n(m)) = p_n(s(m))$.

Here is the set selector version of E :

$$E = \{ n \in \mathbf{N} : \exists p_n : \mathbf{N} \rightarrow \mathbf{N} \text{ such that } p_n(0) = n \text{ and } (\forall m \in \mathbf{N})(s(p_n(m)) = p_n(s(m))) \}.$$

The construction of this set (by specifying the criterion for membership in it) is the key idea in the proof of this Theorem!

If we can do this construction for every n , we can define $p(n, m) := p_n(m)$, for each n and m .

Since E is the set of all n such that we *can* do the construction, we want to show that $E = \mathbf{N}$.

To show that $E = \mathbf{N}$ we will use the set version of Mathematical Induction.

The first step is to show that 0 is in E . So, we need a function p_0 . Let us *construct* p_0 .

Now we are going to “create” something. Here is where we duck into the “back room” and use our knowledge, especially the things we take for granted. We want $p(n, m) = n + m$. We really don’t know how to define addition “in one jump,” but we do know what $0 + m$ “ought” to be — m . So we construct $p_0(m) := m$ for all m .

Let $p_0(m) := m$ for all m . So p_0 exists. Now let’s verify that p_0 has all the properties it needs, to help 0 be a member of E . Now, $p_0(0) = 0$ by construction. And $s(p_0(m)) = s(m)$ because $p_0(m) = m$, and then $s(m) = p_0(s(m))$ because $p_0(\text{anything in } \mathbf{N}) = \text{same thing}$. By transitivity of equality, $s(p_0(m)) = p_0(s(m))$ for all m . So what?

Well, now we know that **0 is in E** , because $p_0(0) = 0$, and $s(p_0(m)) = p_0(s(m))$ for all m , and these are the conditions p_0 had to satisfy, in order for 0 to be in E .

So suppose that some n is in E . Since we are trying to show “for all n in \mathbf{N} , $n \in E \Rightarrow s(n) \in E$ ” is true, we can let n be arbitrary, and then there are two relevant possibilities: just one of the statements “ $n \in E$ ” and “ $n \notin E$ ” is true. If “ $n \notin E$ ” is true, the statement “ $n \in E \Rightarrow s(n) \in E$ ” is true vacuously, so the universal AND is OK for that n . So we usually don’t mention that possibility. That is why we just supposed that some n *is* in E . Supposing that some n is in E is “making the induction hypothesis.”

We want to show that $s(n)$ is in E , to complete the steps needed to apply the axiom of Mathematical Induction.

Since n is in E , we know there is a function $p_n: \mathbf{N} \rightarrow \mathbf{N}$ such that for all m in \mathbf{N} , $p_n(0) = n$, and $s(p_n(m)) = p_n(s(m))$.

Notice that we can put the universal quantifier (for all m in \mathbf{N}) ahead of an “and” that does not contain the variable bound by the quantifier.

Notice that the equation $s(p_n(m)) = p_n(s(m))$, valid for all m , means that we can switch the order of s and p_n .

That is, the functions s and p_n **commute**. So we are going to want to show the same thing about s and $p_{s(n)}$.

We need to construct a function $p_{s(n)}: \mathbf{N} \rightarrow \mathbf{N}$ such that for all m in \mathbf{N} , $p_{s(n)}(0) = s(n)$, and $s(p_{s(n)}(m)) = p_{s(n)}(s(m))$ (why?).

Again we want to go behind our Wizard’s curtain,³ and figure out what to do, **given** p_n , **to** p_n , in order to **construct** $p_{s(n)}$, in terms of p_n . Well, $p_n(m)$ “ought” to be $n + m$, so $p_{s(n)}$ needs to be $s(n) + m$. And $s(n)$ is “really” $n + 1$, so $s(n) + m$ ought to be $n + 1 + m$, and we can write this as $n + m + 1$, and this is $s(n + m)$, and, in terms of p_n , $s(p_n(m))$. So we have cogitated, and come up with the definition $p_{s(n)}(m) := s(p_n(m))$. So let’s emerge from behind the curtain and write that definition down.

Set $p_{s(n)}(m) := s(p_n(m))$. Thus, $p_{s(n)}$ exists. Now, in order to show that $s(n)$ is in E , we need to check that for all m in \mathbf{N} , $p_{s(n)}(0) = s(n)$ and $s(p_{s(n)}(m)) = p_{s(n)}(s(m))$.

By our definition, $p_{s(n)}(0) = s(p_n(0))$,

and $p_n(0) = n$,

so $s(p_n(0)) = s(n)$ by applying s to both sides of the equation $p_n(0) = n$ (Substitution Rule!).

By transitivity of equality, $p_{s(n)}(0) = s(p_n(0))$ and $s(p_n(0)) = s(n)$ imply

$p_{s(n)}(0) = s(n)$.

So far, so good. **We need to show that $s(p_{s(n)}(m)) = p_{s(n)}(s(m))$ for all m .**

By our definition, $p_{s(n)}(m) = s(p_n(m))$ for all m .

Let us work with the right-hand side of the equation first, namely $p_{s(n)}(s(m))$, and change it into its meaning in terms of p_n . Then, we will try to change the left-hand side to the same thing.

This is **a useful technique** to try when we want to show that two mathematical objects are equal: **show that each of the objects is equal to a third object.**

Then, by transitivity of equality, the two original objects are equal to each other.

³The Wizard of Oz, Loew’s, Inc., 1939

In particular, $p_{s(n)}(s(m)) = s(p_n(s(m)))$ for all m , because $s(m)$ is just another “ m .” We know that $s(p_n(m)) = p_n(s(m))$ for all m , because n is in E . Therefore, substituting $s(m)$ for m gives $s(p_n(s(m))) = p_n(s(s(m)))$ for all $s(m)$, i.e., for all m , because there is an $s(m)$ for each m ! That is, by our definition, $p_{s(n)}(s(m)) = p_n(s(s(m)))$ for all m , by transitivity of equality.

Now let’s try to transform the left-hand side of the equation to the same thing, $p_n(s(s(m)))$.

By our definition of $p_{s(n)}$, and substitution, $s(p_{s(n)}(m)) = s(s(p_n(m)))$ for all m . Now **recall** that s and p_n commute — meaning we can change their order without affecting the value of the composite function. Thus, working from the inside out, because that is where s and p_n occur together, $s(s(p_n(m))) = s(p_n(s(m))) = p_n(s(s(m)))$, as desired (you need to look back to check this).

Therefore, $s(p_{s(n)}(m)) = p_{s(n)}(s(m))$ for all m . This means that $s(n)$ is in S , so $S = \mathbf{N}$, because the conditions in the Mathematical Induction Postulate are all true. Now we just define $p(n, m) := p_n(m)$. You are now asked to complete the proof by working the following exercise.

(5.10) Exercise: Show that $p(n, m) (:= p_n(m))$ satisfies the conditions in the theorem.

Do you agree that the proof was difficult to follow? There is more difficulty to come! We are now beginning to rebuild the basic arithmetic operations you learned how to *do* in grade school. Now you are moving toward understanding what numbers mean, and how the operations “work.” I concede the operations don’t work, you do!

(5.11) Exercise: Show that, for all n , $s(n) = n + s(0)$. We now *define* $1 := s(0)$. You are thus showing $s(n) = n + 1$: hence the name *successor* for the function s .

(5.12) Problem: Define $2 := s(1)$, and $3 := s(2)$, and $4 := s(3)$. Show that $2 + 2 = 4$. You will probably need to look in the proof of the theorem about addition.

The preceding theorem **and its proof** show how Landau *constructed* addition.

(5.13) Problem: Show: $(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(p + (q + r) = (p + q) + r)$.

You'll need to fix p and q , and let S denote the set of all r such that the statement $p + (q + r) = (p + q) + r$ is true. What is the name for what this theorem says about the operation of addition?

(5.14) Exercise: Show: $(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(p + q = q + p)$.

You'll need to fix p , and let S denote the set of all q such that the statement $p + q = q + p$ is true. This Theorem is called the _____ Law of Addition.

ORDER AND INEQUALITIES

Inequalities are very important in advanced mathematics. We shall now begin to develop techniques in dealing with them, as we develop the properties of inequalities, or the ordering relations. Here is (in effect) how Landau defines the relation $n \leq m$:

(5.15) Definition and notation: Let n and m belong to \mathbf{N} . Then n is **less than or equal to** m if there exists k in \mathbf{N} such that $n + k = m$. We express this in symbols by writing $n \leq m$.

(5.16) Definition and notation: Let n and m belong to \mathbf{N} . Then n is **less than** m if there exists k in \mathbf{N} such that $k \neq 0$ and $n + k = m$. We express this in symbols by writing $n < m$. The inequality $n < m$ is called a **strict inequality**.

(5.17) Exercise: Show: $(\forall n \in \mathbf{N})(\forall m \in \mathbf{N})(\text{If } n \leq m, \text{ then } n = m \text{ or } n < m)$.

(5.18) Problem: Show: $(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(\text{If } p + q = p + r, \text{ then } q = r)$.

What is the name of this Theorem?

Suggestion: Fix arbitrary q and r in \mathbf{N} . Consider the set $S := \{ p \in \mathbf{N} : p + q = p + r \Rightarrow q = r \}$.

(5.19) Exercise: Show: $(\forall n \in \mathbf{N})(\forall m \in \mathbf{N})(\text{If } n \leq m \text{ and } m \leq n, \text{ then } n = m)$.

Hint: Remember that $n + 0 = n$.

(5.20) Exercise: Show:

$(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(\text{If } p \leq q \text{ and } q < r, \text{ then } p < r)$.

What can you expect to be true, if you encounter a string of inequalities, all in the same direction, such as $p \leq q = t < r$, about the relation between p and r ?

(5.21) Exercise: Show that, for all n , $n < s(n)$.

(5.22) Problem: Show that, if $n < m$ and $m < p$, then $n < p$. You will need to use the associativity of addition. State the problem's statement in a standard logical form. There are some missing quantifiers!

(5.23) Problem: Show that, if $n < m$, then $n + p < m + p$ for all p . You will need to use associativity and commutativity of addition. State the problem's statement in a standard logical form. There are some missing quantifiers!

(5.24) Exercise: Define $n > m$ and $n \geq m$, and show that each of these relations is transitive. We will say "**n is larger than m**" or "**n is greater than m,**" when " $n > m$ " is true, and use similar phrases when " $n \geq m$ " is true. You will need to use associativity of addition to show transitivity.

Please notice that we have NOT shown that " $n \geq m$ " is the denial of " $n < m$ ". It is true, but has yet to be proved! You will do this later, in (5.27), a Special Problem.

(5.25) Exercise: Show that, for all n , if $n \neq 0$, then $1 \leq n$. You need to use the definition of 1 : $1 = s(0)$. You are also showing that there is no natural number strictly between 0 and 1 ! Suggestion: let $S := \{0\} \cup \{n \in \mathbf{N} : 1 \leq n\}$. You'll need to use transitivity of \leq .

The list of things Landau proves is long, and each thing on the list is something you have learned to take for granted. But now you are being asked to take on the task of certifying (or not!) the work of past generations to future ones!

One very important theorem Landau proves is this:

(5.26) Theorem (Trichotomy Law): For all n in \mathbf{N} , and for all m in \mathbf{N} , exactly one of the following is true:

$$(1) \ n = m; \quad (2) \ n < m; \quad (3) \ m < n.$$

(5.27) Special Problem: Prove the Theorem. You will need to use the equation that defines “ $n < m$.” You already know that $s(n) \leq n$ and $s(n) > n$. It may help to prove that, “for all n in \mathbf{N} , $\sim(s(n) < n)$ ” is true.

(5.28) Theorem: $(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(\text{If } p + q < p + r, \text{ then } q < r)$

Proof: We have to show that, for every choice of three elements p , q , and r in \mathbf{N} , the statement

$$\text{If } p + q < p + r, \text{ then } q < r$$

is true. The statement has the form “If A then B .” In case A is false, we don’t have anything to do; the statement is vacuously true. Therefore, we will assume that A is true, and try to deduce B . We usually do this sort of thing without saying so. The way we often say that we are assuming that A is true is, in the present case: “Given: $p + q < p + r$.” By definition of “ $<$,” there exists $s \neq 0$ such that $(p + q) + s = (p + r)$. Therefore, by associativity (see (5.14)), and the transitivity of equality, $p + (q + s) = p + r$. By (5.18), the Cancellation Law for addition, $q + s = r$. Since $s \neq 0$, this means, by definition, that $q < r$, as desired.

This proof is a good example of using of a definition in two ways. We are given that $p + q < p + r$. Then we look up the definition (or, better yet, recall it!), and translate its symbols into the context of the problem. That is why parentheses are used on both sides of the equation in the second sentence of the proof: $p + q$ and $p + r$ are to be thought of as single elements of \mathbf{N} . So we get, using the given truth of the definition’s statement, and associativity, and cancellation, the equation $q + s = r$. Next we use the definition backwards! I call this a “recognition step.” We recognize that the equation $q + s = r$, with $s \neq 0$, occurs in the definition of “ $q < r$.” Since the equation is true, we then conclude that the criterion for saying “ $q < r$ ” is satisfied.

(5.29) Definition: If S is a set contained in \mathbf{N} , S has a least element if there exists $m \in S$ such that, for all $n \in \mathbf{N}$, if $n \in S$, then $m \leq n$.

(5.30) Problem: Write the statement of the definition in logic notation, giving careful attention to the placement of quantifiers. Be sure that no *quantifiers* include “ $\in S$.”

(5.31) Exercise: Show that, if the statement “ S has a least element” is true, then there is only one m such that “ $m \in S$, and, for all $n \in \mathbf{N}$, if $n \in S$, then $m \leq n$ ” is true.

Suggestion: This is a uniqueness theorem, so you might begin by assuming that

“ $m_1 \in S$, and, for all $n \in \mathbf{N}$, if $n \in S$, then $m_1 \leq n$ ” is true, and

“ $m_2 \in S$, and, for all $n \in \mathbf{N}$, if $n \in S$, then $m_2 \leq n$ ” is true,

and then show that $m_1 = m_2$.

(5.32) Definition and notation: If S is a set contained in \mathbf{N} , and S has a least element, then, **the least element of S** is the unique (by (5.31)) m in S such that, for all $n \in \mathbf{N}$, if $n \in S$, then $m \leq n$. We denote this unique m by **$\min(S)$** .

(5.33) Exercise: Show that 0 is the least element of \mathbf{N} , i.e., that $0 = \min(\mathbf{N})$.

(5.34) Exercise: Does the empty subset of \mathbf{N} have a least element? You will probably need the answer to (5.30) to be sure about your answer to this exercise.

(5.35) Exercise: Devise a definition of **S has a greatest element**, and of **$\max(S)$** .

← the Well-Ordering Theorem — a very powerfully applicable theorem

(5.36) Theorem (Well-Ordering): Every non-empty subset of \mathbf{N} has a least element.

Proof: We will use a contradiction argument. We will do this in great detail this time.

To do so, let us express the mathematical statement in the Theorem in logic notation.

$$\left(\forall S \in 2^{\mathbf{N}} \right) \left(S \neq \emptyset \Rightarrow (\exists m \in \mathbf{N}) (m \in S \wedge (\forall n \in \mathbf{N}) (n \in S \Rightarrow m \leq n)) \right).$$

To use a contradiction argument, we assume that the denial of the desired mathematical statement is true, and seek to deduce a contradiction.

The Law of the Excluded Middle, ((3.3), Rule 4) then would say that S *does* have a least element.

Thus, let us assume the denial is true. The denial, now true, of our mathematical statement is

$$\left(\exists S \in 2^{\mathbf{N}} \right) \left(S \neq \emptyset \wedge (\forall m \in \mathbf{N}) (m \notin S \vee (\exists n \in \mathbf{N}) (n \in S \wedge m > n)) \right).$$

By (3.3), Rule 6, we can find a set S_0 such that

$$\left(S_0 \neq \emptyset \wedge (\forall m \in \mathbf{N}) (m \notin S_0 \vee (\exists n \in \mathbf{N}) (n \in S_0 \wedge m > n)) \right) \text{ is true. For convenience, let}$$

us write this in the equivalent form

$$(S_0 \neq \emptyset \wedge (\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))).$$

Let S_0 be such a non-empty subset of \mathbf{N} .

Then each of the mathematical statements

$$S_0 \neq \emptyset \text{ and } (\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)) \text{ is true.}$$

We are not going to use the non-emptiness of S_0 until the very end of the argument.

We are going to show that $(\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)) \Rightarrow S_0 = \emptyset$ is true.

Since we have already assumed that $(\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))$ is true,

what we have to do is deduce that $S_0 = \emptyset$.

It is usually a good idea to examine a statement to see what it means, at the “work” level.

Let’s begin by doing that.

Since $(\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))$ begins with a universal quantifier, by (3.3), Rule 5, we can choose $m = 0$, and deduce that $(0 \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0))$ is

true. The reason for choosing $m = 0$ is this: we can look at the statement

$(\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0)$ and see that it must be false, because $n < 0$ must be false. How can we prove that? By (3.3), Rule 6, we can find n such that $(n \in S_0 \wedge n < 0)$ is true for n . By

(3.3), Rule 1b, we can deduce that $n < 0$ is true. We expect this to be false, since $n \in \mathbf{N}$.

How do we prove that $n < 0$ is false? Here is the argument:

By definition, $n < 0$ means that there exists k in \mathbf{N} such that $k \neq 0$ and $0 = n + k$.

Since $k \neq 0$, we can apply an exercise you have done ((5.07)) that said, using the present notation, “for all k in \mathbf{N} , if $k \neq 0$ then there exists exactly one j in \mathbf{N} such that $k = s(j)$.” Now we can go back to the proof of the theorem about addition, and say

$$0 = n + k = p(n, k) = p(n, s(j)) = s(p(n, j)).$$

Therefore, 0 is the successor of $p(n, j)$. But 0 is not the successor of any element of \mathbf{N} (one of the axioms!). We have produced a contradiction of the form “A and not-A.” Hence $n < 0$ is false.

How does all this help us? Recall that we have deduced that $(0 \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0))$ is true, and we have shown that $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0)$ is false.

The true mathematical statement $(0 \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0))$ has the logic form $A \Rightarrow B$.

Since B is false, that is, $\sim B$ is true, we can deduce, by (3.3) Rule 7b, that $\sim A$ is true, namely, that A is false. Therefore, we have deduced that $0 \in S_0$ is false, so $0 \notin S_0$.

What have we done so far? We have shown that, if a non-empty subset of \mathbf{N} does not have a least element, then it cannot contain 0 . You could, if you wished, show that it cannot contain 1

either. What we want to do is to show that it cannot contain *any* natural number. This is where we will get the desired contradiction to use in proving the whole theorem.

Let us look again at the mathematical statement

$$(S_0 \neq \emptyset \wedge (\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))).$$

We have deduced from it that $0 \notin S_0$.

We did it by showing that $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < 0)$ is false.

We would like to show that, for all m in \mathbf{N} , $m \notin S_0$.

Here is an *idea*: show that, for all m in \mathbf{N} , $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)$ is false.

Then, from the truth of $(\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))$, we can deduce, by (3.3) Rule 7b, that $(\forall m \in \mathbf{N})(m \notin S_0)$ is true.

To show that, for all m in \mathbf{N} , $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)$ is false, let us show that, for all m in \mathbf{N} , the denial of $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)$ is true.

We use Mathematical Induction to show that a mathematical statement is true for all m in \mathbf{N} .

Thus, we need to define a subset E of \mathbf{N} that consists of all those natural numbers m such that the denial of $(\exists n \in \mathbf{N})(n \in S_0 \wedge n < m)$ is true.

We use set-selector notation to display this set: Let $E := \{ m \in \mathbf{N} : (\forall n \in \mathbf{N})(n \notin S_0 \vee n \geq m) \}$.

The defining criterion for membership in E consists of statements (one for each n) of the form not-A or B, where A denotes $n \in S_0$ and B denotes $n \geq m$. Each of these is equivalent to a statement of the form $A \Rightarrow B$. Let us express each one in the equivalent form not-B \Rightarrow not-A. Then $E = \{ m \in \mathbf{N} : (\forall n \in \mathbf{N})(n < m \Rightarrow n \notin S_0) \}$.

In words, E consists of all natural numbers m such that no natural number that is less than m belongs to S .

We know that 0 belongs to E , because for all n in \mathbf{N} , the antecedent in “ $n < m \Rightarrow n \notin S_0$ ” is false when $m = 0$.

To apply Mathematical Induction, we next need to show that, for an arbitrary natural number m , “ $m \in E \Rightarrow m + 1 \in E$ ” is true.

We may suppose $m \in E$. This means that $(\forall n \in \mathbf{N})(n < m \Rightarrow n \notin S_0)$ is true.

In order to show that, therefore, $m + 1 \in E$, we need to show that $(\forall n \in \mathbf{N})(n < m + 1 \Rightarrow n \notin S_0)$ is true. This has a universal quantifier.

We need to show that, for an arbitrary n in \mathbf{N} , $n < m + 1 \Rightarrow n \notin S_0$.

By the Trichotomy Law, we can divide the work into three cases.

In **Case 1**, we will assume $n < m$.

In **Case 2**, we will assume $n = m$.

In **Case 3**, we will assume $n > m$.

Case 1: In this case, $n < m$. This case does not occur if $m = 0$ (why?).

If $m > 0$, and $n < m$, then $n < m \Rightarrow n \notin S_0$ is true because $m \in E$, so by (3.3) Rule 7a, $n \notin S_0$ is true.

But then, since $n < m$, transitivity of inequality shows that $n < m+1$.

Thus, for $n < m$, $n < m+1 \Rightarrow n \notin S_0$ is true.

Case 2: In this case, $n = m$. We already know that no natural number smaller than m is in S_0 .

There are two possibilities, one of which must be true, by the Law of the Excluded Middle:

$m \notin S_0$ and $m \in S_0$.

The first of these is what we are trying to prove, so we have nothing to do if $m \notin S_0$.

In fact, we have to show that $m \in S_0$ must be false. Again we turn to a contradiction argument to prove it.

Suppose, then, that $m \in S_0$. Then no natural number smaller than m is in S_0 .

Therefore, for every n in S_0 , $m \leq n$. This means that m is the least element of S_0 ! Since we are assured, by the truth of the denial that S_0 has a least element, that S_0 does not have a least element, m cannot belong to S_0 .

Therefore, for $n = m$, $n < m+1 \Rightarrow n \notin S_0$ is true.

Case 3: In this case, $n > m$. Therefore, there exists k in \mathbf{N} , $k \neq 0$, such that $n = m + k$. By Exercise (5.25), $k \geq 1$. Therefore, by transitivity, $n \geq m + 1$. Thus, $n < m+1 \Rightarrow n \notin S_0$ is vacuously true in this case.

We have shown that, if $m \in E$ then $(\forall n \in \mathbf{N})(n < m+1 \Rightarrow n \notin S_0)$ is true. This completes the work needed to apply Mathematical Induction. Therefore, $E = \mathbf{N}$.

Let us now show that, because $E = \mathbf{N}$, S_0 is empty, so that we can get our contradiction. Recall that $E = \{ m \in \mathbf{N} : (\forall n \in \mathbf{N})(n < m \Rightarrow n \notin S_0) \}$. Let's suppose that S_0 is not empty. Then there exists m_0 in \mathbf{N} such that $m_0 \in S_0$. Now $m_0 + 1 \in E$ because $E = \mathbf{N}$. Since $m_0 < m_0 + 1$, $m_0 \notin S_0$. This is a contradiction. Thus S_0 is empty if $(\forall m \in \mathbf{N})(m \in S_0 \Rightarrow (\exists n \in \mathbf{N})(n \in S_0 \wedge n < m))$ is true. But at the beginning of the argument, we assumed that S_0 is NOT empty. This is a contradiction. Thus our assumption that there exists a non-empty set S_0 without a least element is false. Therefore, every non-empty subset S of \mathbf{N} has a least element.

Here is a shorter proof, without all the explanations, that is suggested by the proof just given: Let S_0 be a non-empty subset of \mathbf{N} . Suppose that S_0 does not have a least element. Let $E := \{ m \in \mathbf{N} : (\forall n \in \mathbf{N})(n < m \Rightarrow n \notin S_0) \}$. If we can show that $E = \mathbf{N}$, we can contradict the assumption that S_0 is non-empty. Let $m = 0$. The statement $n < m \Rightarrow n \notin S_0$ is vacu-

ously true if $m = 0$. Thus, $0 \in E$. Now suppose $m \in E$. To show that $m+1 \in E$, it is enough to show that $m \notin S_0$. Suppose not. That is, suppose $m \in S_0$. Then, since no element of \mathbf{N} that is smaller than m is in S_0 , m is the least element of S_0 . This contradicts our initial assumption. Thus, $m \notin S_0$. Hence, no natural number smaller than $m+1$ is in S_0 . This shows that $m+1$ is in E , and so by Mathematical Induction, $E = \mathbf{N}$. But this implies that S_0 is empty, because, if some $m_0 \in S_0$, the fact that $m_0+1 \in \mathbf{N}$ implies that $m_0+1 \in E$, since $E = \mathbf{N}$. But $m_0+1 \in E$ implies that $m_0 \notin S_0$. This is a contradiction. Thus S_0 is empty. This is a contradiction. Thus every non-empty subset of \mathbf{N} has a least element.

(5.37) Special Problem: Prove the following **Theorem-with-Definition and notation**.

Theorem and Definition (of) and notation (for) (on multiplication): Recall the notation $p(n, m)$ for addition. There exists one and only one function $t: \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ with the following properties:

- (A) for all n in \mathbf{N} , $t(n, 1) = n$,
- (B) for all n in \mathbf{N} , and for all m in \mathbf{N} , $t(n, s(m)) = p(n, t(n, m))$

We call the finding of the value of $t(n, m)$ **multiplication of n and m** , and we call the value of $t(n, m)$ **the product of n and m** . We use the notations $\mathbf{n m} := t(\mathbf{n}, \mathbf{m})$, $\mathbf{n} \times \mathbf{m} := t(\mathbf{n}, \mathbf{m})$. We won't use the second notation much.

To do this problem, you might use the proof of the theorem about addition as an outline, and make appropriate changes.

(5.38) Exercise: Show that for all n in \mathbf{N} , $n \cdot 0 := t(n, 0) = 0$.

(5.39) Exercise: Show that multiplication is associative.

(5.40) Exercise: Show that multiplication is commutative.

(5.41) Problem: Show that **multiplication distributes over addition**, that is, .

$$(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(p \times (q + r) = p \times q + p \times r),$$

a statement also known as the **Distributive Law**. The equation is usually written $p(q + r) = pq + pr$.

(5.42) Exercise: Show that, if m and n are in \mathbf{N} , and $nm = 0$, then $n = 0$ or $m = 0$.

You might want to prove, instead, that “ $n \neq 0$ and $m \neq 0$ ” implies “ $nm \neq 0$ ” is true. Do you agree that the two statements are equivalent? This is also known as the **Cancellation Law (for multiplication by a non-zero natural number)**.

This is called the Cancellation Law because it is logically equivalent to the next Exercise.

(5.43) Exercise: Show that, if m, n and p are in \mathbf{N} , and $n \neq 0$, then “ $nm = np$ implies $m = p$ ” is true. This is the theorem that is usually called the **Cancellation Law (for multiplication by a non-zero natural number)**.

(5.44) Exercise: There is a Cancellation Law for addition too. State it, and prove it. (Hint: This has been done in a previous exercise; if you haven’t done it yet, now’s the time!)

(5.45) Exercise: Show that

$$(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(p \neq 0 \text{ and } q < r \Rightarrow pq < pr).$$

(5.46) Theorem: $(\forall p \in \mathbf{N})(\forall q \in \mathbf{N})(\forall r \in \mathbf{N})(p \neq 0 \text{ and } pq < pr \Rightarrow q < r)$

The proof will be by contradiction. Please write down the denial of the mathematical statement in the Theorem. Then imagine being given p, q and r in \mathbf{N} for which the denial is true. This is “standard procedure” for a contradiction argument when we have to prove a mathematical statement full of universal quantifiers. Proofs often start with the standard thing “already done.”

Proof: Suppose that $p \neq 0$ and $pq < pr$. Suppose that q is NOT less than r . This gives two possibilities: $q = r$, and $q > r$. If $q = r$, then, by the Substitution Rule, $pq = pr$.

The Substitution Rule, (3.3) Rule 9, says: if $P(x)$ is a statement with a free variable, x , and $P(x_0)$ is true when x is replaced by a particular x_0 , then $y_0 = x_0$ implies that $P(y_0)$ is true. In this application, we let $P(x)$ be the statement “ $pq = px$,” where x is a free variable in \mathbf{N} . Then $P(q)$ is true. Since $q = r$, $P(r)$ is also true. That is, $pq = pr$, as desired.

Since $pq < pr$, the Trichotomy Law shows that we have a contradiction. Thus, $q = r$ is not true. The other possibility is that $r < q$. In the exercise preceding this theorem you showed that $r < q$ implies $pr < pq$. Again, this is false by the given relation $pq < pr$ and the Trichotomy Law. Since $q = r$ and $r < q$ are both false, the Trichotomy Law implies $q < r$, as desired.

Example: Let us use multiplication, addition, and the Well-Ordering Theorem to prove that long division works.

(5.47) Theorem and Definition (The Division Algorithm): Let n be a non-zero natural number, and let m be a natural number. Then there exist unique natural numbers q and r such

that $0 \leq r < n$, and $m = qn + r$. The number q is called the **quotient**, and the number r the **remainder**, (when m is divided by n).

Proof: This is another existence-and-uniqueness theorem. We will prove the existence of q and r first, and then prove that they are unique.

To prove existence, we will first find the least multiple of n that is greater than or equal to m . Then we could ask whether that least multiple of n is equal to m . There would be two possible answers: YES and NO. Each possible answer *could* happen, so we would have to consider what happened in each of two **cases**. We will actually do something a little different, but the idea is similar to what we *might* have done.

Let $n\mathbf{N}$ denote the set $\{nk : k \in \mathbf{N}\}$. This set consists of all multiples of natural numbers by n .

Another way to express $n\mathbf{N}$ is as the image of the function $f : \mathbf{N} \rightarrow \mathbf{N}$ given by the rule $f(k) := nk$, for k in \mathbf{N} , or by $f := \{(j, k) \in \mathbf{N} \times \mathbf{N} : k = nj\}$.

The set $n\mathbf{N}$ is not the set we want to work with, because $n\mathbf{N}$ has nothing to do with m , but a *subset* of $n\mathbf{N}$ will work. We construct a set, S , that does involve m , using set selector notation, by $S := \{p \in \mathbf{N} : p \in n\mathbf{N} \text{ and } p \geq m\}$.

The set S consists of all the products of n times a natural number that are at least as large as m . If S has a least element, p , we can say $p = nk$ and $nk \geq m$.

We want to apply the Well-Ordering Theorem to S . Therefore, we have to show that S is not an empty set. It will be enough to show there is an element of S that is larger than m .

To show that a natural number t is larger than m , we need to show that $t = m + u$, where u is a non-zero natural number.

How can we find t , a multiple of n , that is larger than m ? Well, $m + 1$ is larger than m , and $n \geq 0$, so $n \geq 1$, and thus $n(m + 1)$ ought to work.

Since $n \geq 0$, and $m + 1 \geq 0$, the Cancellation Law (5.42) shows that $n(m + 1) \geq 0$. This will be our t .

By the Distributive Law, $t := n(m + 1) = nm + n$, and there exists i in \mathbf{N} such that $n = s(i)$, because $n \geq 0$. Therefore, $n = i + 1 = 1 + i$, so

$$t = nm + n = (1 + i)m + n = (1m + im) + n = (m + im) + n = m + (im + n).$$

Since $im + n = im + (i + 1) = (im + i) + 1 = s(im + i)$, $im + n \geq 0$. Let $u = im + n$.

We have shown that $t = n(m + 1) = m + u = m + (\text{a non-zero natural number})$, so $t > m$.

This means that S is not an empty set, because $t = n(m + 1)$ is in S .

By the Well-Ordering theorem, S has a least element, p , and $p = nk$, for some k in \mathbf{N} , because every element of S is the product of n times some natural number.

Since $p = nk$ for some k , we will consider two possibilities: $k = 0$, and $k \geq 0$.

If $k = 0$, then $p = nk = n0 = 0$, and nk is in S , so $m \leq p = nk = 0$.

Thus, $m = 0$, and we *choose* $q = 0$, $r = 0$.

Then $m = 0 = 0n + 0$, so a pair q, r ($q = 0 = r$) exists that satisfies $m = qn + r$, if $k = 0$.

Let us show that $q = 0$ and $r = 0$ are the *only* q and r such that $0 = nq + r$.

Suppose not. This means we are assuming that either $q \neq 0$ or $r \neq 0$, and $0 = nq + r$.

But if $q \neq 0$, then $nq \neq 0$, so $nq > 0$, hence $nq + r = 0$, so q cannot be non-zero.

Hence, $q = 0$.

Then $0 = n \cdot 0 + r = 0 + r = 0$, so $r = 0$ as well.

Thus, q and r , both 0 , are unique if $k = 0$: no other pair of natural numbers makes the equation $nq + r = 0$ true, since $n \neq 0$.

If $k \neq 0$, there exists j in \mathbf{N} such that $k = s(j) = j + 1$. We have $p = nk = kn = (j + 1)n = jn + n = nj + n$, so $nk > nj$, by definition of “ $>$.” Recall that $p = nk$ is the least element of S . Therefore, nj is in $n\mathbf{N}$, but nj is not in S , because $nj < nk = p$. By the definition of S , $nj < m$, because nj is not in S . This means, by definition of “ $>$,” that there exists $v (\neq 0)$ in \mathbf{N} such that $m = nj + v$.

Again, there are cases (subcases?) to consider. They are: $v < n$, $v = n$, $v > n$, by the Trichotomy Law.

If $v < n$, we set $r := v$. Then $m = nj + r$, and we set $q := j$. So we have existence in the first case. We’ll show uniqueness later.

In the second case, $v = n$, so $m = nj + n = nj + n1 = n(j + 1) = nk$.

So now we set $q := k$, $r := 0$, and we have $m = nq + r$; again we have shown existence in this case.

Finally, let us show that **the third case, $v > n$, cannot occur**. For if, on the contrary, $v > n$, then $m = nj + v$, and $m \neq p = nk = nj + n < nj + v = m$.

But this implies $m < m$. This cannot be true (Why?!).

Thus, the third case cannot occur, so we have existence in all cases.

We have to show uniqueness, still under the assumption that $k \neq 0$.

So suppose $m = qn + r$, and $m = sn + t$, where $0 < r < n$ and $0 < t < n$.

We have to show $q = s$ and $r = t$.

Because both are equal to m , $qn + r = sn + t$.

There are three possible cases here, for the relation between r and t .

They are $r = t$, $r < t$, and $t < r$ by the Trichotomy Law.

If $r = t$, then by the Cancellation Law for Addition, $qn = sn$.

Then, by the Cancellation Law for Multiplication by a non-zero natural number, $q = s$. Thus in the case “ $r = t$ ” we have $q = s$ and $r = t$.

Now we need to show that neither of the other cases can occur!

Suppose, to the contrary, **that** $r < t$.

Then there exists $w \geq 0$ such that $r + w = t$.

Therefore, by the Substitution Rule,

$$qn + r = m = sn + t = sn + (r + w) = (sn + r) + w > sn + r.$$

By transitivity, $qn + r > sn + r$.

By a previous Theorem ((5.28)), $qn + r > sn + r$ implies $qn > sn$.

By a previous Theorem ((5.46)), $qn > sn$ implies $q > s$ (the Theorem can be applied because $n \geq 0$).

By definition, $q > s$ implies there exists $u \geq 0$ such that $q = s + u$. Now,

$$(*) \quad m = qn + r = (s + u)n + r = (sn + un) + r.$$

Look out! A trick is coming!

Recall that $t < n$. Thus, there exists $v \geq 0$ such that $n = t + v$. Substitute this into the equation (*): $m = qn + r = (sn + un) + r = (sn + u(t + v)) + r = (sn + (ut + uv)) + r = ((sn + ut) + uv) + r = (sn + ut) + (uv + r) > sn + ut$, because $uv \geq 0$ by a previous exercise ((5.42)), and so $uv + r \geq 0$. Thus, by transitivity, $m > sn + ut$ $sn + t = m$. This contradiction ($m > m$) completes the proof of uniqueness in case $r < t$.

There is one more case: $t < r$. But the argument for the case $r < t$ becomes an argument for the case $t < r$ if we simply interchange t and r everywhere in the argument!

Thus the proof is complete.

(5.48) Definition and notation: Let $m \in \mathbf{N}$, $n \in \mathbf{P}$. Then **m is divisible by n** if there exists q in \mathbf{N} such that $m = nq$. We express this in symbols by $n \mid m$. We also say that **n is a divisor of m** .

(5.49) Exercise: Show that “is divisible by” is a transitive and reflexive relation on \mathbf{P} .

(5.50) Exercise: Show that “is divisible by” is not a symmetric relation on \mathbf{P} .

(5.51) Exercise: Suppose $n \in \mathbf{P}$. Show that 0 is divisible by n .

(5.52) Exercise: Suppose $m \in \mathbf{P}$ and $n \in \mathbf{P}$. Show that, if m is divisible by n , then $n \mid m$.

(5.53) **Exercise:** Suppose $n \in \mathbf{P}$. Do the last two Exercises together imply $n = 0$? Why not?

(5.54) **Definitions:** Let $m \in \mathbf{N}$. Then m is **even** if m is divisible by 2, and **odd** otherwise.

(5.55) **Exercise:** Show that the relation defined by “ $n \sim m$ if $n+m$ is divisible by 2” is an equivalence relation on \mathbf{N} .

cardinal numbers: the number of elements in a set

One of the many reasons we need the natural numbers is because we use them to define “model” finite sets that we will use to say what “the number of elements in a set” means when a set is finite.

How many elements are in a set? Officially, we are at a very primitive mathematical state, relative to number in the sense of “how many!” We have only three terms to describe quantity so far: none, one, and two. And each of these is actually a primitive term — not defined in terms of other terms. We also have two terms to describe order: first and second — used especially in talking about ordered pairs. Note that “pair” is not a mathematical term for “twoness,” at least not yet, because the term is “ordered pair,” two words used to make up one mathematical term.

The idea behind describing “how many” elements are in a set must be ancient. Imagine a flock of sheep kept at night in a pen. As the sheep are let out of the pen, one at a time, in the morning, we take a rock from a pile inside the gate and toss it just outside. Then we go about our day’s business. When the sheep are brought back in the late afternoon, we toss the rocks back inside. If some rocks are left over, there probably won’t be many, and we know how many sheep to search for. What we did in the morning was to make a one-to-one correspondence between the sheep and the rocks. If there are no rocks left in the pile when the sheep come back in, we know no sheep are missing. The pile of rocks has the same “how many” as the flock. If all we are interested in most days is whether any sheep are missing, this method works. Sometimes we want to know the actual number of sheep. We can find that out by counting the rocks. But what is “counting?” It is something we are taught as children. I assume we all learn the decimal system of counting, and use it to do arithmetic. The system gives us a way to NAME quantities. It does not purport to tell us what “quantity” is. And yet it gives us a way to define it! What we can do is to very carefully set up a collection of mathematical objects, using our axioms to give us true statements. The ob-

jects we call numbers. They are imagined into existence. More will be said about this later. Right now, we simply want to make some more definitions that address the matter of matching sets, rather than the matter of giving names to “how many.”

(5.56) Definition and notation: For each n in \mathbf{N} , let \mathbf{S}_n denote the set $\{ m \in \mathbf{N} : m < n \}$.

An important point: n does not belong to \mathbf{S}_n .

(5.57) Exercise: Write out \mathbf{S}_0 , \mathbf{S}_1 , and \mathbf{S}_7 .

(5.58) Exercise: For each n in \mathbf{N} , how many elements (in the everyday, intuitive sense) does \mathbf{S}_n have?

(5.59) Exercise: Show that, if $n \in \mathbf{N}$, and there exists $p \in \mathbf{N}$ such that $n = s(p)$, then $p \in \mathbf{S}_n$, and p is the greatest element of \mathbf{S}_n .

An important point: we have not yet defined, *mathematically*, something that does the job of saying “how many!”

(5.60) Definition: A set S is a **finite set** if S is empty, or if there exists $n \in \mathbf{P}$ and a one-to-one correspondence $f: S \rightarrow \mathbf{S}_n$.

The everyday meaning of “cardinal number of” is “the number of elements in.”

(5.61) Definition: A non-empty set S is an **infinite set** if there does not exist a one-to-one correspondence $f: S \rightarrow \mathbf{S}_n$, for any n in \mathbf{P} .

(5.62) Exercise: Translate the definition of infinite set into logic notation, with quantifiers, and with no negation signs (\sim) preceding a quantifier.

(5.63) Theorem: For all n and m in \mathbf{P} , if there exists a one-to-one correspondence between \mathbf{S}_n and \mathbf{S}_m , then $n = m$.

This theorem is hard to prove. Partly this is so because the assertion is so obvious. It means we are given that n and m are definite elements of \mathbf{P} . We just don’t know which ones. We are

given that there is a function $f: \mathbf{S}_n \rightarrow \mathbf{S}_m$ that is one-to-one and onto. That is all we know about the function f . We have to show that n and m are equal to each other. There are three possibilities, by the Trichotomy Law. So we really only have to do *work* on one of the *contrary* cases. Say we *assume* $n < m$. This is a case that's not supposed to happen, so we are looking for a contradiction. From everyday experience, we expect that \mathbf{S}_m has to have some elements that don't get matched with elements of \mathbf{S}_n . The problem is to show that this is true, just using the given information. I don't know a straightforward way to carry out this reasonable plan! So I followed Landau's example and tried to use Mathematical Induction for \mathbf{P} . The idea is to define an appropriate set \mathbf{E} . I'll let \mathbf{E} denote the set of all n in \mathbf{P} such that, if there exists a one-to-one correspondence, f , between \mathbf{S}_n and \mathbf{S}_m , then $n = m$.

Proof: Let $\mathbf{E} :=$

$$\left\{ n \in \mathbf{P} : \left(\forall m \in \mathbf{P} \right) \left(\left(\exists f : \mathbf{S}_m \rightarrow \mathbf{S}_n \right) \left(f \text{ is a one - one correspondence} \right) \Rightarrow m = n \right) \right\}.$$

To show: $\mathbf{E} = \mathbf{P}$, by Mathematical Induction.

To show that $\mathbf{1} \in \mathbf{E}$, let $n = 1$, and let m be an arbitrary element of \mathbf{P} .

We must let m be arbitrary, because we have to show a statement is true "for all m ."

We must show that, if there exists $f: \mathbf{S}_m \rightarrow \mathbf{S}_1$ that is a one-to-one correspondence, then $m = 1$.

Recall that, if there does not exist $f: \mathbf{S}_m \rightarrow \mathbf{S}_1$ that is a one-to-one correspondence, then the statement in the set selector is true, for this m , vacuously!

Here are two possibilities about the arbitrary m . One of them is that $m = 1$, the other that m is not equal to 1. The first case is what we want to show, so there is no more to do in case $m = 1$. So, suppose that $m \neq 1$, and that there exists $f: \mathbf{S}_m \rightarrow \mathbf{S}_1$ that is a one-to-one correspondence. Since $m \neq 1$, and m is in \mathbf{P} , we must have $m > 1$. Thus, $m \in s(1)$, so $\{0, 1\} = \mathbf{S}_{s(1)} \subseteq \mathbf{S}_m$. But $\mathbf{S}_1 = \{0\}$, so $f(0) = 0 = f(1)$, and this contradicts "f is one-one."

Therefore, $m = 1$, or else there does not exist $f: \mathbf{S}_m \rightarrow \mathbf{S}_1$ that is a one-to-one correspondence, so $\mathbf{1} \in \mathbf{E}$.

(5.64) Exercise: Construct $f: \mathbf{S}_1 \rightarrow \mathbf{S}_1$ that is a one-to-one correspondence.

Now **suppose that n (in \mathbf{P}) is in \mathbf{E} .** We have to show this implies $s(n)$ is in \mathbf{E} . Let m be

an arbitrary element of \mathbf{P} . We must then show that, if there exists $f: \mathbf{S}_m \rightarrow \mathbf{S}_{s(n)}$ that is a one-to-one correspondence, then $m = s(n)$.

What we want to do is: show that the existence of a one-to-one correspondence $f: \mathbf{S}_m \rightarrow \mathbf{S}_{s(n)}$ implies the existence of a one-to-one correspondence $g: \mathbf{S}_{m-1} \rightarrow \mathbf{S}_n$. Then by the induction hypothesis, we could say $m-1 = n$, so we'd have $m = s(m-1) = s(n)$, as desired.

Let us assume that there exists $f: \mathbf{S}_m \rightarrow \mathbf{S}_{s(n)}$ that is a one-to-one correspondence. We want to show that we can modify f to construct $g: \mathbf{S}_{m-1} \rightarrow \mathbf{S}_n$ that is a one-to-one correspondence.

But what if $m = 1$? Then $m-1$ wouldn't exist! Let's show m can't be 1, by contradiction.

Suppose $m = 1$.

Then $f^{-1}: \mathbf{S}_{s(n)} \rightarrow \mathbf{S}_1$ is also a one-to-one correspondence.

We have already shown that $1 \in E$, and this implies (do you really agree?) that $s(n) = 1$.

This is impossible, because 1 is not the successor of any element in \mathbf{P} (because 1 is the successor of 0, which is not in \mathbf{P} , and the successor function is one-one).

Therefore, $m \neq 1$.

Therefore, $m > 1$ (why?).

Since $m > 1$, we know that there exists $m-1$ in \mathbf{P} such that $m = s(m-1)$ (why?).

We can now modify the given f and construct a one-to-one correspondence $g: \mathbf{S}_{m-1} \rightarrow \mathbf{S}_n$. Then, because n is in E , we will be able to conclude that $m-1 = n$, so $m = s(m-1) = s(n)$, as desired. Recall that $m-1$ is the predecessor of m .
In everyday terms, g will be constructed this way:
 $g(i) = f(i)$ if $i < p$, and $g(i) = f(i+1)$, if $p \leq i < m-1$.

Recall that a function "is" a set of ordered pairs.

Since f is onto, and because n is in $\mathbf{S}_{s(n)}$, there exists p in \mathbf{S}_m such that $f(p) = n$.

Thus (p, n) belongs to f . Since f is one-to-one, there is only one such p .

There are **two cases** to discuss.

The easy one is: $p = m-1$.

Then we define g by putting into g all the ordered pairs in f *except* $(p, n) = (m-1, n)$.

In other words, if $f(m-1) = n$, we construct g on \mathbf{S}_{m-1} by $g(i) := f(i)$, $0 \leq i < m-1$.

In the other case, $p < m-1$ (why?).

Now we will remove the ordered pair (p, n) from f , and change all the ordered pairs (i, j) in f that have $i > p$.

We define g this way, based on f : If there are any ordered pairs (i, j) in f with $i < p$, then for each one of them we put (a copy of) the ordered pair (i, j) into g ; i. e., $g(i) := f(i)$,

if $0 < i < p$. Please note: the (i, j) 's are "generic" ordered pairs: (i, j) 's with different i 's have different j 's too.

When we get to $i = p$, there is no ordered pair (p, n) . We have removed it. But we know there is an ordered pair (i, j) in f with $i = s(p)$, because $p < m-1$ and $m-1$ is in S_m . We will replace $(s(p), j)$ with (p, j) . But now there is no ordered pair $(s(p), j)$ — we have changed it.

We will do the same thing we did before — keep modifying ordered pairs until we run out of them.

For each ordered pair (i, j) in f with $i > p$, we know $i > 0$, so there exists one and only one h in N such that $s(h) = i$.

Since $h < i$ (why?), h is in S_{m-1} .

Now we remove the pair (i, j) from f and change (only) the i in (i, j) to h , then we put (h, j) into g . Note that the h for $s(p)$ is p .

This gives, in either case, a function $g: S_{m-1} \rightarrow S_n$.

(5.65) Exercise: Show that g is a one-to-one correspondence. This can be done by examining the proof before this point. It may help to draw a picture of an example-map!

Once the exercise is done, you'll conclude that $m-1 = n$, because n is in E . But then, $m = s(m-1) = s(n)$. Therefore, since m was arbitrary, we have shown that, either $m = s(n)$, or, that there does not exist a one-to-one correspondence $f: S_m \rightarrow S_{s(n)}$.

This means that, **if n is in E , then $s(n)$ is in E** . By induction, $E = N$.

This completes the proof.

This is a place where knowing the meaning of "A implies B" is important!

An important point: we can now define, *mathematically*, something that does the job of saying "how many!"

(5.66) Theorem and Definition and notation (cardinal number (of a finite set)): If S is a subset of some set X , and S is a finite set, then S is empty, or else there exists exactly one n in P such that there exists a one-to-one correspondence $f: S \rightarrow S_n$. In this case, the **cardinal number of S** , denoted **card(S)**, is defined to be **n** . If S is an empty set, we assign to S the cardinal number 0 : **card(\emptyset) = 0** .

Proof: If S is finite and not empty, there exists n in P and a one-to-one correspondence $f: S \rightarrow S_n$.

This is by definition of "finite non-empty set."

If it is also true that there exists m in P and a one-to-one correspondence $g: S \rightarrow S_m$, then the

composite function $g \circ f^{-1}: \mathbf{S}_n \rightarrow \mathbf{S}_m$ is a one-to-one correspondence. By Theorem (5.63) $m = n$. Finally, any two empty subsets of X are equal. This completes the proof.

The Principle of Finite Induction

This is a variant of Mathematical Induction that can be used on sets \mathbf{S}_n instead of \mathbf{N} or \mathbf{P} . We will use Mathematical Induction to prove it!

(5.67) Theorem (The Principle of Finite Induction): Let $n \in \mathbf{P}$, and suppose F is a subset of \mathbf{S}_n that contains 0 , and is such that, if $k \in F$, and $k+1 \in \mathbf{S}_n$, then $k+1 \in F$. Then $F = \mathbf{S}_n$.

Proof: Let S be the subset of \mathbf{N} defined by $S := F \cup \{k \in \mathbf{N} : k \leq n\}$.

Notice that F and $\{k \in \mathbf{N} : k \leq n\}$ are disjoint.

We are given that 0 is in F , so 0 is in S .

Suppose m is in S .

Then $m \in F$, or $m \in \{k \in \mathbf{N} : k \leq n\}$.

If $m \in F$, and $m+1 \in \mathbf{S}_n$, we are given that $m+1 \in F$.

Thus, in case $m \in F$, and $m+1 \in \mathbf{S}_n$, $m+1 \in S$.

If $m \in F$ and $m+1 \notin \mathbf{S}_n$, then $m < n$, but $m+1$ is not less than n .

Thus, $m+1 \leq n$. This means that $m+1 \in \{k \in \mathbf{N} : k \leq n\}$.

But then, $m+1 \in S$.

Now suppose that $m \in S$, and $m \notin F$. Then $m \in \{k \in \mathbf{N} : k \leq n\}$.

But then $m \leq n$, so $m+1 = s(m) \leq n$.

Thus $m+1 \in \{k \in \mathbf{N} : k \leq n\} \subseteq S$.

Hence, for all m in S , $m+1$ is in S .

Since 0 is in S , $S = \mathbf{N}$.

Now $\mathbf{N} = \mathbf{S}_n \cup \{k \in \mathbf{N} : k \leq n\} = S = F \cup \{k \in \mathbf{N} : k \leq n\}$.

(5.68) Exercise: Show that the equation

$$\mathbf{S}_n \cup \{k \in \mathbf{N} : k \leq n\} = F \cup \{k \in \mathbf{N} : k \leq n\},$$

and the disjointness of the sets on each side of it, imply that $\mathbf{S}_n = F$. In this way, you complete the proof of the theorem on the Principle of Finite Induction.

☛ a useful variation on the Principle of Mathematical Induction

Recall the usual form of the Principle of Mathematical Induction:

For all subsets S of \mathbf{N} , if S contains 0, and $s(S) \subseteq S$, then $S = \mathbf{N}$.

Here is the variation, known as **the Second Principle of Mathematical Induction**:

(5.69) For all subsets S of \mathbf{N} , if S contains 0, and, for all n in \mathbf{P} , $S_n \subseteq S$ implies $n \in S$, then $S = \mathbf{N}$.

Here it is again, in less dense form: Suppose that $P(n)$ is a mathematical statement with a free variable n . Suppose:

(0) $P(0)$ is true;

(1) for all n in \mathbf{N} , if $P(m)$ is true for all $m < n$, then $P(n)$ is true;

Then $P(n)$ is true for all n in \mathbf{N} .

(5.70) Special Problem: Prove that the variation (either form) is true. Hint: Well-Ordering.

We can use induction to define some important functions that you already know about.

(5.71) Example: Definition (of the power functions m^n): We'll define first, then set notation.

Define $E_0(m) := 1$ for all m in \mathbf{N} . This definition does not need induction! Now we proceed inductively. If E_n is defined for some n in \mathbf{N} , let $E_{n+1}(m) := mE_n(m)$ for all m in \mathbf{N} . In particular, we have $E_1(m) = m$. For n in \mathbf{P} , let $P(n)$ be the statement "There exists a function $E_n : \mathbf{N} \rightarrow \mathbf{N}$ such that, for all m in \mathbf{N} , $E_n(m) = mE_{n-1}(m)$, where $E_0(m) = 1$ for all m in \mathbf{N} ." We know that $P(1)$ is true. Now suppose that $P(n)$ is true for some n in \mathbf{P} . Then, by defining $E_{n+1}(m) := mE_n(m)$ for all m in \mathbf{N} , we see that $P(n+1)$ is true, because $n = (n+1)-1$ (that is, n is the predecessor of $n+1$). Thus $P(n)$ is true for all n . Notice that the induction was repetitive! In the future, you can follow these steps to ensure that you have a function for each n :

Step 1: Define f_0 (or f_1 , or even f_{17} if that's where you need to start)

Step 2: Define f_{n+1} in terms of f_n .

(5.72) Notation: Let $\mathbf{m}^n = E_n(m)$.

(5.73) Theorem (Laws of Exponents (incomplete)): If $n > 0$, then $0^n = 0$, and $0^0 = 1$. For all $n \in \mathbf{N}$, $1^n = 1$. For all p, q , and n in \mathbf{N} , $(pq)^n = p^nq^n$, and $n^{p+q} = n^pn^q$.

(5.74) Exercise (Laws of exponents, completed):

Prove that, for all $p, q,$ and n in \mathbf{N} , $n^{pq} = (n^p)^q$.

Proof(of Theorem (5.73), not the Exercise): By definition, $0^0 = 1$.

If $n > 0$, then $0^n = E_n(0) = 0E_{n-1}(0) = 0$.

By definition, $1^0 = 1$. If $n \in \mathbf{N}$, and $1^n = 1$ then $1^{n+1} = E_{n+1}(1) = 1E_n(1) = 1$.

To show that, for all $p, q,$ and n in \mathbf{N} , $(pq)^n = p^n q^n$, we use induction. Let

$$S := \{ n \in \mathbf{N} : \text{for all } p \text{ and } q \text{ in } \mathbf{N}, (pq)^n = p^n q^n \}.$$

First, $0 \in S$ because $(pq)^0 = 1 = 1 \times 1 = p^0 q^0$, for all p and q in \mathbf{N} .

Now suppose $n \in S$.

Then $(pq)^{n+1} = E_{n+1}(pq) = pqE_n(pq) = pqE_n(p)E_n(q) = (pE_n(p))(qE_n(q)) = E_{n+1}(p)E_{n+1}(q)$, by definition.

Thus, $n+1 \in S$, so $S = \mathbf{N}$. That is, For all $p, q,$ and n in \mathbf{N} , $(pq)^n = p^n q^n$.

To show that, for all $p, q,$ and n in \mathbf{N} , $n^{p+q} = n^p n^q$, let

$$S := \{ p \in \mathbf{N} : \text{for all } n \text{ and } q \text{ in } \mathbf{N}, n^{p+q} = n^p n^q \}.$$

Does $0 \in S$? We have $n^{0+q} = n^q$, and $n^0 n^q = n^q$. Thus for all n and q in \mathbf{N} , $n^{0+q} = n^0 n^q$, as

desired. Suppose $p \in S$. Then $n^{(p+1)+q} = n^{(p+q)+1} = E_{(p+q)+1}(n) = nE_{p+q}(n) = n n^{p+q} = n n^p n^q$

(by the induction hypothesis) $= nE_p(n)n^q = E_{p+1}(n)n^q = n^{p+1}n^q$, as desired.

It follows (why?) that for all $p, q,$ and n in \mathbf{N} , $n^{p+q} = n^p n^q$.

This completes the proof of the Theorem.

(5.75) Exercise: Show that, if $p > 0$, and $m < n$, then $m^p < n^p$.

(5.76) Exercise: Show that, if $n > 1$, and $p < q$, then $n^p < n^q$.

(5.77) Exercise: Show that, for all p in \mathbf{N} , $2^p > p$.

☛ topology on \mathbf{N} , and on \mathbf{N} “with a point at infinity”

The **usual topology** for \mathbf{N} is its discrete topology, consisting of all subsets of \mathbf{N} .

Thus, any function that has \mathbf{N} as its domain, and some topological space Y as its range space, is continuous. As you can guess, we don't use this topology much.

The story is *quite* different when we tack on a point that sits just “above” \mathbf{N} ! This new point is called **the first infinite ordinal**, and is denoted ω . We won't go into what happens when we

continue with the successors of ω . That is part of advanced Set Theory — the theory of ordinal numbers. Our interest is in the topology we will construct for $\mathbf{N} \cup \{\omega\}$, denoted by $\overline{\mathbf{N}}$. The topology we make will give us the basic ideas behind convergent sequences. The discussion that follows is introductory, intuitive and informal.

(5.78) Definition: A subset U of $\overline{\mathbf{N}}$ is **an open set in the usual sense** if $U \subseteq \mathbf{N}$, that is, if U does not contain ω , but, if $\omega \in U$, then, in order for U to be open in the usual sense, U must contain all the natural numbers from some n_0 on.

In other words, if $\omega \in U$, then U is open in the usual sense

if there exists n_0 such that $\{n \in \mathbf{N} : n \geq n_0\} \subseteq U$.

Examples: Every subset of \mathbf{N} is open in the usual sense. Is $\overline{\mathbf{N}}$ open? It would have to be, in order for “open in the usual sense” to define a topology. And $\overline{\mathbf{N}}$ is open in the usual sense, because there exists n_0 such that $\{n \in \mathbf{N} : n \geq n_0\} \subseteq \overline{\mathbf{N}}$, namely $n_0 := 0$. Now here is a non-example: the set that consists of ω , together with all the even natural numbers, is NOT open in the usual sense because the set contains no odd numbers, and every set of the form $\{n \in \mathbf{N} : n \geq n_0\}$ contains odd numbers, hence can't be contained in our constructed set. On the other hand, the set of all the even natural numbers is open in the usual sense!

The point is, the sets that contain ω that are open in the usual sense contain *all* sufficiently large natural numbers! This is where the intuitive idea of a convergent sequence comes in — a sequence $\{x_n\}$ converges to a point x_ω in a topological space X if “ x_n gets closer and closer to x_ω as n gets large.” In topological terms, we notice that $\{x_n\}$ is a function with domain \mathbf{N} and range X . We'll regard \mathbf{N} as a subset of $\overline{\mathbf{N}}$, and recall the definition of “ $\{x_n\}$ has a limit at ω ” (see (4.073)). It said that the inverse image of each neighborhood of x_ω contains a deleted neighborhood of ω . For us right now, that means: the set of all n in \mathbf{N} (note that ω is not mentioned — ω got deleted) such that x_n is in the given neighborhood of x_ω contains all the natural numbers from some n_0 onwards.