

Inductive sets (used to define the natural numbers as a subset of \mathbb{R})

(1) **Definition:** A set $S \subseteq \mathbb{R}$ is an *inductive set* if $0 \in S$ and if, whenever $x \in S$ then $x + 1 \in S$.

In “logic” this is $(\forall S \subseteq \mathbb{R})(S \text{ is an inductive set} \iff [(0 \in S) \wedge (\forall x \in \mathbb{R})(x \in S \Rightarrow x + 1 \in S)])$.

Examples

\mathbb{R} is inductive, because 0 is a real number and because for all real numbers x , it is true that $x + 1 \in \mathbb{R}$.

The set $S_0 := [0, +\infty)$ ($= \{x \in \mathbb{R} : x \geq 0\}$) is inductive too.

It takes more care to show that $S_1 := \{0\} \cup [1, +\infty)$ is inductive. To do so, we begin by noting that $0 \in S_1$ “by construction.” To show that $x \in S_1 \Rightarrow x + 1 \in S_1$ we assume that $x \in S_1$, and consider two cases: $x = 0$ and $x \in [1, +\infty)$. If $x = 0$ then $x + 1 = 1 \in [1, +\infty) \subseteq S_1$, so “ $x \in S_1 \Rightarrow x + 1 \in S_1$ ” is true when $x = 0$. In the other case, x is a real number that is at least one: $x \geq 1$. If we add 1 to both sides of this inequality, the (new) inequality $x + 1 \geq 1 + 1$ is true (this is one of the things we take for granted), and $1 + 1 > 1$ since $1 \in P$. Thus by the transitivity of inequality (another thing to take for granted), $x + 1 \geq 1$, so $x + 1 \in [1, +\infty) \subseteq S_1$.

But $S := \{0\} \cup (1, +\infty)$ is *not* inductive! This is because $0 + 1 \notin S$.

Definition of \mathbb{N} :

The set \mathbb{N} of natural numbers is defined to be the set of all real numbers that are contained in every inductive set.

We will see that, in other words, \mathbb{N} is the *smallest* inductive set. In symbols, the definition reads

$$\mathbb{N} := \bigcap_{S \text{ is inductive}} S.$$

To express the Definition “in logic,” it will be useful to have some notation: we let \mathcal{J} denote the collection (synonymous with “set”) of *all* inductive subsets of \mathbb{R} . That is, $S \in \mathcal{J} \iff S$ is an inductive set. Then

$$(2) \quad \mathbb{N} := \{x \in \mathbb{R} : (\forall S \in \mathcal{J})(x \in S)\}.$$

This equation will be our official definition of \mathbb{N} . The equation only uses set axioms and the axioms for \mathbb{R} .

Since every inductive set must contain 0 , it is certainly true that $0 \in \mathbb{N}$. Moreover, if $x \in \mathbb{N}$, it is true that $x + 1 \in \mathbb{N}$. This is true because this particular x is in every inductive set S , by definition of \mathbb{N} . But then $x + 1 \in S$, for every inductive set S . Thus $x + 1$ belongs to every inductive set, and so $x + 1 \in \mathbb{N}$.

We have proved:

(3) **Theorem:** The set \mathbb{N} of natural numbers is an inductive set.

This was all we needed to know about \mathbb{N} in order to prove, using the **Completeness Axiom**, that \mathbb{N} is not bounded above! Let us state that Theorem here.

(4) **Theorem:** The set \mathbb{N} of natural numbers is not bounded above.

(5) **Exercise:** Prove that for all $n \in \mathbb{N}$, $n \geq 0$. That is, 0 is the least element of \mathbb{N} . Hint: Use S_0 , above.

The next Theorem is easy to prove, but it is very important!

(6) **Theorem:** If $S \subseteq \mathbb{N}$ and S is an inductive set, then $S = \mathbb{N}$.

Proof: By (1), every element x in \mathbb{N} is in every inductive set. Since S is given to be an inductive set, every element x in \mathbb{N} is in S , and this proves that $\mathbb{N} \subseteq S$.

This Theorem says that \mathbb{N} is the smallest inductive set. This Theorem has another name too! It is known as “The Principle of Mathematical Induction!” However, the Principle of Mathematical Induction is usually stated in a different way!

Mathematical Induction

Sometimes we can prove theorems of the form $(\forall n \in \mathbb{N})P(n)$ (which is read "For all n in \mathbb{N} , $P(n)$ is true") in two steps:

First step: Prove (that) $P(0)$ (is true).

We then prove that, if $P(n)$ is true, then $P(n+1)$ is true. Of course, there is a "missing" quantifier! We are to actually carry out the

Second step: Prove that $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$ is true.

Conclusion: $(\forall n \in \mathbb{N})P(n)$ is true.

The Principle of Mathematical Induction is actually a Theorem!

(7) Theorem (The Principle of Mathematical Induction): Suppose that, for each $n \in \mathbb{N}$, we are given a mathematical statement $P(n)$. Suppose, in addition, that

- (i) $P(0)$ is true
and
(ii) $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$ is true.

Then

$$(\forall n \in \mathbb{N})P(n) \text{ is true.}$$

Proof: Let $S := \{n \in \mathbb{N} : P(n)\}$. We will prove that S is an inductive set contained in \mathbb{N} , so that by Theorem (6), $P(n)$ is true for all $n \in \mathbb{N}$.

By (i), $P(0)$ is true, so $0 \in S$. Next, suppose that $n_o \in S$, meaning $P(n_o)$ is true. From (ii) we deduce that $P(n_o) \Rightarrow P(n_o+1)$ is true. But then, from the truth table for implication, we deduce that $P(n_o+1)$ is true. Thus $n_o+1 \in S$. Since n_o was an arbitrary element of S , we deduce that $(\forall n \in S)(n \in S \Rightarrow n+1 \in S)$ is true. Hence S is an inductive set, and by the definition of S , $S \subseteq \mathbb{N}$. By Theorem (6), $S = \mathbb{N}$. This says that $P(n)$ is true for all $n \in \mathbb{N}$.

The Peano Postulates (or Axioms)

In principle, we can use the four following statements as our fundamental axioms, then define the integers, the rational numbers and finally the real numbers. It would take about one semester to do all that. Instead, we have begun by assuming the Axioms for the Real Numbers as our basic statements. Thus the Peano Postulates are not (for us) postulates at all. They are definitions or theorems. First we state them in a precise form, followed by a vague version. After all that we'll deal with them in turn.

(P1) There exists a non-empty set \mathbb{N} , whose elements we will call *natural numbers*.

(P2) There exists a one-to-one function $s : \mathbb{N} \rightarrow \mathbb{N}$, that we will call the *successor function*.

(P3) There exists an element $0 \in \mathbb{N}$ such that 0 is not in the image, $s(\mathbb{N})$, of s .

(P4) For all subsets S of \mathbb{N} , if S contains 0 , and $s(S) \subseteq S$, then $S = \mathbb{N}$.

According to the Encyclopedia Britannica, 15th edition, 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.

The statement (P1) is introductory; it is there to provide a "context" for the following statements. We defined \mathbb{N} in (2), and \mathbb{N} is nonempty because it contains 0 . Thus (P1) is true.

The function s defined by $s(n) := n + 1$ is the one we use in (P2). We have to prove that s is one-to-one. Thus we suppose that $s(m) = s(n)$, where $m \in \mathbb{N}$ and $n \in \mathbb{N}$. We have to show that $m = n$. We use the fact that m and n and 1 are real numbers. We are given that $m + 1 = n + 1$. In Axiom (4) we select $x = 1$, and obtain w such that $1 + w = 0$. Then

$$\begin{aligned} m &= m + 0 \quad (\text{Axiom (3)}) \\ &= m + (1 + w) \quad (\text{Substitution of } 1 + w \text{ for } 0) \\ &= (m + 1) + w \quad (\text{Associativity, Axiom (1)}) \\ &= (n + 1) + w \quad (\text{Substitution of } n + 1 \text{ for } m + 1) \\ &= n + (1 + w) \quad (\text{Assoc.}) \\ &= n + 0 = n \quad (\text{Substitution of } 0 \text{ for } 1 + w, \text{ then Axiom (3)}). \end{aligned}$$

Thus (P2) is true. If we had proved the Cancellation Law for Addition, we could have simply written:

$$“m + 1 = n + 1 \Rightarrow m = n, \text{ by (additive) cancellation.}”$$

Were we starting with the Peano Postulates, we would not have the operation of addition yet!

There is something strange about (P3), as it asserts the existence of an element of \mathbb{N} with a special property. That element is 0, which we already know about. The statement has to stand as it is, in case it is the Peano Axioms that we *start* with! We are here making a real (pun intended) “model” of \mathbb{N} . So all we need to do is prove that for all $n \in \mathbb{N}$, $0 \neq s(n) = n + 1$. We return to the real numbers, since $\mathbb{N} \subseteq \mathbb{R}$. Suppose, to the contrary, that $0 = n + 1$ for some $n \in \mathbb{N}$. Then $n \neq 0$ since $0 \neq 1$ by Axiom (10). But n cannot be positive either, since then $0 = n + 1$ would be positive (Axiom (?)). Thus $n \notin [0, +\infty)$. But then, n cannot be a natural number, because $\mathbb{N} \subseteq [0, +\infty)$. This contradiction shows that for all $n \in \mathbb{N}$, $s(n) = n + 1 \neq 0$. Thus (P3) is true.

Finally, (P4) is really Theorem (6) in disguise. For, $0 \in S$ and $s(S) \subseteq S$ says that S is an inductive subset of \mathbb{N} , so by Theorem (6), $S = \mathbb{N}$.

Here are the details: S is given to be a subset of \mathbb{N} . It is given that $0 \in S$. We have to verify that, for all $n \in S$, $n + 1 \in S$. But $n + 1 = s(n)$, and we are given that $s(S) \subseteq S$, which means that for every $n \in S$, $n + 1 = s(n) \in S$, so S is inductive. The hypotheses of Theorem (6) are true, hence so is its conclusion, namely $S = \mathbb{N}$.

Sequences A *sequence* is a function with domain \mathbb{N} . Nothing has yet been said about the range space of the function. Here is the official definition, of a sequence in a set X .

(7.1) **Definition** Let X be a non-empty set. A *sequence in X* is a function with domain \mathbb{N} and range X .

If $x : \mathbb{N} \rightarrow X$ is a sequence, we usually write x_n instead of $x(n)$. This emphasizes the intuitive idea that a sequence is an *ordered list* of elements of X , in the sense that there is a first one, then a second one and so on. We distinguish between a *term* x_n of a sequence and we write $\{x_n\}$ for the sequence as a whole.

You have seen sequences that follow a repeatedly applied rule. For example, the Fibonacci sequence is usually described by the requirements that $F_0 = 1$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. This way of defining a sequence is called “definition by induction.” To be sure that this sequence actually exists as a function that is defined for every $n \in \mathbb{N}$, and not just for the n ’s that we can compute it for before we tire, we need a Theorem that uses the Peano Postulates and Set Theory.

The Recursive Sequence Theorem: used to justify “definition by induction”

Introduction (may be skipped) The Recursive Sequence Theorem is an Existence and Uniqueness Theorem. It asserts the existence of a certain kind of function with domain \mathbb{N} (or \mathbb{Z}^+) and *any* specified non-empty range space X .

Let’s look at another example: Let $x_1 := 1$, and decree that for each $n \geq 1$, $x_{n+1} = \frac{1}{2} \left(\frac{2}{x_n} + x_n \right)$. This is a “definition by induction.” If you are bothered by this, you are absolutely right! Does this process *really* define a sequence? The answer is that it does, but a Theorem is needed to connect \mathbb{N} and the set theory that is needed to define functions.

We defined a function to be a set of ordered pairs. The ordered pairs here are not actually specified, as they are in the definition $F_n := \frac{n(n+1)}{2}$. The Recursive Sequence Theorem justifies this definition. See [1] and [2, p 48].

(10) **Recursive Sequence Theorem:** *Let X be a non-empty set, and suppose that $x_0 \in X$. Suppose also that $H : X \times \mathbb{N} \rightarrow X$ is a function. Then there exists a unique sequence $s : \mathbb{N} \rightarrow X$ such that $s_0 = x_0$ and such that for all $n \in \mathbb{N}$, $s_{n+1} = H(s_n, n)$.*

Proof of existence: Our objective is to construct a set s of ordered pairs that has the properties of a function $s : \mathbb{N} \rightarrow X$, and another property. We will begin by using set-selector notation to select unimaginably many sets of ordered pairs! We define a family \mathcal{G}_0 of subsets of $\mathbb{N} \times X$ by

$$\mathcal{G}_0 := \{U \in 2^{\mathbb{N} \times X} : (0, y_0) \in U \text{ and } (\forall n \in \mathbb{N})(\forall x \in X)((n, x) \in U \Rightarrow (n+1, H(x, n)) \in U)\}.$$

In words, \mathcal{G}_0 is the family of all sets U of ordered pairs in $\mathbb{N} \times X$ such that $(0, x_0) \in U$ and, whenever $(n, x) \in U$, then $(n+1, H(x, n)) \in U$ as well. Since $\mathbb{N} \times X$ contains all possible ordered pairs of natural numbers n and elements x of X , $\mathbb{N} \times X \in \mathcal{G}_0$. Thus \mathcal{G}_0 is a non-empty family of non-empty sets.

The set s of ordered pairs we want is the set of all ordered pairs that are in every one of the sets $U \in \mathcal{G}_0$. Before we define the set s in detail, let's check that it can "act" like a function. We define

$$E_0 := \{n \in \mathbb{N} : \text{there exists } x \in X \text{ such that } (n, x) \in U \text{ for all } U \in \mathcal{G}_0\}.$$

Let us show that every natural number n is in E_0 . This will show that when we form the set s of all ordered pairs in $\mathbb{N} \times X$ that are in every $U \in \mathcal{G}_0$ (we have a notation for this: $s = \bigcap_{U \in \mathcal{G}_0} U$), it will be true that for every $n \in \mathbb{N}$

there exists $x \in X$ such that $(n, x) \in s$. This is one of the requirements s must satisfy if s is to be a function from \mathbb{N} to X .

Proof that $E_0 = \mathbb{N}$: We will use induction. By our definition of \mathcal{G}_0 , $(0, x_0) \in U$ for every $U \in \mathcal{G}_0$. Thus $0 \in E_0$. Now we suppose that $n \in E_0$. This means that there is some $x \in X$ such that (n, x) belongs to every $U \in \mathcal{G}_0$. But $(n, x) \in U \in \mathcal{G}_0$ means that $(n+1, H(x, n)) \in U \in \mathcal{G}_0$. Therefore, for every $U \in \mathcal{G}_0$, $(n+1, H(x, n)) \in U$, so $n+1 \in E_0$. But then E_0 satisfies the conditions in the Induction Axiom, so $E_0 = \mathbb{N}$.

Now we officially define the set s :

$$s := \bigcap_{U \in \mathcal{G}_0} U, \text{ the set of all ordered pairs } (n, x) \text{ that are in every } U \in \mathcal{G}_0.$$

(11) **Exercise:** *Prove that $s \in \mathcal{G}_0$.*

(12) **Exercise:** *Prove that s is the smallest set in \mathcal{G}_0 .*

To prove that s is (the graph of) a function with domain \mathbb{N} and range X , we have to verify two things:

- (i) For every $n \in \mathbb{N}$ there exists $x \in X$ such that $(n, x) \in s$;
- (ii) For all n in \mathbb{N} and all x_1 and x_2 in X , if $(n, x_1) \in s$ and $(n, x_2) \in s$ then $x_1 = x_2$.

We already showed that (i) is true for s , because for every $n \in \mathbb{N}$, there is an $x \in X$ such that $(n, x) \in U$ for every $U \in \mathcal{G}_0$. Therefore $(n, x) \in s$.

To verify (ii) we might begin by supposing that $(n, x_1) \in s$ and $(n, x_2) \in s$. We would then have to show that $x_1 = x_2$. We will do this, but by induction. We define

$$E_1 := \{n \in \mathbb{N} : (\forall x_1 \in X)(\forall x_2 \in X)((n, x_1) \in s \wedge (n, x_2) \in s) \Rightarrow [x_1 = x_2]\}.$$

If we can show that $E_1 = \mathbb{N}$, this will show, for arbitrary $n \in \mathbb{N}$ and arbitrary x_1 and x_2 in X , that whenever $(n, x_1) \in s$ and $(n, x_2) \in s$ then $x_1 = x_2$. **In other words, $n \in E_1$ means that the x such that $(n, x) \in s$ is unique.**

Proof that $E_1 = \mathbb{N}$: We will use this idea: assume the contrary, and then construct sets in \mathcal{G}_0 that are *strictly smaller* than s . Since s is the smallest set in \mathcal{G}_0 , this will give the desired contradictions.

By our definition of s , $(0, x_0) \in s$. If also $(0, y_0) \in s$ and $y_0 \neq x_0$, we construct a new set $U' := s \setminus \{(0, y_0)\}$.

Claim: the set U' is in \mathcal{G}_0 . To prove the Claim, we take two steps, as follows.

First, $(0, x_0) \in s$, and, since $x_0 \neq y_0$, $(0, x_0) \in s \setminus \{(0, y_0)\} = U'$. Thus $(0, x_0) \in U'$.

Second, if $(m, x) \in U'$ then $(m, x) \in s$, so $(m+1, H(x, m)) \in s$. Moreover, $(m+1, H(x, m)) \neq (0, y_0)$ because $m+1 \neq 0$ for any m . Therefore $(m+1, H(x, m)) \in s \setminus \{(0, y_0)\} = U'$. Thus $(m, x) \in U' \Rightarrow (m+1, H(x, m)) \in U'$.

Therefore $U' \in \mathcal{G}_0$. But U' is s with one element removed, so U' is strictly smaller than the smallest set in \mathcal{G}_0 . This is a contradiction, so $0 \in E_1$.

We assume $n \in E_1$, and seek to show that this implies $n+1 \in E_1$. Again we proceed by contradiction, assuming that $n+1 \notin E_1$. Since $n \in E_1$, $(n, x) \in s$ for a *unique* $x \in X$. Then $(n+1, H(x, n)) \in s$. However, by our assumption of the contrary, there is also some $y_1 \in X$ such that $y_1 \neq H(x, n)$ and $(n+1, y_1) \in s$ as well. We construct another set, $U'' := s \setminus \{(n+1, y_1)\}$.

Our strategy again is to show that $U'' \in \mathcal{G}_0$. As before, this will give a contradiction.

Once again, $(0, x_0) \in U''$ because $0 \neq n+1$ for any natural number means that $(0, x_0) \neq (n+1, y_1)$.

Now we suppose that $(m, y) \in U''$. Then $(m, y) \in s$, so $(m+1, H(y, m)) \in s$.

To show that $(m+1, H(y, m)) \in U''$ we consider two cases: $m \neq n$ and $m = n$.

If $m \neq n$, we have $m+1 \neq n+1$, so $(m+1, H(y, m)) \neq (n+1, y_1)$. Thus $(m+1, H(y, m)) \in s \setminus \{(n+1, y_1)\} = U''$. That is, when $m \neq n$, $(m, y) \in U'' \Rightarrow (m+1, H(y, m)) \in U''$.

Finally we have to deal with the case $m = n$. Here, $(m, y) = (n, y) \in s$, so $y = x$ (by uniqueness, because $n \in E_1$) and therefore $(m+1, H(y, m)) = (n+1, H(x, n)) \in s$.

Since $y_1 \neq H(x, n)$, $(m+1, H(y, m)) = (n+1, H(x, n)) \neq (n+1, y_1)$.

Hence $(m+1, H(y, m)) = (n+1, H(x, n)) \in U''$. Thus $U'' \in \mathcal{G}_0$, which gives a contradiction. We have proved that $n+1 \in E_1$, so $E_1 = \mathbb{N}$. Hence (ii) is true for s so s is a function.

Proof of uniqueness: Suppose s and s' satisfy the conditions of the Theorem. That is, $s_0 = x_0 = s'_0$ and for all $n \in \mathbb{N}$, $s_{n+1} = H(s_n, n)$ and $s'_{n+1} = H(s'_n, n)$. We define the set

$$E_2 := \{n \in \mathbb{N} : s_n = s'_n\}.$$

To show that $s' = s$ all we have to do is show that $E_2 = \mathbb{N}$. We use induction. We are given that $0 \in E_2$. If $n \in E_2$, then $s'_n = s_n$. But then $s'_{n+1} = H(s'_n, n) = H(s_n, n) = s_{n+1}$. The second equality is by substitution. The first and third equalities are given. Thus $n+1 \in E_2$, so $E_2 = \mathbb{N}$ and so $s' = s$.

This completes the proof of the Recursive Sequence Theorem.

Examples

(13) With $X = \mathbb{R}$ and $H(t, n) = xt$, and $x_0 = 1$, the Recursive Sequence Theorem, gives the sequence $\{x^n\}$, namely $1, x, x^2, x^3, \dots, x^n, \dots$ of *powers of x* , or $x_n = x^n$. We notice: this $H(x, n)$ does not depend on n .

(14) Suppose we are given a sequence $\{x_n\}$ of real numbers. With $X = \mathbb{R}$, $s_0 = x_0$ and $H(x, n) = x + x_n$ the Recursive Sequence Theorem gives the sequence $\{s_n\}$ of *partial sums* of $\{x_n\}$:

$$s_0 = x_0; s_1 = s_0 + x_1 = x_0 + x_1; s_2 = s_1 + x_2 = x_0 + x_1 + x_2; \dots \text{ we usually write } \sum_{k=0}^n x_k \text{ for } s_n.$$

(15) Prove that for all natural numbers n , $n < 2^n$. Note: 2^n was actually *defined* inductively in (13): We put $2^0 := 1$, and for arbitrary $n \in \mathbb{N}$ we defined $2^{n+1} := 2 \cdot 2^n$.

Proof: First we need to know that, for all $n \in \mathbb{N}$, $2^n \geq 1$. You should prove this as an exercise!

We will use induction. We let $P(n)$ denote the assertion “ $n < 2^n$.” Then $0 < 1 = 2^0$ so $P(0)$. (Now we suppose that $n \in \mathbb{N}$ is arbitrary.) If $P(n)$, then $n < 2^n$, so $n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$. Here, we have used Exercise (5) and manipulations that we take for granted. That is, $P(n) \Rightarrow P(n + 1)$ is true for arbitrary $n \in \mathbb{N}$, as desired.

(16) Prove that for all natural numbers $n > 2$, $n \leq 2^{(n-1)} - 1$. Here we have a problem: what is our statement $P(n)$ going to be? Here is one (messy) way to cope: we let $P(n)$ denote the statement “ $n > 2 \Rightarrow n \leq 2^{(n-1)} - 1$.” You should verify that “ $n \leq 2^{(n-1)} - 1$ ” is false for $n = 1$ and $n = 2$, but true for $n = 3$. With this version of $P(n)$, $P(1)$ and $P(2)$ are true “vacuously,” because the antecedent is false in each case. (In a statement of the form $A \Rightarrow B$, A is called the “antecedent,” and B is called the “consequent.”) When $n = 3$, “ $n > 2$ ” is true, so the only way $P(3)$ can be true is for “ $n \leq 2^{(n-1)} - 1$ ” to be true when $n = 3$. You have checked that it is, so now we assume that $m \geq 3$ and that $P(m)$ is true. Thus “ $m > 2 \Rightarrow m \leq 2^{(m-1)} - 1$ ” is true, and $m \geq 3$. We deduce that “ $m \leq 2^{(m-1)} - 1$ ” is true, and we need to show that “ $m + 1 \leq 2^m - 1$ ” is therefore true in order for $P(m + 1)$ to be true (again, because $m + 1 > m \geq 3$). Since $m \leq 2^{(m-1)} - 1$, we know $m + 1 \leq (2^{(m-1)} - 1) + 1$. Since $2^{(m+1)-1} = 2^m = 2^{(m-1)} + 2^{(m-1)}$ we have $2^{(m-1)} = 2^m - 2^{(m-1)}$ and so

$$(17) \quad m + 1 \leq (2^m - 2^{(m-1)} - 1) + 1 = (2^{(m+1)-1} - 1) - (2^{(m-1)} - 1).$$

We apply “ $m \leq 2^{(m-1)} - 1$ ” once more, and multiply through by -1 : $-(2^{(m-1)} - 1) \leq -m \leq -3 < 0$. We substitute the inequality $-(2^{(m-1)} - 1) < 0$ into (17), ignoring intermediate terms, and find that

$$(18) \quad m + 1 \leq (2^{(m+1)-1} - 1) - (2^{(m-1)} - 1) < 2^{(m+1)-1} - 1.$$

We have thus shown, for an arbitrary $m \in \mathbb{N}$, that $P(m)$ is true. Thus, if $n > 2$, $n \leq 2^{(n-1)} - 1$. We actually showed more (can you see why? say why?):

$$n > 2 \Rightarrow n \leq 2^{(n-1)} - 1 \quad \text{and} \quad n > 3 \Rightarrow n < 2^{(n-1)} - 1.$$

(19) Prove that for all natural numbers $n > 3$, $n^2 \leq 2^n$. Again we have the problem of the few “exceptional” values of n at the beginning of \mathbb{N} . What we can do is to extend the definition of “inductive set.” Given $n_o \in \mathbb{N}$, we say that a set S is an “inductive set starting at n_o ” if $n_o \in S$ and, for all $n \in S$, we know that $n + 1 \in S$. Now we can start our induction at n_o , and avoid the smaller values of n .

In the problem at hand, we let $P(n)$ denote the statement “ $n^2 \leq 2^n$.” We take $n_o = 4$. Then $n_o^2 = 16 = 2^{n_o}$, so $P(4)$ is true. Now we assume $P(n)$ for some $n \geq n_o$. We want to show $P(n + 1)$, namely “ $(n + 1)^2 \leq 2^{(n+1)}$.” We start on the left and try to arrive at the right, using intermediate quantities that are only allowed to increase relative to the quantities on their left:

$$\begin{aligned} (n + 1)^2 &= n^2 + 2n + 1 \\ &\leq 2^n + 2n + 1 \quad (\text{by } P(n)) \\ &< 2^n + 2(2^{n-1} - 1) + 1 \quad (\text{by (16)}) \\ &= 2^n + 2^n - 2 + 1 \quad (\text{“arithmetic”}) \\ &= 2^{n+1} - 1 < 2^{n+1}. \end{aligned}$$

Thus $P(n)$ for all $n \geq 4$. Again, we have shown more: when $n > 4$, the inequality is strict.

(20) Prove that for all natural numbers $n > 15$, $n^4 \leq 2^n$. Our desired result can be rewritten “ $\frac{n^4}{2^n} \leq 1$ for $n > 15$.”

We can approach this in two steps: Prove that if we define $x_n := \frac{n^4}{2^n}$, then (i) $\{x_n\}$ is a decreasing sequence, and (ii) $x_{16} = 1$. We will then have $x_n \leq x_{16} = 1$ if $n > 15$. There are two common methods we might use to show that $\{x_n\}$ is a decreasing sequence. The first is to show that $x_n - x_{n+1} \geq 0$ for all $n > 15$. The other common method is to show that $x_{16} = 1$ and $\frac{x_{n+1}}{x_n} \leq 1$ for all $n > 15$.

First common method:

$$x_n - x_{n+1} = \frac{n^4}{2^n} - \frac{(n+1)^4}{2^{(n+1)}} = \frac{2n^4 - (n+1)^4}{2^{(n+1)}}.$$

Since the denominator is positive, all we need to do is show that the numerator is non-negative for $n > 15$. We notice that $n^k < n^\ell$ if $n > 1$ and $k < \ell$, both being natural numbers. Do we need induction for that? Now our numerator is

$$n^4 - 4n^3 - 6n^2 - 4n - 1 > n^4 - 15n^3 > n^4 - n^4 = 0, \text{ if } n > 15.$$

Thus $\{x_n\}$ is a decreasing sequence for $n > 15$. Next we look at x_{16} :

$$x_{16} = \frac{16^4}{2^{16}} = \frac{(2^4)^4}{2^{16}} = 1.$$

Once more we have proved more: $x_n < 1$ if $n > 16$, and $x_{16} = 1$.

Second common method:

$$\frac{x_{n+1}}{x_n} = \frac{(n+1)^4}{2n^4} = \frac{1}{2} \left(1 + \frac{1}{n}\right)^4.$$

The quantity $\left(1 + \frac{1}{n}\right)^4$ is easily shown to decrease (can you show it?). Thus all we have to do is compute $\frac{1}{2} \left(1 + \frac{1}{16}\right)^4$ and hope that it's at most 1. The size estimation can be done easily even without a calculator. It is, for example, definitely less than 7/10.

Some obvious properties of \mathbb{N} that have to be proved

(21) **Theorem:** For all $n \in \mathbb{N}$, if $n > 1$ then $n - 1 \in \mathbb{N}$.

Proof: This proof is not at all obvious! We will use a "construction" in the proof that will be useful later as well, so we begin by defining the construction, then state and prove a Lemma that asserts the useful property of the construction.

(22) **Definition:** If $S \subseteq \mathbb{R}$, we define a set $\tau(S)$ by

$$\tau(S) := \{0\} \cup (S + 1), \text{ where } S + 1 := \{y + 1 : y \in S\} = \{x \in \mathbb{R} : (\exists y \in S)(x = y + 1)\}.$$

There are actually two definitions here; $S + 1$ is called the *translation* of S to the right by 1. Here translation means "change in location;" everything in S is moved to the right by 1 to form the new set $S + 1$.

(23) **Lemma:** If S is an inductive set, so is $\tau(S)$.

Proof: There is a missing quantifier in the statement of the Lemma!

By construction, $0 \in \tau(S)$. Since $0 \in S$, the number $1 = 0 + 1 \in S + 1 \subseteq \tau(S)$. Thus, if $x \in \tau(S)$ and $x \neq 0$, then $x + 1 \in \tau(S)$. If $x \in \tau(S)$ and $x \neq 0$, then $x \in S + 1$, so there exists $y \in S$ such that $x = y + 1$. Thus $x = y + 1 \in S$ because S is an inductive set. Thus by construction $x + 1 \in S + 1 \subseteq \tau(S)$. This completes the proof that $\tau(S)$ is an inductive set.

We can now return to the proof of (21). Since \mathbb{N} is an inductive set, so is $\tau(\mathbb{N})$, by (23). But $0 \in \mathbb{N}$, and for all $n \in \mathbb{N}$, $n + 1 \in \mathbb{N}$ since \mathbb{N} is an inductive set. Moreover, by construction, $n + 1 \in (\mathbb{N} + 1)$. Therefore $\mathbb{N} + 1 \subseteq \mathbb{N} \subseteq \tau(\mathbb{N})$. Hence $\tau(\mathbb{N})$ is an inductive set that is contained in \mathbb{N} . By Theorem (6), $\tau(\mathbb{N}) = \mathbb{N}$.

Now we can prove that if $n \in \mathbb{N}$ and $n > 1$ then $n - 1 \in \mathbb{N}$. For then $n \in \tau(\mathbb{N})$ but $n \neq 1$, so $n \in (\mathbb{N} + 1)$. This means that there exists $m \in \mathbb{N}$ such that $n = m + 1$, so $n - 1 = m \in \mathbb{N}$!

(24) **Remark:** The set S_1 defined earlier to be $\{0\} \cup [1, +\infty)$ can be expressed as $\tau([0, +\infty))$. Since $[0, +\infty)$ is an inductive set, so is S_1 . Thus $\mathbb{N} \subseteq S_1$. Now $S_1 \cap (0, 1) = \emptyset$, by inspection. What this means in words is that **there are no natural numbers strictly between 0 and 1**, another obvious property of \mathbb{N} that requires proof! And we just proved it.

A natural question now arises: what about the non-existence of natural numbers between n and $n+1$, for arbitrary $n \in \mathbb{N}$?

To answer this question in the affirmative let us construct a sequence of sets that will help.

(25) **Definition:** Let $S_0 := [0, +\infty)$. For all $n \in \mathbb{N}$, if S_n is defined, let $S_{n+1} := \tau(S_n)$.

Does this make sense? Does this really define a set S_n for every $n \in \mathbb{N}$? We use the Recursion Theorem here, to produce a sequence $\{S_n\}$ of sets. With $X = 2^{\mathbb{R}}$, $H(x, n) = \tau(x)$ (here, x stands for a set!) and $x_0 = S_0$ we get the sequence we want.

(26) **Exercise:** Prove that each S_n is an inductive set.

(27) **Theorem:** For all $n \in \mathbb{N}$, if $n > 0$ then $S_n \cap (n-1, n) = \emptyset$.

Proof: Let us use Mathematical Induction, starting with 1. We can let $P(n)$ be the statement " $S_n \cap (n-1, n) = \emptyset$." We showed in Remark (24) that $P(1)$.

If $P(n)$ we consider the set

$$S_{n+1} \cap (n, n+1) = (\{0\} \cup [S_n + 1]) \cap (n, n+1).$$

This has the form $(A \cup B) \cap C$, and we know that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, so

$$\begin{aligned} S_{n+1} \cap (n, n+1) &= (\{0\} \cap (n, n+1)) \cup ([S_n + 1] \cap (n, n+1)) \\ &= \emptyset \cup ([S_n + 1] \cap (n, n+1)) \quad \text{because } 0 \notin (n, n+1) \\ &= [S_n + 1] \cap [(n-1, n) + 1] \quad \text{by inspection} \\ &= [S_n \cap (n-1, n)] + 1 \quad \text{explained below} \\ &= \emptyset + 1 = \emptyset. \quad \text{explained below} \end{aligned}$$

The next-to-last equation has the form $(A+1) \cap (B+1) = (A \cap B) + 1$, where A and B are sets of real numbers. It "says" that if we move each of two sets one unit to the right and then form the intersection, that we get the same set we would have gotten by intersecting first and then moving one unit right. The expression on the left-hand side is, in set selector notation, $\{x \in \mathbb{R} : (\exists y \in A)(x = y + 1) \wedge (\exists z \in B)(x = z + 1)\}$. Thus $x \in (A+1) \cap (B+1) \Rightarrow y+1 = x = z+1$ for some $y \in A$ and some $z \in B$. By additive cancellation $y = z \in A \cap B$, so $x = y + 1 = z + 1 \in (A \cap B) + 1$. Thus the left-hand set is contained in the right-hand set. You should "do" the proof that the right-hand set is contained in the left-hand set yourself, right now!

To explain the last equation we write the meaning of $\emptyset + 1$ in set selector notation:

$$\emptyset + 1 = \{x \in \mathbb{R} : (\exists y \in \mathbb{R})[(y \in \emptyset) \wedge (x = y + 1)]\}.$$

Since $y \in \emptyset$ is false for every $y \in \mathbb{R}$, there are no $x \in \mathbb{R}$ that satisfy the criterion for membership in the set, so the set $\emptyset + 1$ is empty.

Now $S_{n+1} \cap (n, n+1) = \emptyset$, which is $P(n+1)$, and the proof of Theorem (27) is done.

Theorem (27) will enable us to prove **another obvious property** of \mathbb{N} : for all $n \in \mathbb{N}$, there are no natural numbers between n and $n+1$.

(28) **Theorem:** For all $n \in \mathbb{N}$, $\mathbb{N} \cap (n, n+1) = \emptyset$.

Proof: In Exercise (26) you proved that each set S_n is inductive. Thus $\mathbb{N} \subseteq S_n$ for every $n \in \mathbb{N}$. Then (another set calculation is used here) $\mathbb{N} \cap (n, n+1) \subseteq S_n \cap (n-1, n) = \emptyset$, by (27). This completes the proof.

The next Theorem, a *generalization* of Theorem (21), proves another obvious property of \mathbb{N} .

(29) **Theorem:** For all $m \in \mathbb{N}$, for all $n \in \mathbb{N}$, $m < n \Rightarrow n - m \in \mathbb{N}$.

Proof: We let $P(m)$ denote " $(\forall n \in \mathbb{N})(m < n \Rightarrow n - m \in \mathbb{N})$." By Theorem (10), $P(0)$. Given $P(m)$ we consider $P(m+1)$:

$$(\forall n \in \mathbb{N})(m+1 < n \Rightarrow n - (m+1) \in \mathbb{N}).$$

We now regard m as a constant and consider the statements $Q(n)$ to be “ $m + 1 < n \Rightarrow n - (m + 1) \in \mathbb{N}$.” If $n \leq m + 1$ then $Q(n)$ is true vacuously. We now assume that $n > m + 1$ in what follows. Now $Q(n)$ is not true vacuously; by the truth table for implication we have to show that $n - (m + 1) \in \mathbb{N}$ in order to show that $Q(n)$ is true when $n > m + 1$. But then $n > m$ by the transitivity of inequality, so by $P(m)$ we know that $n - m \in \mathbb{N}$. Then, since $n - m > 1$, by Theorem (21) $(n - m) - 1 \in \mathbb{N}$. Since $(n - m) - 1 = n - (m + 1)$ we have shown that $P(m + 1)$ is true. By Mathematical Induction, Theorem (29) follows.

Please notice that in this proof, the statements $Q(n)$ were not proved by induction. They were just used as convenient nicknames. In the next Theorem we prove **an obvious property of increasing sequences**.

(30) **Theorem:** Let $\{x_n\}$ be an increasing sequence. For all $m \in \mathbb{N}$, for all $n \in \mathbb{N}$, $m \leq n \Rightarrow x_n \leq x_m$.

Proof: We denote by $P(m)$ the statement “ $(\forall n \in \mathbb{N})(m \leq n \Rightarrow x_m \leq x_n)$.” For m a constant, a fixed element of \mathbb{N} , we let $Q(n)$ denote “ $m \leq n \Rightarrow x_m \leq x_n$.” The statements $Q(n)$ in $P(m)$ are vacuously true for $n < m$, and true by inspection for $n = m$. Now we suppose $Q(n)$ for some positive integer $n \geq m$. Since $m \leq n$, we have to show that $Q(n + 1)$ is true. But $x_m \leq x_n \leq x_{n+1}$, the first inequality true by $Q(n)$ and the second true by the definition of increasing sequence. Thus $(\forall n \in \mathbb{N})Q(n)$. Thus $P(m)$ is true for arbitrary $m \in \mathbb{N}$, QED.

A non-obvious property of \mathbb{N} : The Well-Ordering Theorem

A set in a space X with a transitive and reflexive ordering is said to be *well-ordered* if every non-empty subset of X has a least element. That is, every non-empty set $E \subseteq X$ has an element $m \in E$ such that $m \leq x$ for every $x \in E$. Although \mathbb{R} has the transitive and reflexive ordering \leq , \mathbb{R} is *not* well-ordered by \leq , since $(0, 1)$ is non-empty but has no least element (if $x \in (0, 1)$ then $x/2 \in (0, 1)$ and $x/2 < x$). However, \mathbb{N} , with the “inherited” ordering \leq , is well-ordered by \leq , which is the content of the next Theorem. Later we will give a different proof.

(30.5) **Theorem:** Every non-empty subset of \mathbb{N} has a least element.

Proof: Suppose that $E \subseteq \mathbb{N}$ is non-empty but that E has no least element. Let’s define the set

$$S := \{n \in \mathbb{N} : (\forall m \in \mathbb{N})(m \leq n \Rightarrow m \notin E)\}.$$

We will prove that S is an inductive set, so $S = \mathbb{N}$ by (6), and then by the definition of S , E is empty, a contradiction.

We begin by showing $0 \in S$. If 0 were in E , it would be the least element of E , because, by **Exercise** (5), $0 \leq x$ for all $x \in \mathbb{N}$. Thus $0 \notin E$. But for the same reason, $m \in \mathbb{N}$ and $m \leq 0$ implies $m = 0$, so

$$(\forall m \in \mathbb{N})(m \leq 0 \Rightarrow m \notin E) \text{ is true, hence } 0 \in S.$$

If $n \in S$, then $(\forall m \in \mathbb{N})(m \leq n \Rightarrow m \notin E)$ is true. We want to show that

$$(\forall m \in \mathbb{N})(m \leq n + 1 \Rightarrow m \notin E) \text{ is true, for then } n + 1 \in S \text{ will be true.}$$

We consider two cases, for $m \in \mathbb{N}$: $m < n + 1$ and $m = n + 1$. By (28), these cases take care of all possible $m \in \mathbb{N}$ such that $m \leq n + 1$. But if $m < n + 1$ then, again by (28), $m \leq n$, so $m \notin E$. If $m = n + 1$, then $m \notin E$ because if it were, it would be the least element of E , because no element of \mathbb{N} that is smaller is in E . Hence $n + 1 \in S$. Thus S is an inductive subset of \mathbb{N} , hence by (6) $S = \mathbb{N}$. Thus E is empty, a contradiction.

Natural numbers and “how many;” finite and infinite sets

You brought with you to class the idea of using natural numbers to express “how many” elements a set has. This idea is not mentioned in the axioms, so it needs to be connected to them. We will define a sequence of sets, $\{F_n\}$, that will serve as “models” for sets with n elements. We must not forget the empty set!

(31) **Exercise:** State and prove the Principle of Mathematical Induction for statements $P(n)$, $n \in \mathbb{Z}^+$.

The following Definition specifies the sets F_n , defines the *mathematical* meanings of “finite set,” “infinite set” and “the number of elements in a finite set,” all in terms of the sets F_n . The definition uses functions of a certain type,

called “one-to-one correspondences.” You may be familiar with these terms. If not, they are explained after the Definition, along with some other terms related to functions, that will be used later as well as now.

(32) **Definition:** For $n \in \mathbb{N}$, we set $F_n := \{m \in \mathbb{N} : m < n\}$, and we say that a set X is finite if there exists $n \in \mathbb{N}$ and a function $h : X \rightarrow F_n$ that is one-to-one and onto, and we say that X has n elements. A set X is infinite if it is not finite. We notice that $F_0 = \emptyset$.

As review, we say (32.1) that a function $f : X \rightarrow Y$ is one-to-one, or injective, if

$$\text{for all } x_1 \text{ and } x_2 \text{ in } X, \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2,$$

and (32.2) that a function $f : X \rightarrow Y$ is onto, or surjective, if

$$\text{for all } y \text{ in } Y, \text{ there exists } x \in X \text{ such that } f(x) = y.$$

We say (32.3) that a function $f : X \rightarrow Y$ is a one-to-one correspondence, or a bijection, if

$$f \text{ is one-to-one and onto.}$$

There are certain sets associated with functions.

(33) If $f : X \rightarrow Y$, we say X is the domain (space) of f and Y is the range (space) of f (we usually omit the word “space”).

(34) If $f : X \rightarrow Y$, and $E \subseteq X$, we define the image of E under f to be the set

$$f(E) := \{f(x) : x \in E\} = \{y \in Y : (\exists x \in X)[y = f(x)]\}.$$

In words, $f(E)$ is the set of all the values $f(x)$ as x “runs through” E . Some authors call $f(X)$ the “range” of the function f . We will call $f(X)$ the “image” of f . For example, if $X = \mathbb{R} = Y$ and $f(x) = x^2$, the domain and range of f are both \mathbb{R} . But the image of f , the set $f(X)$, is the set $[0, \infty)$ (another obvious thing not yet proved!). This function is neither one-to-one nor onto. However, if we replace \mathbb{R} by $[0, \infty)$ the new version of f is a one-to-one correspondence (not yet proved).

(34) If $f : X \rightarrow Y$, and $S \subseteq Y$, we define the inverse image of S under f to be the set

$$f^{-1}(S) := \{x \in X : f(x) \in S\}.$$

In words, $f^{-1}(S)$ is the set of all the $x \in X$ that are carried into S . An important way to put this is that $f^{-1}(S)$ is the set of all solutions x of the equations $f(x) = y$, where $y \in S$. In the example $f : \mathbb{R} \rightarrow \mathbb{R}$ where $f(x) = x^2$, $f^{-1}(\{-1\}) = \emptyset$ because the equation $x^2 = -1$ has no real solutions.

We note that $E \rightarrow f(E)$ is a function with domain 2^X and range 2^Y , while $S \rightarrow f^{-1}(S)$ is a function with domain 2^Y and range 2^X . The inverse image is the more useful function.

The notation f^{-1} is also used to denote an inverse function. This happens when $f : X \rightarrow Y$ is a one-to-one correspondence. Then, for every element $y \in Y$, there is a unique $x \in X$ that solves the equation $f(x) = y$. We then write $f^{-1}(y) = x$. The inverse function “undoes” what f does. An example is the function $f(x) = x^2$ with domain and range $[0, +\infty)$. Here $f^{-1}(y) = \sqrt{y}$. We have not yet proved that “square root” makes sense!

The sets in Definition (32) are well-defined, by set-selector notation. But saying that “a set has n elements” is not necessarily meaningful! We have to prove that no two of the sets F_n and F_m have n elements, say, unless $m = n$. This amounts to showing that if $m \neq n$ and both belong to \mathbb{N} , then there exists no function $h : F_n \rightarrow F_m$ that is a one-to-one correspondence.

Before we do that, we’ll use the sets F_n for another purpose.

A set X with an order \leq is well-ordered if every non-empty subset E of X has a least element. If X is \mathbb{R} with the usual order \leq there exists sets (such as $(0, +\infty)$) that have no least element, so \mathbb{R}, \leq is not well-ordered. However, \mathbb{N} is well-ordered. This is what the next Theorem is about.

(35) **Theorem:** Every non-empty subset of \mathbb{N} has a least element.

Proof: Suppose that $E \subseteq \mathbb{N}$ is non-empty but that E has no least element. Let's define the set

$$S := \{n \in \mathbb{N} : F_{n+1} \cap E = \emptyset\}.$$

Since \mathbb{N} has least element 0, by Exercise (5), $0 \notin E$. Thus $\{0\} \cap E = \emptyset$. Since $F_1 = \{0\}$, $F_{0+1} \cap E = \emptyset$. Thus $0 \in S$. Now suppose $n \in S$. This means that

$$\emptyset = F_{n+1} \cap E = \{m \in \mathbb{N} : m \leq n\} \cap E.$$

If it were true that $n+1 \in E$, then $n+1$ would be the least element of E and we have assumed that E does not have a least element. Hence $n+1 \notin E$, so that

$$\{m \in \mathbb{N} : m \leq n+1\} \cap E = \emptyset = F_{n+2} \cap E,$$

so $n+1 \in S$ and so S is an inductive set contained in \mathbb{N} . By Theorem (6), $S = \mathbb{N}$. But then E must be empty. This is a contradiction, and the proof is complete. **Note:** many small steps were left out of this argument!

Reference

- [1] Leonard Blackburn: was my TA in a course, and taught me about the need to use the Recursion Theorem.
- [2] Paul Halmos, *Naive Set Theory*, Springer-Verlag, Undergraduate Texts in Mathematics, 1974.