Chapter 6 The mathematics of the natural numbers

Section 6.1 The system of the natural numbers

The most important concept of mathematics is that of *natural number*. These are the numbers used for *counting*, among others; we talk about a set having 0, or 1, or 2, 3, etc. elements. Before we discuss counting in detail, we need to give an overview of certain basic properties of the natural numbers.

The natural numbers are 0, 1, 2, 3, ...; all numbers obtained by repeatedly adding 1 to the previous number, starting with 0. This is a rather poor "definition"; and in fact, rather than defining, one has to postulate the existence of the (set of the) natural numbers. Here we do not attempt to build up the theory of the natural number system in an axiomatic way. Rather, we only summarize the main points, some of which should be very familiar.

The set of all the natural numbers is denoted by $\mathbb{N}$. The most fundamental operation on the natural numbers is the *successor operation*:

$$\begin{aligned} S : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n+1 , \end{aligned}$$

that is, the operation of adding 1 to a number. This operation satisfies the following properties:

$$0 \neq S(n) \text{ for all } n \in \mathbb{N} ;$$

$$S(n) = S(m) \Longrightarrow n = m \text{ for all } n , m \in \mathbb{N} .$$

The first of these says that 0 is not the successor of any natural number, the second says that $S:\mathbb{N}\longrightarrow\mathbb{N}$ is injective. Of course, every child knows these; the reason for pointing them out is that, together with the principle of mathematical induction (see below), they are enough for establishing all the needed properties of natural numbers (which is certainly a surprising fact).

One considers many other operations on natural numbers; foremost among them are those of addition and multiplication:

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (k, n) &\longmapsto k + n \end{aligned}$$

$$\begin{aligned} \cdot : \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (k, n) &\longmapsto k \cdot n \ . \end{aligned}$$

(In the notation of multiplication, the dot may be omitted if no confusion arises as a result: kn may be written for $k \cdot n$. On the other hand, especially with numerical factors, sometimes we use × in place of $\cdot$.)

We may define these by the method of *recursion*, or *recurrence*, a very important concept not only in mathematics, but also in computer science. The recursive definition of addition, via the successor function, is as follows:

$$k + 0 = k , \qquad \text{(ADD 1)}$$

$$k + S(n) = S(k + n) \ . \qquad \text{(ADD 2)}$$

Certainly, these equations are *true* as we know addition (the second says that $k + (n + 1) = (k + n) + 1$), but in what sense do they give a definition of addition? The answer is that, although these equations do not explicitly specify what $k + n$ is in general, by repeated application of them, we can calculate any value of $k + n$. To see this, first recall that any natural number is obtained, in fact in a unique way, by applying the S operation to 0 . If $m = SS...S0$ (we omitted parentheses in the function-value notation), then, according to the second equation, (ADD 2),

$$k + m = k + SS...S0 = S(k + S...S0) ,$$

and on the right-hand-side, inside the parentheses, we now have an instance of addition with *one less* S *operators in the second argument*. That is, we have *reduced* the calculation of

$k + m$ to another calculation, namely to that of $k + n$ where n is the *predecessor* of m, $m = \mathtt{S}n$. We may continue reducing in this way until we hit 0 in the second argument, in which case we apply the first recursion equation (ADD 1).

For instance,

$$\begin{aligned}4 + 3 = 4 + \mathtt{SSS}0 &= \mathtt{S}(4 + \mathtt{SS}0) \quad (\text{ADD } 2 \text{ with } n = \mathtt{SS}0)\\ &= \mathtt{SS}(4 + \mathtt{S}0)\\ &= \mathtt{SSS}(4 + 0)\\ &= \mathtt{SSS}4 \qquad (\text{ADD } 1)\\ &\qquad = \mathtt{SS}5 = \mathtt{S}6 = 7\ .\end{aligned}$$

As another example for recursion, here is a recursive definition for multiplication among the natural numbers:

$$k \cdot 0 = 0 \qquad\qquad (\text{MULT } 1)$$

$$k \cdot \mathtt{S}n = k \cdot n + k \qquad\qquad (\text{MULT } 2)$$

This recursion uses the addition as already given, but otherwise it operates in the same way as the previous definition: the second equation *reduces* the calculation of an instance of multiplication, $k \cdot \mathtt{S}n$, to one, namely $k \cdot n$, in which the second argument is *one less* than in the first instance. This circumstance, together with the first equation, allows us to calculate any instance of multiplication of natural numbers in a series of steps each of which is an application of the recursion equations (MULT 1), (MULT 2); when doing so, we have to be able to calculate addition for any pair of arguments. E.g.,

$$\begin{aligned}4\times 3 = 4\times\mathtt{SSS}0 = 4\times\mathtt{SS}0 + 4 = (4\times\mathtt{S}0 + 4) + 4 &=\\ &= ((4\times 0 + 4) + 4) + 4\\ &= ((0 + 4) + 4) + 4\\ &= 12\ .\end{aligned}$$

In the case of addition and multiplication, their definition via recursion has a theoretical significance only; however, recursion is used to specify many functions on the natural numbers which would be harder to define without recursion. An important example is the factorial function:

$$! : \mathbb{N} \longrightarrow \mathbb{N} ::$$

$$0! = 1 \qquad (!1)$$

$$(Sn)! = n! \cdot Sn \qquad (!2)$$

E.g., $4! = 3! \cdot 4 = 2! \cdot 3 \cdot 4 = 1! \cdot 2 \cdot 3 \cdot 4 = 0! \cdot 1 \cdot 2 \cdot 3 \cdot 4 = 1 \cdot 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Related but more general recursions define *sums* and *products*. Suppose x_i is a quantity, one for each natural number i (in other words, $i \longmapsto x_i$ is a given function defined on $\mathbb{N}$). Then, for any $n \in \mathbb{N}$, we may define the quantities

$$\sum_{i<n} x_i ,$$

$$\prod_{i<n} x_i$$

by recursion on the variable n :

$$\sum_{i<0} x_i = 0 \qquad (\text{SUM } 1)$$

(the sum of zero-many terms is 0)

$$\sum_{i<Sn} x_i = \sum_{i<n} x_i + x_n \qquad (\text{SUM } 2)$$

$$\prod_{i<0} x_i = 1 \qquad (\text{PROD } 1)$$

(the product of zero-many terms is 1)

$$\prod_{i<Sn} x_i = (\prod_{i<n} x_i) \cdot x_n . \qquad (\text{PROD } 2)$$

$\sum_{i<n} x_i$ is the sum of all terms x_i where the subscript runs over the given range, in this case the set of natural numbers less than n. We may write

$$\sum_{i<n} x_i = x_0 + x_1 + ... + x_{n-1} ;$$

the recursive definition of the expression makes the three dots precise. Similarly,

$$\prod_{i<n} x_i = x_0 \cdot x_1 \cdot ... \cdot x_{n-1} .$$

We may write sum and product expressions with ranges of subscripts different from " $i < n$ ". E.g.,

$$\sum_{i=2}^{n+1} x_i \text{ is the sum } \quad x_2 + x_3 + ... + x_n + x_{n+1} ;$$

of course, it is really just another case of the original kind of expression:

$$\sum_{i=2}^{n+1} x_i = \sum_{j<n} x_{j+2}$$

(here, $j = i-2$, i.e., $i = j+2$; while i ranges from 2 to $n+1$, j ranges from 0 to $n-1$).

The factorial function is a special case of the product-expression;

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot ... \cdot n .$$

The famous *Fibonacci numbers* are defined by recursion:

$$f_0 = 0 ,$$

$$f_1 = 1 ,$$

$$f_{n+2} = f_n + f_{n+1} \qquad (n \in \mathbb{N})$$

In other words, a sequence $\langle f_n \rangle_{n\varepsilon\mathbb{N}}$ is defined, by saying that the first two terms of the sequence (the ones indexed by 0 and 1) be equal to 1 , and any other term equal the sum of the two previous terms. The first few Fibonacci numbers are:

$$f_0 = 0 ,\ f_1 = 1 ,\ \ f_2 = f_0 + f_1 = 1 ,\ \ f_3 = f_1 + f_2 = 2 ,$$

$$f_4 = f_3 + f_2 = 3 ,\ \ f_5 = f_3 + f_4 = 5 ,\ \ldots$$

The fundamental method of proving facts about the natural numbers is *mathematical induction*. In the axiomatic introduction of the natural number system, the principle of mathematical induction is taken as a basic axiom. The principle says that in order to prove that all natural numbers have a certain property , it suffices to convince oneself of two things: **one**, that 0 has the property, and **two**, that the property is inherited from any natural number to the next. One sees that this is correct, by the following intuitive argument. 0 has the property, as assumed. But then, since it is inherited from 0 to 1 , 1 has it . Since it is inherited from 1 to 2 , 2 has it. Etc. Since by starting with 0 , applying the successor operation repeatedly, every natural number will be eventually reached, we obtain that the every natural number has the property.

Let us analyze the principle of mathematical induction in terms of sets. With a property P of natural numbers, let us take the set of all those natural numbers that have property P , and let us call this set X . Thus, " $n \in X$ " is now synonymous with " n has property P ". To say that 0 has property P is the same as to say that

$$0 \in X . \qquad (1)$$

To say that the property is inherited from any natural to its successor is expressed more mathematically in this way:

for all $n \in \mathbb{N}$, if $n \in X$, then $\mathrm{S}n \in X$, or, with logical abbreviations,

$$\forall n\in\mathbb{N}\ (\, n \in X \implies Sn \in X\,)\ . \qquad (2)$$

(Read " $\forall n\in\mathbb{N}$ " as "for all n in $\mathbb{N}$ ".) The principle says that from the two assumptions (1), (2) it follows that every natural number has property P ; this latter is simply the statement that every natural number is in X , or even more simply, since X is already a subset of $\mathbb{N}$, that

$$X = \mathbb{N}\ . \qquad (3)$$

Thus, finally, the principle of mathematical induction is as follows.

Principle of Mathematical Induction (**PMI**) Let X be any subset of $\mathbb{N}$. Assume that

$$0 \in X \qquad (1)$$

and that

$$\forall n\in\mathbb{N}\ (\, n \in X \implies Sn \in X\,)\ . \qquad (2)$$

Then

$$X = \mathbb{N}\ . \qquad (3)$$

Here is a formulation, directly in terms of properties rather than sets. Let us write $P(n)$ for: " n has property P ". Then the PMI may be stated as follows:

PMI (**second form**). Let P be any property of natural numbers. Assume

$$P(0) \qquad (1')$$

and

$$\forall n \in \mathbb{N} \ (P(n) \implies P(\mathrm{S}n)) \ . \tag{2'}$$

Then

$$\forall n \in \mathbb{N} \ P(n) \ . \tag{3'}$$

Induction may be used, on a very basic level, to establish the fundamental laws of arithmetic for addition, multiplication and exponentiation on the natural numbers (the same laws concerning more comprehensive number systems are established as later steps in the process of building up mathematics axiomatically). This happens very naturally, because those operations are defined by recursion, and recursion and induction go hand in hand.

To see the Principle of Mathematical Induction at work, that is, for an example for a proof by induction, let us consider a simple example concerning sums. The sum of the first n odd numbers may be written as $\sum\limits_{i=1}^{n} (2i\text{-}1)$. Experimenting with the first few values, we find

$$\sum_{i=1}^{1} (2i\text{-}1) = 1 \, ,$$

$$\sum_{i=1}^{2} (2i\text{-}1) = 1 + 3 = 4 \, ,$$

$$\sum_{i=1}^{3} (2i\text{-}1) = 1 + 3 + 5 = 9 \, ,$$

$$\sum_{i=1}^{4} (2i\text{-}1) = 1 + 3 + 5 + 7 = 16 \, ,$$

from which we may conjecture that

$$\sum_{i=1}^{n} (2i\text{-}1) = n^2 \tag{4}$$

for all values of $n \in \mathbb{N}$. We propose to show that (4) holds for all natural numbers n , by *induction on* n . This phrase means that we consider the property P of an arbitrary natural number n that (4) holds true, or equivalently, we consider the set X of all those natural numbers n such that (4) is true, and we apply the PMI to this property/set. First, we have to show that $0 \in X$ (see (1)); in other words, that (4) holds for $n = 0$; this is called the ***basis step*** of the induction.

Basis step: $n = 0$ in (4) .

The sum $\sum_{i=1}^{0}(2i-1)$ is empty, hence, by definition, it is 0 . Also, $0^2 = 0$. The basis step is complete.

Secondly, we have to show that the property in question is inherited from *any* n to $Sn = n+1$. In other words, we want to show the statement under (2). To this end, let n be an *arbitrary* natural number, and *assume* $n \in X$; using this assumption, we will show that $Sn = n+1 \in X$. This is called the ***induction step***.

Induction step: For all $n\in\mathbb{N}$, (4) for n implies (4) for $n+1$.

We fix an arbitrary natural number n , and we assume (4) for n , that is,

$$!: \quad \sum_{i=1}^{n}(2i-1) = n^2 . \tag{5}$$

We call (5) the ***induction hypothesis***; in general, when establishing (2), or (2'), we *assume* $n \in X$, respectively $P(n)$, and we call this assumption the induction hypothesis.

We will show that (4) holds for $n+1$ in place of n , that is

$$?: \quad \sum_{i=1}^{n+1}(2i-1) = (n+1)^2 \tag{6}$$

But, according to the recursive definition of summation,

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + \underset{\overset{\uparrow}{2(n+1)-1}}{(2n+1)} \ .$$

Using the induction hypothesis (5), we find that the latter equals

$$= n^2 + (2n+1)$$

and this is indeed the same as $(n+1)^2$, as needed for (6). The induction step is complete.

According to the PMI, we may now conclude that (4) holds generally, for all $n \in \mathbb{N}$.

There are other forms of the PMI. For one thing, we may start with any fixed number, rather than 0 , and seek to prove that a property holds from that number on. E.g., if we had not wanted to consider the empty sum in the previously proved identity, we might have asserted it for integers $n = 1$ and greater; in this case, the Basis Step would have been the case $n = 1$, and in the Induction Step, we would have argued for an arbitrary positive natural number n , rather than an arbitrary natural number.

More importantly, we have the version of the PMI in which we infer the truth of the induction statement at n from the truth of the statement at *all* numbers less than n , rather than at the immediately preceding value.

Wellordering Principle (**WOP**). Let X be a subset of $\mathbb{N}$. Assume that for any $n \in \mathbb{N}$,

if $k \in X$ holds for all $k \in \mathbb{N}$ such that $k < n$,
then $n \in X$ (7)

(in logical abbreviation:

$$((\forall k \in \mathbb{N})(k < n \implies k \in X) \implies n \in X \qquad).$$

Then

$X = \mathbb{N}$.

WOP, second form. Let P be any property of natural numbers. Assume that for any $n \in \mathbb{N}$,

if $P(k)$ holds for all $k < n$, then $P(n)$

(in logical abbreviation:

$$((\forall k \in \mathbb{N})(k < n \Longrightarrow P(k)) \Longrightarrow P(n) \qquad).$$

Then

for all $n \in \mathbb{N}$, $P(n)$ holds.

In comparison with the PMI, we find only one assumption (7) in place of the two in the PMI. First of all, let us note that $0 \in X$, the "basis step" occurring as an assumption in the PMI, follows from the present "global induction step" (7). This is because the proposition

" $k \in X$ holds for all $k \in \mathbb{N}$ such that $k < 0$ " (8)

is always true, no matter what the set X is, since there is no natural number less than 0 . (The proposition asserts that something holds for all members of the empty set; and any such proposition is automatically true; we also say it is *vacuously true*.) Since the global induction step (7) says that from (8), $0 \in X$ follows, we have that $0 \in X$.

To give an application, let us prove that every natural number can be written as the sum of distinct integral powers of 2 :

for any $n \in \mathbb{N}$, *there are natural numbers* m *and* $i_0 < i_1 < ... < i_{m-1}$ *such that*

$$n = \sum_{j<m} 2^{i_j} = 2^{i_0} + 2^{i_1} + ... + 2^{i_{m-1}} .$$

(Note that when $n=0$, then also $m=0$, and the sum is an empty one, with value equal to 0 as it should be.)

Now, the property $P(n)$, the one that we want to prove to hold for all $n\in\mathbb{N}$, is this:

$P(n)$: *there are natural numbers* m *and* $i_0 < i_1 < ... < i_{m-1}$ *such that*

$$n = \sum_{j<m} 2^{i_j} = 2^{i_0} + 2^{i_1} + ... + 2^{i_{m-1}} .$$

Global Induction Step. Let $n \in \mathbb{N}$ be arbitrary. Assume

$$\forall k\in\mathbb{N}\ (k < n \implies P(k)) , \tag{9}$$

to show

$$P(n) . \tag{10}$$

(9) is called the ***induction hypothesis***.

In the proof of the implication (9) $\implies$ (10), we make a *case distinction*; we distinguish the cases $n=0$ and $n>0$; this has nothing to do with the "basis step" and the "induction step" of the earlier form of induction; more remarks on this later.

Case 1. $n = 0$. As we noted before, in this case, we can take $m = 0$; 0 is the empty sum of powers of 2.

Case 2. $n > 0$. Let 2^i be the largest (integral) power of 2 for which $2^i \le n$ (we will justify this intuitively obvious step below by what we'll call the **Greatest Number Principle**; for the time being, it should be enough to note that, certainly, there is at least one integral power 2^h of 2 for which $2^h \le n$, namely the one with the exponent $h = 0$; $2^0 = 1 \le n$; it is here that we use the case assumption $n > 0$). Let $k = n - 2^h$. Since $2^h \ge 1$, we have that $k < n$. Now, let us apply the induction hypothesis (9) to this k;

$P(k)$ holds, that is, $k = \sum_{j<\ell} 2^{i_j}$ with strictly increasing $i_j \in \mathbb{N}$. Then,

$$n = k + 2^h = \sum_{j<\ell} 2^{i_j} + 2^h ;$$

the only thing left to show is that h is strictly greater than all the indices i_j , $i<\ell$. But, otherwise, we must have that $\ell\geq 1$, $h \leq i_{\ell-1}$, and

$$n \geq 2^{i_{\ell-1}} + 2^h \geq 2^h + 2^h = 2 \cdot 2^h = 2^{h+1} ,$$

and this is in contradiction with the choice of 2^h as the largest power of 2 still $\leq n$; this shows what we wanted.

The Global Induction Step is completed; by the Wellordering Principle, $P(n)$ holds for all n , which is what we wanted.

Note that within the proof of the Global Induction Step, there was a case distinction that resembled the distinction between the "Basis Step" and "Induction Step" in the PMI. However, this is merely coincidental. The important point is that the proof uses the Wellordering Principle in an essential way. Note that in the "induction step", we inferred the truth of $P(n)$ *not* from the truth of $P(n-1)$ as in a proof by the ordinary PMI, but from the truth of $P(k)$ for *some* $k<n$, namely $k=n-2^h$, where we only know that $k<n$, and k may well be different from $n-1$.

Uses of the WOP are also called proofs by induction; the distinction in the names serves the clarity of the discussion here, and later the principles mentioned in this section will all be referred to as "induction".

The WOP can be *proved* on the basis of the PMI. The proof consists in showing that, under the assumption of the WOP, the property

$$Q(n) \equiv \text{ for all } k\in\mathbb{N} , \text{ if } k < n , \ P(k) \text{ holds}$$

satisfies the assumptions of the PMI; we will not give the details here (the reader may try to complete the proof; it is not hard!). By the PMI, then $Q(n)$ holds for all n, which, applied to $n+1$ in place of n, one gets that $P(n)$ holds for all n.

There is an equivalent version of the WOP, the

Least Number Principle (LNP). Let X be any subset of $\mathbb{N}$. If X is non-empty, then there is a least element of X: there is $n \in X$ such that $x \leq y$ for all $y \in X$.

The connection between the WOP and the LNP can be summarized by saying that applying the LNP to X is the same as applying the WOP to its complement, the set $\mathbb{N} - X$.

[Let us prove the LNP for X by applying the WOP to $\mathbb{N} - X$. Assume X is non-empty, but, contrary to the assertion, there is no least element in it; we will derive a contradiction. We claim that the Global Induction Step (7) holds for $\mathbb{N} - X$ in place of X. Assume that for all $k < n$, we have $k \in \mathbb{N} - X$. Then $n \in \mathbb{N} - X$: otherwise $n \in X$ and since for all $k < n$, we have $k \in \mathbb{N} - X$, this is exactly to say that x is the least element of X, which is not supposed to exist. This shows (7) for the set $\mathbb{N} - X$. By the WOP, $\mathbb{N} - X = \mathbb{N}$, which is to say that $X = \emptyset$ (since $X \subset \mathbb{N}$). We have arrived at the desired contradiction.]

Perhaps it is not superfluous to mention that the LNP is a special property of the system of the natural numbers. When you replace $\mathbb{N}$ by $\mathbb{Z}$, the principle becomes incorrect: do you see that?

As a first application of the LNP, let us state and prove the

Greatest Number Principle (GNP). Let N be any natural number, and let X be a subset of $\{i \in \mathbb{N} : i < N\}$ (in other words, $X \subset \mathbb{N}$ and it is *strictly bounded* by N). If X is non-empty, then there is a greatest element of X: there is $n \in X$ such that $x \leq n$ for all $x \in X$.

Note that, unlike in the LNP, now the side-condition of X being bounded is essential; do you see that?

Here is the proof of the GNP. Let X be as in the statement. Consider the set of all *strict upper* *bounds* of X, and call it Y:

$$Y = \{y\in\mathbb{N} : x<y \text{ for all } x\in X\} .$$

Y is non-empty: $N\in Y$ (why?). Therefore, by the LNP, Y has a least element; call it m . m cannot be 0 since m is a strict upper bound of X, and X is non-empty. Now, consider $m-1\in\mathbb{N}$. I claim that $m-1\in X$, and $n=m-1$ is the maximal element of X. We have that $x<m$ for all $x\in X$; that is,

$$x\le m-1 \text{ for all } x\in X ;$$

and in yet different words,

either $x<m-1$ (Case 1) or $x=m-1$ (Case 2) for all $x\in X$.

It cannot be that we have Case 1 for all $x\in X$, since then $m-1$ would be also a strict upper bound of X, which is impossible since $m-1<m$, and m was the *least* strict upper bound of X. Therefore, there must be an $x\in X$ for which Case 2 holds, that is, $m-1=x$; but this means that $m-1\in X$. But we already know that $x\le m-1$ for all $x\in X$; thus, x is the largest element of X.

Note that we are in fact using the GNP in our proof above of the "binary decomposition of numbers"; in Case 2 there, we said: "Let 2^h be the largest integral power of 2 for which $2^h\le n$." Can you justify this step formally by the GNP?

Let us give another application of the LNP.

We will prove in the next section that, for every $n\in\mathbb{N}$, there are prime numbers greater than n. Using this, we may define the sequence $\langle p_n\rangle_{n\in\mathbb{N}}$ by recursion as follows:

$$p_0 \underset{\text{def}}{=} 2 ,$$

$$p_n \underset{\text{def}}{=} \text{the least prime number greater than } p_{n-1} .$$

The point is that the set

$$\{p\in\mathbb{N} \mid p \text{ is prime and } p > p_{n-1}\}$$

is non-empty, by what we just said; hence, by the LNP, p_n is well-defined. The sequence

$$p_0 = 2\,,\quad p_1 = 3\,,\quad p_2 = 5\,,\quad ...$$

is the list of all primes in increasing order; p_n is the $n+1^{\text{st}}$ prime number.

Finally in this section, let us mention still another equivalent form of the "wellorderedness" of the natural numbers, the method of "infinite descent". This is the form the principle of mathematical induction takes explicitly in the work of Pierre de Fermat (1601-1665), one of the greatest of all mathematicians. Actually, the principle should be called "*the impossibility of infinite descent*". What it says is that if we have a sequence

$$n_1 > n_2 > n_3 > n_4 > ...$$

of strictly decreasing natural numbers, then the sequence cannot be infinite: there must be a stage k such that n_{k+1} is not defined any more. The truth of this fact is seen by applying the Least Number Principle: consider the *set*

$$\{n_1\,,\ n_2\,,\ n_3\,,\ n_4\,,\ ...\}$$

of all the numbers in the sequence; this non-empty set has to have a least element; but if that is n_k, then n_{k+1} cannot be defined, since if it were, it would be smaller than n_k, and thus the latter would not be the least element of the said set.

In the next section, we will see an application of the "impossibility of infinite descent".