Contents

1 The natural numbers 1
  1.1 Introduction ................................................. 1
    1.1.1 A simple example, illustrating what the principle of mathematical induction says ............................................. 1
    1.1.2 How Peano studied the natural number system ........... 2
    1.1.3 How we are going to define and study the natural numbers 3
  1.2 Definition of the set of natural numbers as a subset of the set of real numbers ........................................... 4
  1.3 The four basic facts you need to know about the natural numbers ......................................................... 7
  1.4 The principle of mathematical induction ........................... 9
  1.5 Does “our” N look like the “true” N? .......................... 12
  1.6 Examples of proofs by induction ................................ 18
    1.6.1 Another example ........................................... 21

2 More on the natural numbers and induction 22
  2.1 Inductive definitions .......................................... 25
    2.1.1 The inductive definition of powers of a real number .... 25
    2.1.2 The inductive definition of the factorial ................ 26
    2.1.3 The inductive definition of summation ................... 27
    2.1.4 Inductive definition of product ........................ 28
    2.1.5 Some examples of proofs using inductive definitions .... 29

3 The main theorems of elementary natural number arithmetic 33
  3.1 Existence and uniqueness ................................... 34
    3.1.1 An example of a proof of existence and uniqueness .... 35
  3.2 Proof of Theorem 19 (the division theorem for natural numbers) ...................................................... 36

4 The Well Ordering Principle 37
  4.1 Statement of the well ordering principle ...................... 38
  4.2 Proof of the well ordering principle ........................... 38
4.3 An example of a proof using well-ordering 41
4.4 Two theorems about the Fibonacci numbers 44
1 The natural numbers

1.1 Introduction

In 1889, the Italian mathematician Giuseppe Peano presented a set of axioms that provided a complete and rigorous way of building the theory of the natural number system \( \mathbb{N} \).

Peano’s formulation was based on the notion of “successor”. Each natural number \( n \) has a “successor”, the number commonly known as \( n + 1 \). And the successor function is assumed to have certain properties. Specifically, Peano’s axioms read as follows:

(PA1) 1 is a natural number.

(PA2) If \( n \) is a natural number then the successor of \( n \) is a natural number. Hence every natural number has a unique successor, which is itself a natural number.

(PA3) No two different natural numbers have the same successor.

(PA4) 1 is not the successor of any natural number.

(PA5) If a property is possessed by 1 and possessed by the successor of every natural number that possesses the property, then the property is possessed by all natural numbers.

Axiom (PA5) is called the Principle of Mathematical Induction.

It is by far the most important and most widely used property of the natural numbers, and also the one that students find most difficult to understand.

So let me try to explain what it means, with a simple example.

1.1.1 A simple example, illustrating what the principle of mathematical induction says

Suppose there a very large number of people are waiting to get into a theater for a show. The people are standing in line: somebody is first, then there
is a second person, then a third one, and so on. So we can think of these people as labeled by natural numbers: there is a person No.1, a person no.2, a person no. 3, and so on. Suppose you write a message on a piece of paper (for example, “after the show come to my restaurant and if you show your theater ticket you will get a 10% discount for a delicious meal”), and you want everybody to read it. How can you achieve this? One way is as follows: you put in the message the words “after you read this, pass it on to the person standing in line behind you”. Then you give it to Person No. 1, and if everybody follows your request to pass on the message, then everybody will read it. Why? Because Person No. 1 will read it and then pass it on to Person No. 2, who will then pass it on to Person No. 3, and so on.

So, as you see, if

1. person No. 1 gets the message,
2. for every natural number $n$, person $n$ passes on the message to person $n + 1$,

then you can conclude that they all get it.

Now, instead of “getting the message”, think of any property $P(n)$ that may be true or false of a natural number $n$. (For example, $P(n)$ could be the sentence “$n^3 - n$ is divisible by 3”. Or it could be “$n$ is even or odd”.) The Principle of Mathematical Induction says that, if

1. $P(1)$ is true,
2. for every natural number $n$, if $P(n)$ is true then $P(n + 1)$ is true,

then you can conclude that $P(n)$ is true for all natural numbers $n$.

That is, if

1. $P(1),$
2. $(\forall n \in \mathbb{N})(P(n) \implies P(n + 1)),$

then you can conclude that $(\forall n \in \mathbb{N})P(n)$.

### 1.1.2 How Peano studied the natural number system

Starting from his axioms (PA1), (PA2), (PA3), (PA4), and (PA5), Peano showed how it was possible to build the whole theory of the natural number system.
In particular, one can define addition and multiplication of natural numbers, and prove various properties of these operations, such as the associative laws:

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall q \in \mathbb{N})(m + n) + q = m + (n + q)\]

and

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall q \in \mathbb{N})(m.n.q = m.(n.q))\],

the commutative laws:

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n = n + m\]

and

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m.n = n.m\],

the distributive law of multiplication with respect to addition:

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall q \in \mathbb{N})m.(n + q) = m.n + m.q\],

the cancellation laws:

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall q \in \mathbb{N})(m + q = n + q \implies m = n)\],

and

\[(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(\forall q \in \mathbb{N})(m.q = n.q \implies m = n)\],

and many other basic properties.

And one can also define the predicate “less than” (by defining “\(m < n\)” to mean “(\(\exists q \in \mathbb{N}\)\(m + q = n\)” and then prove various properties of “\(<\)”, as well as properties relating “\(<\)” to addition and multiplication.

And then one can go on and define divisibility, prime numbers, greatest common divisor, and all the other basic concepts of elementary arithmetic, and prove results about them.

1.1.3 How we are going to define and study the natural numbers

In these notes we follow an approach different from Peano’s.

a. We take the real numbers as given, with the basic operations of addition, subtraction, multiplication, and division, the special real numbers 0 and 1, and the two-variables predicate “\(<\)”.
b. And we will also take for granted the axioms for the real numbers given in earlier lectures.

c. The natural numbers will then be defined as a special kind of real numbers, and then we will prove their basic properties.

d. In our approach it will not be necessary to define the sum $m + n$ and the product $m.n$ of two natural numbers $m, n$, because these numbers are already real numbers and, as such, $m + n$ and $m.n$ are already defined. And there will be no need to prove the basic properties of addition and multiplication, such as the associative and commutative laws, because these properties are already known to be valid for real numbers, so in particular they are valid for natural numbers, because the natural numbers are real numbers. (So, for example, if $m$ and $n$ are natural numbers, the fact that $m + n = n + m$ follows because $m$ and $n$ are real numbers, and we know that $m + n = n + m$ if $m, n$ are real numbers.)

But it will be necessary to prove that the sum and the product of two natural numbers is a natural number, because this is not going to be automatically true by virtue of the definition of “natural number”.

1.2 Definition of the set of natural numbers as a subset of the set of real numbers

Definition 1. An inductive set of real numbers is a set $S$ of real numbers such that

\[(\forall n)(n \in S \implies n + 1 \in S).\] (1.1)

In other words: a set $S$ of real numbers is inductive if, for every member $n$ of $S$, it follows that $n + 1 \in S$.

Definition 2. A 1-inductive set of real numbers is a set $S$ of real numbers such that

1. $1 \in S$,

2. $S$ is inductive.

In other words: a set $S$ of real numbers is 1-inductive if it is inductive and such that 1 belongs to $S$. 

**Definition 3.** A natural number is a real number that belongs to every 1-inductive set of real numbers. □

**Notation.** We use \( \mathbb{N} \) to denote the set of all natural numbers.

**Remark 1.** Remember than “\( \mathbb{N} \)” is a special mathematical symbol. It is not \( n \), or \( N \), or \( N \). It’s \( \mathbb{N} \). □

It is clear from the above definition of “natural number” that every natural number is a real number. In other words,

**Theorem 1.** \( \mathbb{N} \subseteq \mathbb{R} \). □

And we also have:

**Theorem 2.** 1 is a natural number (that is, \( 1 \in \mathbb{N} \)).

**Proof.** To prove that \( 1 \in \mathbb{N} \) we have to prove that if \( S \) is an arbitrary 1-inductive set of real numbers then \( 1 \in S \).

So let \( S \) be an arbitrary 1-inductive set of real numbers. Then the definition of “1-inductive set” tells us that \( 1 \in S \).

So we have proved that if \( S \) is an arbitrary 1-inductive set of real numbers then \( 1 \in S \). Hence 1 belongs to very 1-inductive set of real numbers. So \( 1 \in \mathbb{N} \). Q.E.D.

**Theorem 3.** If \( n \) is a natural number then \( n + 1 \) is a natural number. (In other words, \((\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N})\), or \((\forall n \in \mathbb{N})n + 1 \in \mathbb{N}\)).

**Proof.** We want to prove that \((\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N})\),

Let \( n \) be arbitrary.

Assume that \( n \in \mathbb{N} \).

We want to prove that \( n + 1 \in \mathbb{N} \).

For this purpose, we have to prove that \( n + 1 \) belongs to every 1-inductive set of real numbers.

Let \( S \) be a 1-inductive set of real numbers.
We want to prove that \( n + 1 \in S \).

Since \( n \in \mathbb{N} \), \( n \) belongs to every 1-inductive set of real numbers.

So in particular \( n \in S \).

Since \( S \) is 1-inductive, \( S \) is inductive, so \( n \in S \implies n+1 \in S \).

But \( n \in S \). So \( n + 1 \in S \). \([\text{Rule } \implies_{use}, \text{ Modus Ponens}]\)

Since \( S \) was an arbitrary 1-inductive set of real numbers, we have proved that \( n + 1 \) belongs to every 1-inductive set of real numbers.

So \( n + 1 \in \mathbb{N} \).

Since we have proved that \( n + 1 \in \mathbb{N} \) assuming that \( n \in \mathbb{N} \), it follows that \( n \in \mathbb{N} \implies n + 1 \in \mathbb{N} \). \([\text{Rule } \implies_{prove}]\)

Since we have shown that \( n \in \mathbb{N} \implies n + 1 \in \mathbb{N} \) for an arbitrary \( n \), we can conclude that \( (\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N}) \). \( \text{Q.E.D.} \)

We can summarize the three theorems we have just proved in the following statement:

**Corollary 1.** The set \( \mathbb{N} \) is a 1-inductive set of real numbers.

**Proof.** To prove this we have to show that \( 1 \in \mathbb{N} \) and that \( (\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N}) \).

But “\( 1 \in \mathbb{N} \)” was proved in Theorem 2, and “\( (\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N}) \)” was proved in Theorem 3. So everything we need has been proved. \( \text{Q.E.D.} \)

**Theorem 4.** (The principle of mathematical induction, inductive set version.) If \( S \) is a set of natural numbers and \( S \) is 1-inductive then \( S = \mathbb{N} \).

**Proof.** Let \( S \) be a set of natural numbers. Suppose that \( S \) is 1-inductive. Let us prove that \( S = \mathbb{N} \).

Since \( S \) is a set of natural numbers, \( S \subseteq \mathbb{N} \). We want to prove that \( \mathbb{N} \subseteq S \), that is, that every natural number is in \( S \).

So let \( n \) be an arbitrary natural number. The fact that \( n \in \mathbb{N} \) says, according to the definition of “natural number”, that \( n \) belongs to every 1-inductive set. So in particular \( n \) belongs to \( S \).

So we have proved that if \( n \) is an arbitrary natural number then \( n \in S \).

That is, we have proved that \( \mathbb{N} \subseteq S \).

Since \( \mathbb{N} \subseteq S \) and \( S \subseteq \mathbb{N} \), it follows that \( S = \mathbb{N} \), as desired. \( \text{Q.E.D.} \)
1.3 The four basic facts you need to know about the natural numbers

In case you find the previous section, with the definition of “natural number” in terms of 1-inductive sets of real numbers, hard to understand, here is a list of the four basic facts about the natural numbers that we proved before. These four facts are all you need to know in order to work with the natural numbers and prove things about them.

The Four Basic Facts about the Natural Numbers

Fact B1. \( \mathbb{N} \subseteq \mathbb{R} \). (That is, every natural number is a real number.)

Fact B2. 1 is a natural number (that is, \( 1 \in \mathbb{N} \)).

Fact B3. \( (\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N}) \). (That is: if \( n \) is a natural number then \( n + 1 \) is a natural number.)

Fact B4. (The principle of mathematical induction, inductive set version.) If \( S \) is a set of natural numbers and \( S \) is 1-inductive then \( S = \mathbb{N} \).

And, if you find the concept of “1-inductive set” too difficult to work with, here is another version of the Four Basic Facts that does not mention 1-inductive sets at all.
The Four Basic Facts about the Natural Numbers

Fact B1. \( \mathbb{N} \subseteq \mathbb{R} \). (That is, every natural number is a real number.)

Fact B2. 1 is a natural number (that is, \( 1 \in \mathbb{N} \)).

Fact B3. \((\forall n)(n \in \mathbb{N} \implies n + 1 \in \mathbb{N})\). (That is: if \( n \) is a natural number then \( n + 1 \) is a natural number.)

Fact B4. (The principle of mathematical induction, inductive set version.) If \( S \) is a set of natural numbers such that \( 1 \in S \) and \((\forall n)(n \in S \implies n+1 \in S)\), then \( S = \mathbb{N} \).

And here is still another way of saying exactly the same thing:
The Four Basic Facts about the Natural Numbers

**Fact B1.** \( \mathbb{N} \subseteq \mathbb{R} \). (That is, every natural number is a real number.)

**Fact B2.** 1 is a natural number (that is, \( 1 \in \mathbb{N} \)).

**Fact B3.** \( \forall n \in \mathbb{N} \implies n + 1 \in \mathbb{N} \). (That is: if \( n \) is a natural number then \( n + 1 \) is a natural number.)

**Fact B4.** (*The principle of mathematical induction, inductive set version.*) If \( S \) is a set of natural numbers and you want to prove that every natural number belongs to \( S \), you can do it by proving the following two things:

1. \( 1 \in S \),
2. \( \forall n \in S \implies n + 1 \in S \).

Once you have proved these two facts, you can conclude that \( S = \mathbb{N} \), so every natural number is in \( S \).

### 1.4 The principle of mathematical induction

Fact B4 is very important, so let me say again what the theorem says, in words that may be clearer to you.
How to use the principle of mathematical induction, set version.

Suppose you want to prove that something is true for all natural numbers. That is, you have a one-variable predicate\(^a\) \(P(n)\) (For example, \(P(n)\) could be “\(n \geq 1\)”, or “\(n\) is even or \(n\) is odd”, or “\(n(n+1)\) is even”) and you want to prove that \((\forall n \in \mathbb{N})P(n)\). (That is, you want to prove that \(P(n)\) is true for every natural number \(n\).)

Then you can do the following:

1. Introduce the set \(S\) of all the natural numbers \(n\) such that \(P(n)\) is true, by saying “Let \(S = \{n : n \in \mathbb{N} \land P(n)\}\)”.

2. Prove that \(S = \mathbb{N}\), by proving that \(S\) is a 1-inductive set. For this purpose, you must

   B. Prove that \(1 \in S\). (That is, \(P(1)\) is true.)

   I. Prove that \(((\forall n)(n \in S \implies n + 1 \in S))\).

   To prove that \(((\forall n)(n \in S \implies n + 1 \in S))\), you write

   Let \(n\) be arbitrary.

   Assume that \(n \in S\).

   and then prove that \(n + 1 \in S\).

   Step B is called the **basis step** of the inductive proof, and Step I is called the **inductive step**.

   Once you have successfully carried out the basis step and the inductive step, you can conclude that \(S = \mathbb{N}\), that is, that \((\forall n \in \mathbb{N})P(n)\). (In other words, you can conclude that \(P(n)\) is true for all natural numbers \(n\).)

---

\(^a\) A predicate is a statement about one or several variable objects, denoted by letters, that can be true or false for specific values of the letters. For example “\(n\) is even” is a one-variable predicate; it is true, for example, for \(n = 2\) or \(n = 4\), but it is false, for \(n = 1\) or \(n = 3\). And “\(n\) is divisible by \(m\)” is a two-variable predicate: it is true for \(n = 6\) and \(m = 3\), but it is false for \(n = 6\) and \(m = 5\).
How to use the principle of mathematical induction, predicate version.

Suppose you want to prove that something is true for all natural numbers. That is, you have a one-variable predicate $P(n)$ and you want to prove that $(\forall n \in \mathbb{N})P(n)$. (That is, you want to prove that $P(n)$ is true for every natural number $n$.) Then, in order to prove that $P(n)$ is true for all $n \in \mathbb{N}$, you can do the following:

B. Prove that $P(1)$ is true.

I. Prove that $(\forall n)(P(n) \implies P(n+1))$. To prove that $(\forall n)(P(n) \implies P(n+1))$, you write

Let $n$ be arbitrary.

Assume $P(n)$.

and then prove $P(n+1)$.
Step B is called the **basis step** of the inductive proof, and Step I is called the **inductive step**. In the inductive step, the assumption that $P(n)$ holds is called the **inductive hypothesis**.

Once you have successfully carried out the basis step and the inductive step, you can conclude that $(\forall n \in \mathbb{N})P(n)$. (In other words, you can conclude that $P(n)$ is true for all natural numbers $n$.)

*Why is this a consequence of Theorem 4?* Well, suppose you find yourself in the situation described in the box. That is, you have proved that $P(1)$ is true and that $(\forall n \in \mathbb{N})(P(n) \implies P(n+1))$, and you want to conclude that $(\forall n \in \mathbb{N})P(n)$, and
Then you can do the following:

a. Form the set \( S = \{ n \in \mathbb{N} : P(n) \} \). (That is, \( S \) is the set of all natural numbers \( n \) for which \( P(n) \) is true.)

b. Then \( 1 \in S \), because \( P(1) \) is true.

c. And \( (\forall n)(n \in S \implies n + 1 \in S) \). (Reason: if \( n \in S \) then \( n \in \mathbb{N} \) and \( P(n) \) is true, so \( P(n + 1) \) is true, because \( P(n) \implies P(n + 1) \)).

d. So \( S \) is 1-inductive.

e. So by Theorem 4 \( S = \mathbb{N} \).

This means that every natural number is in \( S \). So if \( n \) is an arbitrary natural number, then \( n \) is in \( S \), and that means that \( P(n) \) is true.

So \( (\forall n \in \mathbb{N})P(n) \). This shows that you can indeed conclude that \( (\forall n \in \mathbb{N})P(n) \) if you have managed to carry out Steps B and I.

1.5 Does “our” \( \mathbb{N} \) look like the “true” \( \mathbb{N} \)?

I am sure that at this point you must be thinking that you already know what the natural numbers are, and that the definition we have given here does not look at all like what you know.

I would like to persuade you that the \( \mathbb{N} \) that we have defined is exactly the one that you know. In other words, I claim that the definition of \( \mathbb{N} \) that I have given captures your intuition of what \( \mathbb{N} \) is supposed to be.

But this is going to take some work, because Definition 3 is not that easy to digest. You need to work with it for a while, until you begin to see that the definition is just right, that it gives us exactly the set of natural numbers that we all know, or think we know.

You probably have a mental picture of the real line \( \mathbb{R} \) as a straight line extending indefinitely in both directions. And, within that line, there are a few dots—the number 1, the number 2, the number 3, and so on—that stand out: those dots are the natural numbers. The dot farthest to the left is 1 (there are no dots to the left of 1. And then, as you move right, you encounter another dot, the number 2, and there are no dots between 1 and 2. And then, if you move even farther right, you encounter another dot, the

\footnote{Notice that we are using the Modus Ponens rule (Rule \( \implies \) use) here.}
number 3. And there are no dots between 2 and 3. And this goes on: as you move to the right, there is 4, then 5, and so on. And you never come to a “last dot”, because for every dot \( n \) there is the dot \( n + 1 \) farther to the right.

Think of the real line as a dark night sky, and of the dots that represent the natural numbers as stars.

I am going to show you how, if you analyze “our” set \( \mathbb{N} \) (that is, the set that we have defined in Definition 3), you get exactly the picture that I have just sketched for the “true” \( \mathbb{N} \).

To begin with, we know nothing about our \( \mathbb{N} \), except that 1 is in \( \mathbb{N} \). That is, we have this one star, the number 1, but for all you know there could be natural numbers all over the place. It could even be that every real number is a natural number, so we don’t have 1 as an isolated star but we have a huge undifferetiated cloud of stars, forming a fog that covers the whole real line.

With the next three theorems, the fog around the number 1 will dissipate, and you will see 1 more clearly, standing in splendid isolation.

First, let us recall that we have defined 2, 3, and 4 as follows:

\[
2 = 1 + 1, \quad (1.2) \\
3 = 2 + 1, \quad (1.3) \\
4 = 3 + 1. \quad (1.4)
\]

**Theorem 5.** 1, 2, 3 and 4 are natural numbers.

**Proof.** We use Basic facts B2 and B3.

Thanks to B2, 1 is a natural number. Then B3 tells us that \( 1 + 1 \) is a natural number, so 2 is a natural number.

Using B3 again, since \( 2 \in \mathbb{N} \), we conclude that \( 3 \in \mathbb{N} \).

And, finally, using B3 one more time, since \( 3 \in \mathbb{N} \), we conclude that \( 4 \in \mathbb{N} \). Q.E.D.

**Theorem 6.** \( (\forall n)(n \in \mathbb{N} \implies n \geq 1) \). In other words: **every natural number is greater than or equal to 1.** That is:

1 is the smallest of all the natural numbers. In the real line \( \mathbb{R} \), there are no natural numbers to the left of 1.
**Proof.** We do a proof by induction, using the set version.

Let

\[ S = \{ n \in \mathbb{N} : n \geq 1 \}. \]

(That is, \( S \) is the set of all natural numbers that are \( \geq 1 \).)

We will prove that \( S = \mathbb{N} \). This will tell us that every natural number is in \( S \), so every natural number is \( \geq 1 \).

**Basis step.** We must prove that \( 1 \in S \). But this is easy: We already know that \( 1 \in \mathbb{N} \), and of course \( 1 \geq 1 \). So \( 1 \in S \).

**Inductive step.** We must prove that

\[ (\forall n)(n \in S \implies n + 1 \in S) \]  \hspace{1cm} (1.5)

Here is the proof:

Let \( n \) be arbitrary.

Assume \( n \in S \).

Then \( n \) is a natural number and \( n \geq 1 \).

Therefore \( n + 1 \) is a natural number (by B2).

And \( n + 1 \geq 1 \) (because \( n \geq 1 \) and \( 1 > 0 \), so \( n + 1 \geq 1 + 0 \), i.e., \( n + 1 \geq 1 \)).

So \( n + 1 \in S \).

Hence \( n \in S \implies n + 1 \in S \). (Rule \( \implies \) prove)

Since \( x \) is arbitrary, we have proved that \((\forall n)(n \in S \implies n + 1 \in S)\).

That is, we have proved (1.5).

This completes the inductive step. It follows from the Principle of Mathematical Induction that \( S = \mathbb{N} \), and this implies that \( n \geq 1 \) for every natural number \( n \).

Q.E.D.

**Theorem 7.** Every natural number is equal to \( 1 \) or \( \geq 2 \). (In other words, \((\forall n)(n \in \mathbb{N} \implies (n = 1 \lor n \geq 2))\). That is,
1 is the smallest of all the natural numbers, 2 is a natural number as well, and in the real line $\mathbb{R}$, there are no natural numbers to the left of 2 other than 1.

**Proof.** We do a proof by induction, using the set version.

Let

$$S = \{ n \in \mathbb{N} : n = 1 \lor n \geq 2 \}.$$  

(That is, $S$ is the set of all natural numbers that are $\geq 2$, together with the number 1.)

We will prove that $S = \mathbb{N}$. This will tell us that every natural number is in $S$, so every natural number is either equal to 1 or $\geq 2$.

**Basis step.** We must prove that $1 \in S$. But this is easy: We already know that $1 \in \mathbb{N}$, and the condition “$n = 1 \lor n \geq 2$” is clearly satisfied when $n = 1$. So $1 \in S$.

**Inductive step.** We must prove that

$$(\forall n)(n \in S \implies n + 1 \in S) \quad (1.6)$$

Here is the proof:

Let $n$ be arbitrary.

Assume $n \in S$.

Then $n$ is a natural number and $n = 1 \lor n \geq 2$.

Therefore $n + 1$ is a natural number (by B2).

And $n + 1 \geq 2$ (because $n \geq 1$ and $1 > 0$, so $n + 1 \geq 1 + 0$, i.e., $n + 1 \geq 1$.)

So $n + 1 \in S$.

Hence $n \in S \implies n + 1 \in S$. (Rule $\implies_{\text{prove}}$)

Since $x$ is arbitrary, we have proved that $(\forall n)(n \in S \implies n + 1 \in S)$. That is, we have proved (1.5).
This completes the inductive step. It follows from the Principle of Mathematical Induction that \( S = \mathbb{N} \), and this implies that \( n \geq 1 \) for every natural number \( n \).

**Q.E.D.**

**Theorem 8.** Every natural number is equal to 1 or 2, or \( \geq 3 \). (In other words, \((\forall n)(n \in \mathbb{N} \implies (n = 1 \lor n = 2 \lor n \geq 3))\). That is,

1 is the smallest of all the natural numbers, 2 and 3 are natural numbers as well, and in the real line \( \mathbb{R} \), there are no natural numbers to the left of 3 other than 1 and 2.

**Proof.** This time, for a change, we will use the predicate version of the Principle of Mathematical Induction.

Let \( P(n) \) be the statement “\( n = 1 \lor n = 2 \lor n \geq 3 \)”.

We will prove that

\[
(\forall n \in \mathbb{N}) P(n) .
\]

This will tell us that every natural number \( n \) satisfies “\( n = 1 \lor n = 2 \lor n \geq 3 \)”, which is exactly what we want to prove.

To prove \((1.7)\), we that \( S = \mathbb{N} \), we use the Principle of Mathematical Induction.

**Basis step.** We have to prove that \( P(1) \) is true. But \( P(1) \) says that \( 1 = 1 \lor 1 = 2 \lor 1 \geq 3 \), which is obviously true because \( 1 = 1 \).

**Inductive step.** We have to prove that

\[
(\forall n \in \mathbb{N}) \left( P(n) \implies P(n + 1) \right) .
\]

Let \( n \in \mathbb{N} \) be arbitrary.

Assume \( P(n) \).

Then either \( n = 1 \) or \( n = 2 \) or \( n \geq 3 \).

Let \( m = n + 1 \).

We consider the three possible cases: \( n = 1 \), \( n = 2 \), \( n \geq 3 \).
If \( n = 1 \) then \( m = 2 \), so the statement “\( m = 1 \lor m = 2 \lor m \geq 3 \)” is true; that is, \( P(m) \) is true.

If \( n = 2 \) then \( m = 3 \), so \( m \geq 3 \), and then the statement “\( m = 1 \lor m = 2 \lor m \geq 3 \)” is true; that is, \( P(m) \) is true.

If \( n \geq 3 \) then \( m \geq 4 \), so \( m \geq 3 \), and then the statement “\( m = 1 \lor m = 2 \lor m \geq 3 \)” is true; that is, \( P(m) \) is true.

We have proved that \( P(m) \) is true in each of our three cases, and we know that one of the three cases holds. So we can conclude that \( P(m) \) is true, i.e., that \( P(n+1) \) is true. [Rule \( \lor \text{use} \)]

We have proved \( P(n+1) \) assuming \( P(n) \). Hence we can conclude that
\[
\begin{array}{c}
P(n) \implies P(n+1)
\end{array}
\]

We have proved that \( P(n) \implies P(n+1) \) for arbitrary \( n \in \mathbb{N} \). Hence we can conclude that
\[
(\forall n \in \mathbb{N})(P(n) \implies P(n+1)),
\]
which is exactly Equation (1.8). So we have completed the inductive step.

Hence we can apply the Principle of Mathematical Induction and conclude that \( (\forall n \in \mathbb{N})(P(n) \text{, i.e., that } (\forall n \in \mathbb{N})(n = 1 \lor m = 2 \lor n \geq 3)) \). Q.E.D.

Let’s take a look at what we have done. We have proved that 1 and 2 are natural numbers, and all other natural numbers are greater than or equal to 3. This tells us that, in the real line, the set \( \mathbb{N} \) consists of two isolated dots at 1 and 2, and then stuff that we don’t know much about to the right of 3. But there are no natural numbers to the left of 3, except for 1 and 2.

So a lot of the fog has dissipated: 1 and 2 stand isolated as two stars surrounded by empty space: except for those two dots, there is no “natural number stuff” to the left of \( s \).

Isn’t our set \( \mathbb{N} \) beginning to look like what you you think \( \mathbb{N} \) should be?
Of course we could go on proving more theorems like Theorems (6), (7) and (8).

For example, we could prove

**Theorem 9.** Every natural number other than 1, 2, and 3, is greater than or equal to 4.

**Proof.** YOU DO IT.

And, exactly as we defined 2, 3 and 4 on page 13, we could define 5, 6, 7 and 8 by

\[
\begin{align*}
5 &= 4 + 1, \\
6 &= 5 + 1, \\
7 &= 6 + 1, \\
8 &= 7 + 1. 
\end{align*}
\]

(1.9) (1.10) (1.11) (1.12)

And then we could prove:

**Theorem 10.** Every natural number other than 1, 2, 3, 4, 5, 6, and 7 is greater than or equal to 8.

**Proof.** YOU DO IT.

**Problem 1.** Prove Theorems 9 and 10. □

Clearly, this can go on and on and on. But it gets very boring. So let us turn instead to more interesting things.

### 1.6 Examples of proofs by induction

Here is an example of a proof by induction using the above format. As we explained earlier, the fact that the sum of two natural numbers is a natural number is not contained in the Basic Facts about the natural numbers, so it has to be proved.

**Theorem 11.** The sum of two natural numbers is a natural number. (That is, \((\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n \in \mathbb{N}\).)
Proof. We want to prove that \( (\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n \in \mathbb{N} \). For this purpose, we fix an arbitrary natural number \( m \), and set out to prove that

\[
(\forall n \in \mathbb{N})m + n \in \mathbb{N}.
\]  

(1.13)

Formula (1.13) is precisely of the form \( (\forall n \in \mathbb{N})P(n) \) (where \( P(n) \) is the statement “\( m + n \in \mathbb{N} \)”. So we find ourselves exactly in the kind of situation where we can use induction\(^2\).

Basis step. We have to prove that \( P(1) \) is true. But \( P(1) \) is the statement “\( m + 1 \in \mathbb{N} \)”. And we know that \( m \) is a natural number. So Basic Fact B3 tells us that \( m + 1 \) is a natural number, that is, that \( m + 1 \in \mathbb{N} \). So \( P(1) \) is indeed true.

Inductive step. We let \( n \) be an arbitrary natural number and assume that \( P(n) \). That is, we assume that \( m + n \in \mathbb{N} \). We want to prove that \( P(n+1) \) is true, i.e., that \( m + (n+1) \in \mathbb{N} \). But Basic Fact B3 tells us, since \( m + n \in \mathbb{N} \), that \( (m+n)+1 \in \mathbb{N} \). And, by the associative law for addition, \( (m+n)+1 = m + (n+1) \). So \( m + (n+1) \in \mathbb{N} \). In other words, \( P(n+1) \) is true. So we have proved that \( (\forall n \in \mathbb{N})(P(n) \implies P(n+1)) \), thus completing the inductive step.

Conclusion. So \( P(n) \) is true for all \( n \in \mathbb{N} \). That is, \( (\forall n \in \mathbb{N})m + n \in \mathbb{N} \).

But \( m \) was an arbitrary natural number. So we have proved our desired conclusion, that is, that \( (\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n \in \mathbb{N} \). Q.E.D.

Another version of the same proof, using inductive sets. We want to prove that \( (\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n \in \mathbb{N} \). For this purpose, we fix an arbitrary natural number \( m \), and set out to prove that

\[
(\forall n \in \mathbb{N})m + n \in \mathbb{N}.
\]  

(1.14)

Let \( S \) be the set of all natural numbers \( n \) that are such that \( m + n \in \mathbb{N} \).

Then \( 1 \in S \), because \( m + 1 \) is a natural number thanks to Basic Fact B3.

We now prove that the set \( S \) is inductive. We have to prove that for every \( n \in \mathbb{N} \), if \( n \in S \) then \( n + 1 \in S \). So let \( n \) be an arbitrary natural number. Assume that \( n \in S \). Then \( m+n \in \mathbb{N} \). So, by Basic Fact BF3, \( (m+n)+1 \in \mathbb{N} \). But by the associative law for addition, \( (m+n)+1 = m + (n+1) \). So \( m + (n+1) \in \mathbb{N} \). In other words, \( n + 1 \in S \). So we have proved that \( (\forall n \in \mathbb{N})(n \in S \implies n + 1 \in S) \). Therefore the set \( S \) is inductive.

\(^2\)And do not forget that we have fixed \( m \) before, so “\( m + n \in \mathbb{N} \)” is a statement about \( n \) only.
Conclusion. We have proved that \(1 \in S\) and \(S\) is inductive. So \(S\) is 1-inductive. Then the principle of mathematical induction tells us that \(S = \mathbb{N}\). Hence every natural number belongs to \(S\), which means that \((\forall n \in \mathbb{N})m+n \in \mathbb{N}\).

But \(m\) was an arbitrary natural number. So we have proved the assertion that \((\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m+n \in \mathbb{N}\). Q.E.D.

**Theorem 12.** The product of two natural numbers is a natural number. (That is, \((\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m.n \in \mathbb{N}\).)

**Proof.** We want to prove that \((\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m.n \in \mathbb{N}\). For this purpose, we fix an arbitrary natural number \(m\), and set out to prove that \((\forall n \in \mathbb{N})m.n \in \mathbb{N}\). (1.15)

Formula (1.15) is precisely of the form \((\forall n \in \mathbb{N})P(n)\) (where \(P(n)\) is the statement “\(m.n \in \mathbb{N}\)”. So we find ourselves exactly in the kind of situation where we can use induction\(^3\).

**Basis step.** We have to prove that \(P(1)\) is true. But \(P(1)\) is the statement “\(m.1 \in \mathbb{N}\)”. And we know that \(m\) is a natural number. Furthermore, one of our real number axioms tells us that \(x.1 = x\) for every real number \(x\). So in particular \(m.1 = m\). But then \(m.1 \in \mathbb{N}\), because \(m \in \mathbb{N}\). So \(P(1)\) is indeed true.

**Inductive step.** We let \(n\) be an arbitrary natural number and assume that \(P(n)\). That is, we assume that \(m.n \in \mathbb{N}\). We want to prove that \(P(n+1)\) is true, i.e., that \(m.(n+1) \in \mathbb{N}\).

The distributive law of multiplication of real number with respect to addition tells us that \(x.(y+z) = x.y + x.z\) for all real numbers \(x, y, z\). Hence \(m.(n+1) = m.n + m.1\), so

\[
m.(n+1) = m.n + m.
\]

We know that \(m.n \in \mathbb{N}\) and that \(m \in \mathbb{N}\). And Theorem 11 tells us that the sum of two natural numbers is a natural number. Hence \(m.n + m \in \mathbb{N}\). In other words, \(m.(n+1) \in \mathbb{N}\). So \(P(n+1)\) is true. So we have proved that \((\forall n \in \mathbb{N})(P(n) \implies P(n+1))\), thus completing the inductive step.

\(^3\)And do not forget that we have fixed \(m\) before, so “\(m.n \in \mathbb{N}\)” is a statement about \(n\) only.
Conclusion. We have shown that $P(n)$ is true for all $n \in \mathbb{N}$. That is, $(\forall n \in \mathbb{N}) m.n \in \mathbb{N}$.

But $m$ was an arbitrary natural number. So we have proved our desired conclusion, that is, that $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N}) m.n \in \mathbb{N}$. Q.E.D.

1.6.1 Another example

Here is another example of a proof by induction. (NOTE: The meaning of "$2^n$" will be explained in the next lecture, where the following inductive definition of "$2^n$" will be given:

$$
2^1 = 2, \\
2^{n+1} = 2 \times 2^n \quad \text{for every } n \in \mathbb{N}.
$$

Actually, we will define $a^n$ for every natural number $n$ and every real number $a$.)

Proposition 1. For all $n \in \mathbb{N}$, $n < 2^n$.

Proof. Let $P(n)$ be the statement "$n < 2^n$".

Basis step. $P(1)$ is the statement "$1 < 2$" (because $2^1 = 2$), which is clearly true. So $P(1)$ is true.

Inductive step. We want to prove that $(\forall n \in \mathbb{N})(P(n) \implies P(n + 1))$. For this purpose, we let $n$ be an arbitrary natural number, and try to prove that $P(n) \implies P(n + 1)$. And, to prove this implication, we assume $P(n)$ and try to prove $P(n + 1)$.

So we are now assuming that $n < 2^n$. Then $P(n + 1)$ is the statement "$(n + 1) < 2^{n+1}$". Let us prove that this statement is true. Since $n < 2^n$, we have $n + 1 < 2^n + 1$. Moreover, $1 < 2^n$ for every $n \in \mathbb{N}$.

So $n + 1 < 2^n + 1$ and $2^n + 1 < 2^n + 2^n = 2^{n+1}$. Hence $n + 1 < 2^{n+1}$. So $P(n + 1)$ is true. Hence we have shown that

$$(\forall n \in \mathbb{N})(P(n) \implies P(n + 1)). \quad (1.16)$$

Everybody would agree that this is so trivial that there is no need to prove it. But, just in case, here is the proof (by induction, of course) using the inductive definition of $2^n$ given above: Let $Q(n)$ be the sentence "$1 < 2^n$". Then $Q(1)$ says that $1 < 2$, because $2^1 = 2$. So $Q(1)$ is true. Next let $n$ be arbitrary, and assume that $Q(n)$ is true. Then $1 < 2^n$, and $2^{n+1} = 2 \times 2^n$. Since $1 < 2^n$, we get $2^{n+1} = 2 \times 2^n > 2^n > 1$, so $2^{n+1} > 1$, and then $1 < 2^{n+1}$. Q.E.D.
Conclusion. Since $P(1)$ is true, and (1.16) is also true, the principle of mathematical induction implies that

$$(\forall n \in \mathbb{N}) P(n),$$

i.e., that $(\forall n \in \mathbb{N}) n < 2^n$. Q.E.D.

2 More on the natural numbers and induction

Recall the definitions of “even” and odd:

Definition 4. A natural number $n$ is even if there exists $k \in \mathbb{N}$ such that $n = 2k$.

Definition 5. A natural number $n$ is odd if there exists $k \in \mathbb{N}$ such that $n = 2k - 1$.

Theorem 13. Every natural number is either even or odd.

Proof. Let $P(n)$ be the statement “$n$ is either even or odd”, for natural numbers $n$. We want to prove that $(\forall n \in \mathbb{N}) P(n)$.

We will prove this by induction. For this purpose, we will prove that $P(1)$ and that $(\forall n)(P(n) \implies P(n + 1))$.

Basis step. $P(1)$ is true, because $P(1)$ says that “1 is even or odd”, and that is true because 1 is odd.$^5$

Inductive step. We prove that $(\forall n \in \mathbb{N})(P(n) \implies P(n + 1))$.

Let $n$ be an arbitrary natural number.

We want to prove that $P(n) \implies P(n + 1)$. To prove this, we assume $P(n)$ and prove $P(n + 1)$.

So assume that $P(n)$ is true. Then $n$ is even or $n$ is odd. To prove that $P(n + 1)$ is true, we consider the cases when $n$ is even and when $n$ is odd. If $n$ is even, then we may pick $k \in \mathbb{N}$ such that $n = 2k$. Then $n + 1 = 2k + 1 = 2(k + 1) - 1$, and $k + 1 \in \mathbb{N}$. So $n + 1$ is odd. Hence $n + 1$ is even or odd, so $P(n + 1)$ is true. If $n$ is odd, then we may pick $k \in \mathbb{N}$ such

$^5$Why is 1 odd? Because $1 = 2k - 1$, if we take $k = 1$. 


that \( n = 2k - 1 \), so \( n + 1 = 2k \), and then \( n + 1 \) is even, so \( n + 1 \) is even or odd, so \( P(n + 1) \) is odd.

So we have proved that \( P(n+1) \) is true in both cases, so \( P(n+1) \) is true.

Since we have proved \( P(n + 1) \) assuming \( P(n) \), we have shown that \( P(n) \implies P(n + 1) \). Since this has been established for arbitrary \( n \in \mathbb{N} \), we have proved that \( (\forall n \in \mathbb{N})(P(n) \implies P(n + 1)) \). This concludes the inductive step.

Hence, by the PMI, \( P(n) \) is true for all \( n \in \mathbb{N} \). \( \Box \).

The following theorem is very important. It says that 1 is the only natural number which is not the successor of a natural number.

**Theorem 14.** If \( n \) is a natural number then:

1. If \( n = 1 \) then \( n - 1 \) is not a natural number.

2. If \( n \neq 1 \) then \( n - 1 \) is a natural number.

**Proof.** First of all, \( 1 - 1 = 0 \), and 0 is not a natural number, because Theorem 6 says that every natural number is greater than or equal to 1, while on the other hand \( 0 < 1 \), so 0 is not a natural number. This proves Part 1.

Now let us prove Part 2. For \( n \in \mathbb{N} \), let \( P(n) \) be the statement “\( n \neq 1 \implies n - 1 \in \mathbb{N} \)”.

We want to prove that \( (\forall n \in \mathbb{N})P(n) \).

We will prove this by induction. For this purpose, we will prove that \( P(1) \) and that \( (\forall n)(P(n) \implies P(n + 1)) \).

**Basis step.** \( P(1) \) is true, because \( P(1) \) says that “\( 1 \neq 1 \implies 1 - 1 \in \mathbb{N} \)” and this is true because it is an implication whose premise (“\( 1 \neq 1 \)” ) is false.

**Inductive step.** We must show that \( (\forall n \in \mathbb{N})(P(n) \implies P(n + 1)) \).

Let \( n \in \mathbb{N} \) be arbitrary. We want to prove that \( P(n) \implies P(n + 1) \). To show this, we assume \( P(n) \) and prove \( P(n + 1) \).

So assume \( P(n) \). That means that

\((*)\) \( n \neq 1 \implies n - 1 \in \mathbb{N} \).

Then \( P(n + 1) \) says

\((#)\) \( n + 1 \neq 1 \implies (n + 1) - 1 \in \mathbb{N} \).
But \((n + 1) - 1 = n\), and \(n \in \mathbb{N}\), so the conclusion \(\left( (n + 1) - 1 \in \mathbb{N} \right)\) of the implication \((\#)\) is true. Hence \((\#)\) is true. That is, \(P(n + 1)\) is true. So we have proved \(P(n + 1)\).

Since we have proved \(P(n + 1)\) assuming \(P(n)\), we have shown that \(P(n) \implies P(n + 1)\). Since this has been established for arbitrary \(n \in \mathbb{N}\), we have proved that \((\forall n \in \mathbb{N})(P(n) \implies P(n + 1))\). This concludes the inductive step.

Hence, by the PMI, \(P(n)\) is true for all \(n \in \mathbb{N}\). Q.E.D.

Now we prove another important theorem, that clarifies even more what the set \(\mathbb{N}\) looks like. We know that \(\mathbb{N}\) contains the numbers 1, 2, 3, etc. The next theorem says that \(\mathbb{N}\) contains nothing else: there is no natural number between 1 and 2, or between 2 and 3, or between 142 and 143.

**Theorem 15.** If \(n \in \mathbb{N}\) then there is no natural number \(q\) such that \(n < q < n + 1\).

**Proof.** For \(n \in \mathbb{N}\), let \(P(n)\) be the statement “there is no natural number \(q\) such that \(n < q < n + 1\).” We want to prove that \((\forall n \in \mathbb{N})P(n)\).

We will prove this by induction. For this purpose, we will prove that \(P(1)\) and that \((\forall n)(P(n) \implies P(n + 1))\).

**Basis step.** \(P(1)\) is true, because \(P(1)\) says that there are no natural numbers between 1 and 2, and this is true because of Theorem 7 on page 14. (“Every natural number is equal to 1 or \(\geq 2\). Hence a natural number \(q\) such that \(1 < q < 2\) cannot exist.)

**Inductive step.** We must show that \((\forall n \in \mathbb{N})(P(n) \implies P(n + 1))\).

Let \(n \in \mathbb{N}\) be arbitrary. We want to prove that \(P(n) \implies P(n + 1)\). To show this, we assume \(P(n)\) and prove \(P(n + 1)\).

So assume \(P(n)\). That means that

\((*)\) There does not exist a natural number \(q\) such that \(n < q < n + 1\).

We want to prove that \(P(n + 1)\) is true, i.e.,

\((\#)\) There does not exist a natural number \(q\) such that \(n + 1 < q < n + 2\).

We prove this by contradiction. Suppose that a natural number \(q\) such that \(n + 1 < q < n + 2\) exists. Pick one such number and call it \(q_0\). Then \(q_0 \in \mathbb{N}\) and \(n + 1 < q_0 < n + 2\). It then follows that \(q_0 \neq 1\) (because \(q_0 > n + 1\) and \(n + 1 > 1\), so \(q_0 > 1\)).
So, by Theorem 14, $q_0 - 1$ is a natural number. And it is clear that $n < q_0 - 1 < n+1$. So there exists a natural number $q$ such that $n < q < n+1$. But this contradicts (*).

So we have proved (♯). Hence $P(n + 1)$ is true.

Since we have proved $P(n + 1)$ assuming $P(n)$, we have shown that $P(n) \implies P(n + 1)$. Since this has been established for arbitrary $n \in \mathbb{N}$, we have proved that $(\forall n \in \mathbb{N})(P(n) \implies P(n + 1))$. This concludes the inductive step.

Hence, by the PMI, $P(n)$ is true for all $n \in \mathbb{N}$. Q.E.D.

### 2.1 Inductive definitions

In an earlier set of lectures, we defined “$x^2$”, for a real number $x$, to mean “$x \cdot x$”. And we can define “$x^3$” to mean “$(x \cdot x) \cdot x$”, or, if you prefer, “$x^2 \cdot x$”. But how can we define “$x^n$” for an arbitrary natural number $n$? One possibility would be to write something like this

$$x^n = x \times x \times \cdots \times x \quad \text{n times}$$

But this is very unclear. I do not know what “⋯” means, precisely (and if you think you do, please tell me!). And, in any case, “⋯” is not one of the basic symbols that are all the symbols we are allowed to use. (That is, 0, 1, +, −, ×, ÷, =, <, ≤, ≥, >, (, ), ∃, ∀, ∧, ∨, →, ↔, ~, ∈, ℝ, ℕ, ℤ, plus letter variables, and symbols defined later, such as 2, 3, 4, |, and ⊆).

#### 2.1.1 The inductive definition of powers of a real number

The way to define “$x^n$” correctly is by means of an inductive definition: we first define $x^1$ to be $x$, and then define $x^{n+1}$ to be $x^n \cdot x$, for every $n$. That is, we write:

**Definition 6.** (*Inductive definition of positive integer powers of a real number*) For all $a \in \mathbb{R}$, we set

$$a^1 = a,$$

$$a^{n+1} = a^n \cdot a \quad \text{for } n \in \mathbb{N}.$$ 

We also set $a^0 = 1$. □
Using this definition, we can write down what $a^n$ is for any $n$.

Suppose, for example, that we want to know what $a^5$ is. By the second line of our inductive definition of $a^n$,

$$a^5 = a^4 . a.$$  

This answers our question about $a^5$, in terms of $a^4$. And what is $a^4$? Again, using the second line of the inductive definition, we find

$$a^4 = a^3 . a.$$  

So

$$a^5 = ((a^3) . a) . a.$$  

And what is $a^3$? Once again, we can use the second line of the inductive definition, and find

$$a^3 = a^2 . a$$

So

$$a^5 = (((a^2) . a) . a) . a.$$  

One more step yields

$$a^2 = a^1 . a,$$

so

$$a^5 = (((a^1) . a) . a) . a.$$  

And, finally, the first line of the inductive definition, tells us that $a^1 = a$, so we end up with

$$a^5 = (((a . a) . a) . a) . a.$$  

Furthermore, since multiplication of real numbers has the associative property, we can omit the parentheses and just write:

$$a^5 = a . a . a . a . a.$$  

### 2.1.2 The inductive definition of the factorial

The “factorial” of a natural number $n$ is supposed to be the product $1 \times 2 \times 3 \times \cdots \times n$. That is, the factorial of $n$ is the product of all the natural numbers from 1 to $n$. Here is the inductive definition:
**Definition 7.** The factorial of a natural number $n$ is the number $n!$ given by

\[
\begin{align*}
1! &= 1, \\
(n + 1)! &= n! \times (n + 1) \quad \text{for } n \in \mathbb{N}.
\end{align*}
\]

(2.17) (2.18)

In addition, we define

\[0! = 1,\]

so $n!$ is defined for every nonnegative integer $n$. □

**Example 1.** Let us compute $7!$ using the inductive definition. Using (2.18) we get $7! = 7 \times 6!$. Then using (2.18) again we get $6! = 6 \times 5!$, so $7! = 7 \times 6 \times 5!$. Continuing in the same way we get $5! = 5 \times 4!$, so $7! = 7 \times 6 \times 5 \times 4!$, and then $4! = 4 \times 3!$, so $7! = 7 \times 6 \times 5 \times 4 \times 3!$. Then $3! = 3 \times 2!$, so $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2!$. And $2! = 2 \times 1!$, so $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1!$. Finally, (2.17) tells us that $1! = 1$, so we end up with

\[7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1.\]

**2.1.3 The inductive definition of summation.**

**Definition 8.** Suppose we have a natural number $n$, and a list

\[\mathbf{a} = (a_1, a_2, \ldots, a_n)\]

of length $n$ of real numbers. We define the sum (or summation) of the list $\mathbf{a}$ (also called the sum of the $a_j$ for $j$ from 1 to $n$) to be the number $\sum_{j=1}^{n} a_j$ determined as follows:

\[
\begin{align*}
\sum_{j=1}^{1} a_j &= a_1, \\
\sum_{j=1}^{n+1} a_j &= \left(\sum_{j=1}^{n} a_j\right) + a_{n+1} \quad \text{for } n \in \mathbb{N}.
\end{align*}
\]

And we also define $\sum_{j=1}^{0} a_j = 0$. 
Example 2. Let us compute $\sum_{j=1}^{5} j^2$. We have

\[
\sum_{j=1}^{5} j^2 = \left( \sum_{j=1}^{4} j^2 \right) + 5^2 = \left( \sum_{j=1}^{3} j^2 \right) + 4^2 + 5^2 = \sum_{j=1}^{2} j^2 + 3^2 + 4^2 + 5^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 1 + 4 + 9 + 16 + 25 = 55.
\]

2.1.4 Inductive definition of product.

Definition 9. For a natural number $n$, and a list $a = (a_1, a_2, \ldots, a_n)$ of length $n$ of real numbers, we define the product of the $a_j$ for $j$ from 1 to $n$ to be the number $\prod_{j=1}^{n} a_j$ determined as follows:

\[
\prod_{j=1}^{1} a_j = a_1,
\]

\[
\prod_{j=1}^{n+1} a_j = \left( \prod_{j=1}^{n} a_j \right) \times a_{n+1} \text{ for } n \in \mathbb{N}.
\]

And we also define $\prod_{j=1}^{0} a_j = 1$.

Example 3. If you compare the inductive definition of a product with inductive definition of the factorial, you can easily see that

\[
n! = \prod_{j=1}^{n} j \text{ for every } n \in \mathbb{N}.
\]
2.1.5 Some examples of proofs using inductive definitions

**Theorem 16.** For all $n \in \mathbb{N}$

$$
\sum_{k=1}^{n} (2k - 1) = n^2.
$$

(That is, the sum of the first $n$ odd numbers is a perfect square, namely, $n^2$.)

**Proof.** For $n \in \mathbb{N}$, let $P(n)$ be the statement \("\sum_{k=1}^{n} (2k - 1) = n^2 \)\). We want to prove that $(\forall n \in \mathbb{N})P(n)$.

We will prove this by induction. For this purpose, we will prove that $P(1)$ and that $(\forall n)(P(n) \implies P(n + 1))$.

**Basis step.** $P(1)$ is true, because $P(1)$ says that $\sum_{k=1}^{1} (2k - 1) = 1^2$, which is true because $\sum_{k=1}^{1} (2k - 1) = 1$ and $1^2 - 1$.

**Inductive step.** We prove that $(\forall n \in \mathbb{N})(P(n) \implies P(n + 1))$.

Let $n$ be an arbitrary natural number. We want to prove that $P(n) \implies P(n + 1)$. To prove this, we assume $P(n)$ and prove $P(n + 1)$.

So assume that $P(n)$ is true. Then

$$
\sum_{k=1}^{n} (2k - 1) = n^2.
$$

We want to prove that $P(n + 1)$ is true, i.e., that

$$
\sum_{k=1}^{n+1} (2k - 1) = (n + 1)^2. \quad (2.19)
$$

But, by the inductive definition of “summation”,

$$
\sum_{k=1}^{n+1} (2k - 1) = \sum_{k=1}^{n} (2k - 1) + (2(n + 1) - 1).
$$

And our inductive assumption tells us that

$$
\sum_{k=1}^{n} (2k - 1) = n^2.
$$
So
\[
\sum_{k=1}^{n+1} (2k - 1) = \sum_{k=1}^{n} (2k - 1) + (2(n + 1) - 1)
\]
\[
= n^2 + (2(n + 1) - 1)
\]
\[
= n^2 + (2n + 2 - 1)
\]
\[
= n^2 + 2n + 1
\]
\[
= (n + 1)^2.
\]

Hence (2.19) is true. So we have proved that \( P(n + 1) \) is true, assuming \( P(n) \).

Since we have proved \( P(n + 1) \) assuming \( P(n) \), we have shown that \( P(n) \Rightarrow P(n + 1) \). Since this has been established for arbitrary \( n \in \mathbb{N} \), we have proved that \( (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n + 1)) \). This concludes the inductive step.

Hence, by the PMI, \( P(n) \) is true for all \( n \in \mathbb{N} \).

Q.E.D.

**Theorem 17.** For all \( n \in \mathbb{N} \)
\[
\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.
\]

**Proof.** For \( n \in \mathbb{N} \), let \( P(n) \) be the statement \( \sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \). We want to prove that \( (\forall n \in \mathbb{N})(P(n)) \).

We will prove this by induction. For this purpose, we will prove that \( P(1) \) and that \( (\forall n)(P(n) \Rightarrow P(n + 1)) \).

**Basis step.** \( P(1) \) is true, because \( P(1) \) says that
\[
\sum_{k=1}^{1} k^2 = \frac{1}{3} + \frac{1}{2} + \frac{1}{6},
\]
and this is true because \( \sum_{k=1}^{1} k^2 = 1 \) and \( \frac{1}{3} + \frac{1}{2} + \frac{1}{6} = 1 \).

**Inductive step.** We prove that \( (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n + 1)) \).

Let \( n \) be an arbitrary natural number. We want to prove that \( P(n) \Rightarrow P(n + 1) \). To prove this, we assume \( P(n) \) and prove \( P(n + 1) \).
So assume that $P(n)$ is true. Then

$$\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$  

We want to prove that $P(n + 1)$ is true, i.e., that

$$\sum_{k=1}^{n+1} k^2 = \frac{(n + 1)^3}{3} + \frac{(n + 1)^2}{2} + \frac{n + 1}{6}. \quad (2.20)$$

But, by the inductive definition of “summation”,

$$\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n + 1)^2.$$  

And our inductive assumption tells us that

$$\sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}.$$  

So

$$\sum_{k=1}^{n+1} k^2 = \left( \sum_{k=1}^{n} k^2 \right) + (n + 1)^2$$
$$= \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} + (n + 1)^2.$$  

Now we have to prove that

$$\frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} + (n + 1)^2 = \frac{(n + 1)^3}{3} + \frac{(n + 1)^2}{2} + \frac{n + 1}{6}. \quad (2.21)$$

But

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

so

$$\frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} + (n + 1)^2 = \frac{n^3}{3} + \frac{3n^2}{2} + \frac{13n}{6} + 1,$$
and

\[
\frac{(n + 1)^3}{3} + \frac{(n + 1)^2}{2} + \frac{n + 1}{6} = \frac{n^3 + 3n^2 + 3n + 1}{3} + \frac{n^2 + 2n + 1}{2} + \frac{n + 1}{6}
\]

\[
= \frac{n^3}{3} + n^2 + n + \frac{1}{3} + \frac{n^2}{2} + n + \frac{1}{2} + \frac{n}{6} + \frac{1}{6}
\]

\[
= \frac{n^3}{3} + \frac{3n^2}{2} + \frac{13n}{6} + 1.
\]

So both sides of (2.21) are equal to \(\frac{n^3}{3} + \frac{3n^2}{2} + \frac{13n}{6} + 1\). Hence (2.21) is true, and therefore (2.20) is true. So we have proved that \(P(n + 1)\) is true. Since we have proved \(P(n + 1)\) assuming \(P(n)\), we have shown that \(P(n) \implies P(n + 1)\). Since this has been established for arbitrary \(n \in \mathbb{N}\), we have proved that \((\forall n \in \mathbb{N})(P(n) \implies P(n + 1))\). This concludes the inductive step.

Hence, by the PMI, \(P(n)\) is true for all \(n \in \mathbb{N}\). \(\text{Q.E.D.}\)

**Theorem 18.** Let \(n\) be a natural number, and let \(A\) be a finite set and suppose that \(A\) has \(n\) members. i.e., that \(|A| = n\). Then \(|\mathcal{P}(A)| = 2^n\). That is, the power set \(\mathcal{P}(A)\) has \(2^n\) members.

**Proof.** For \(n \in \mathbb{N}\), let \(P(n)\) be the statement “\((\forall A)(|A| = n \implies |\mathcal{P}(A)| = 2^n)\)”.

We prove \((\forall n \in \mathbb{N})P(n)\), which is exactly what we want.

**Basis step.** We want to prove that \(P(1)\) is true. But \(P(1)\) says that “if a set \(A\) has one member, then the power set \(\mathcal{P}(A)\) has 2 members. And that is true, because if \(A = \{a\}\), then \(\mathcal{P}(A) = \{\emptyset, \{a\}\}\), so \(|\mathcal{P}(A)| = 2\).

**Inductive step.** We want to prove that \((\forall n \in \mathbb{N})(P(n) \implies P(n + 1))\).

Let \(n \in \mathbb{N}\) be arbitrary. Assume that \(P(n)\) is true. This means that if \(A\) is any set with \(n\) members then \(\mathcal{P}(n)\) has \(2^n\) members. We want to prove \(P(n + 1)\), that is, that

\[
(\forall A)(|A| = n + 1 \implies |\mathcal{P}(A)| = 2^{n+1}).
\]  

(2.22)

In order to prove (2.22), we let \(A\) be an arbitrary set and assume that \(|A| = n + 1\). We want to prove that \(\mathcal{P}(A)\) has \(2^{n+1}\) members.
Pick a member of A and call it a. Then the set $B = A - \{a\}$ has n members. Since we are assuming that $P(n)$ is true, we can assert that the power set $\mathcal{P}(B)$ has $2^n$ members.

So we can list the members of $\mathcal{P}(B)$ in a list

$$L = (S_1, S_2, \ldots, S_{2^n})$$

of length $2^n$.

Now, for every subset $S$ of $B$, we can construct two subsets $\tilde{S}$ and $\hat{S}$ of $A$ as follows:

$$\tilde{S} = S,$$
$$\hat{S} = S \cup \{a\}.$$ 

The sets $\tilde{S}$ are exactly the subsets $X$ of $A$ such that $a \notin X$. And the sets $\hat{S}$ are exactly the subsets $X$ of $A$ such that $a \in X$. So the list

$$M = (\tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_{2^n}, \hat{S}_1, \hat{S}_2, \ldots, \hat{S}_{2^n})$$

is a list without repetition of all the members of $\mathcal{P}(A)$.

Hence $|\mathcal{P}(A)| = 2 \times 2^n = 2^{n+1}$. So $P(n + 1)$ holds. Q.E.D.

3 The main theorems of elementary natural number arithmetic

We now study the phenomena that make the natural numbers and the integers different in crucial ways from the real numbers. The root of this difference is that the division operation in $\mathbb{N}$ and $\mathbb{Z}$ is very different from division in $\mathbb{R}$.

In this section we will focus on the natural numbers. Later we will extend the theorems to the integers.

The first theorem about division of natural numbers is the one that tells us that one can always “divide two natural numbers with a remainder”. If $a$ and $b$ are natural numbers, then we cannot find a “quotient” $a \div b$ in $\mathbb{N}$ or in $\mathbb{Z}$, but we can “divide with a remainder”, that is, find integers $q, r$, such that $a = bq + r$ and $0 \leq r < |b|$.

**Theorem 19.** If $a, b$ are natural numbers, then there exist unique integers $q, r$ such that $a = bq + r$ and $0 \leq r < b$.

The above statement needs clarification: I have to tell you what the word “unique” means.
3.1 Existence and uniqueness

Suppose $P(x)$ is a one-variable predicate. We write

$$(\exists! x) P(x)$$

for “there exists a unique $x$ such that $P(x)$.”

This means “there is one and only one $x$ such that $P(x)$”.

The precise meaning of this is that

1. there exists an $x$ such that $P(x)$,

and

2. if $x_1$, $x_2$ are such that $P(x_1) \land P(x_2)$, then $x_1 = x_2$.

In formal language:

$$(\exists! x) P(x) \iff (\exists x) P(x) \land (\forall x_1)(\forall x_2)(P(x_1) \land P(x_2)) \implies x_1 = x_2$$.

It follows that, in order to prove that there exists a unique $x$ such that $P(x)$, you must prove two things:

**Existence:** There exists $x$ such that $P(x)$,

**Uniqueness:** Any two $x$’s that satisfy $P(x)$ must be equal.

That is:

To prove $$(\exists! x) P(x)$$

it suffices to prove

$$(\exists x) P(x) \quad (3.23)$$

and

$$(\forall x_1)(\forall x_2)\left((P(x_1) \land P(x_2)) \implies x_1 = x_2\right). \quad (3.24)$$

(Formula (3.23) is the existence assertion, and Formula (3.24) is the uniqueness assertion.)
Example 4. “I have one and only one mother” means:

- I have a mother,

and

- Any two people who are my mother must be the same person. (That is: if $u$ is my mother and $v$ is my mother than $u = v$.)

\[\square\]

3.1.1 An example of a proof of existence and uniqueness

Problem 2. Prove that there exists a unique natural number $n$ such that $n^3 = 2n - 1$.

Solution. We want to prove that

$$\exists! n \in \mathbb{N} n^3 = 2n - 1.$$

First let us prove existence. We have to prove that $\exists n \in \mathbb{N} n^3 = 2n - 1$. To prove this, we exhibit a witness: we take $n = 1$. Then $n$ is a natural number, and $n^3 = 2n - 1$. So $\exists n \in \mathbb{N} n^3 = 2n - 1$.

Next we prove uniqueness. We have to prove that if $u, v$ are natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$, then it follows that $u = v$.

So let $u, v$ be natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$.

We want to prove that $u = v$.

Since $u^3 = 2u - 1$ and $v^3 = 2v - 1$, we have

$$u^3 - v^3 = 2u - 1 - (2v - 1)$$
$$= 2u - 2v$$
$$= 2(u - v),$$

so

$$u^3 - v^3 - 2(u - v) = 0.$$

But it is easy to verify that

$$u^3 - v^3 = (u - v)(u^2 + uv + v^2).$$

(If you do not believe this, just multiply out the right-hand side and you will find that the result equals $u^3 = v^3$.) Hence

$$0 = u^3 - v^3 - 2(u - v)$$
$$= (u - v)(u^2 + uv + v^2) - 2(u - v)$$
$$= (u - v)(u^2 + uv + v^2 - 2).$$
We know from a previous set of lectures that if a product of two real numbers is zero then one of the numbers must be zero. Hence
\[ u - v = 0 \quad \text{or} \quad u^2 + uv + v^2 - 2. \]

But \( u^2 + uv + v^2 - 2 \) cannot be equal to zero, because \( u^2, \ uv \) and \( v^2 \) are natural numbers, so each of them is greater than or equal to 1, and then \( u^2 + uv + v^2 \geq 3 \), so \( u^2 + uv + v^2 - 2 \geq 1 \), and then \( u^2 + uv + v^2 - 2 \neq 0 \). Therefore \( u - v = 0 \), so \( u = v \), and our proof of uniqueness is complete.

\textbf{Problem 3.} Prove that there exists a unique real number \( x \) such that \( x > 0 \) and \( x^2 = x + 1 \).

\[ \square \]

3.2 \textbf{Proof of Theorem 19 (the division theorem for natural numbers)}

We will first prove the existence part. Let \( a, b \) be arbitrary natural numbers. I will prove by induction that
\[ (\forall n \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \land 0 \leq r < b). \quad (3.25) \]

Once we have proved (3.25), we can apply it with \( n = a \) and conclude that there exist natural numbers \( q, r \) such that \( a = bq + r \) and \( 0 \leq r < b \).

We let \( P(n) \) be the statement “(\( \exists q \in \mathbb{Z} \)(\( \exists r \in \mathbb{Z} \))(n = bq + r \land 0 \leq r < b) \)”.

\textbf{Basis step.} We prove \( P(1) \). We have to produce integers \( q, r \) such that \( 1 = bq + r \) and \( 0 \leq r < b \). But this is easy: if \( b - 1 \) we take \( q = 1 \) and \( r = 0 \); then \( 1 = bq + r \) and \( 0 \leq r < b \). And if \( b > 1 \) we take \( q = 0, \ r = 1 \). And we also have \( 1 = bq + r \) and \( 0 \leq r < b \).

\textbf{Inductive step.} Let \( n \in \mathbb{N} \) be arbitrary. Assume \( P(n) \) is true. Let us prove \( P(n + 1) \).

Since \( P(n) \) is true, we can pick integers \( q, r \) such that \( n = bq + r \) and \( 0 \leq r < b \).

Then the number \( r + 1 \) cannot be greater than \( b \). (Reason: suppose \( r + 1 > b \). Then \( r < b < r + 1 \). But this contradicts theorem 15.)

Hence \( r + 1 \leq b \). We distinguish two cases: \( r + 1 < b \) and \( r + 1 = b \).

\textbf{The case when} \( r + 1 < b \). In this case, we take \( q' = q \) and \( r' = r + 1 \), and we get \( n + 1 = bq' + r' \) and \( 0 \leq r' < b \). So \( P(n + 1) \) is true.
The case when $r + 1 = b$. In this case, we take $q' = q + 1$ and $r' = 0$, and we get $n + 1 = bq' + r'$ and $0 \leq r' < b$. So $P(n + 1)$ is true.

we have proved that $P(n + 1)$ is true in both cases. So we have proved $P(n + 1)$.

This completes the inductive step. It follows from the PMI that $(\forall n \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \land 0 \leq r < b)$. We can then apply this to $n = a$, and conclude that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \land 0 \leq r < b).$$

This completes the proof of the existence part of the theorem.

Now let us prove uniqueness. Suppose $q_1, q_2, r_1, r_2$ are integers such that

\[
\begin{align*}
  a &= bq_1 + r_1 \\
  0 &\leq r_1 < b \\
  a &= bq_2 + r_2 \\
  0 &\leq r_2 < b.
\end{align*}
\]

We prove that $q_1 = q_2$ and $r_1 = r_2$. Assume that $r_1 \geq r_2$. Then $0 \leq r_1 - r_2 < b$. And $bq_1 + r_1 = bq_2 + r_2$, so

\[
b(q_2 - q_1) = r_1 - r_2.
\]

Then $r_1 - r_2$ is divisible by $b$, which is impossible since $0 \leq r_1 - r_2 < b$, unless $r_1 - r_2 = 0$.

So $r_1 - r_2 = 0$, and then $r_1 = r_2$. Hence $bq_1 = bq_2$, and this implies that $q_1 = q_2$, since $b \neq 0$.

This completes the proof of the uniqueness part. So our proof is complete.

Q.E.D.

4 The Well Ordering Principle

The well ordering principle is a very powerful tool for proving results about the natural numbers. Every proof by induction can easily be transformed into a proof by well ordering, but there are many proofs by well ordering that cannot easily be turned into a proof by induction\(^6\).

In this section we are going to

\(^6\)The key word here is “easily”. Every proof by well ordering can be reformulated as a proof by induction, but often this is rather complicated.
1. state the well ordering principle,
2. prove it,
3. give examples of proofs using well ordering.

4.1 Statement of the well ordering principle

Theorem 20. Every nonempty set of natural numbers has a smallest member.

In formal language, this says that

\[(\forall S)\left((S \subseteq \mathbb{N} \land S \neq \emptyset) \implies (\exists s)(s \in S \land (\forall s \in S)s \leq s)\right) .\]

4.2 Proof of the well ordering principle

First we prove a lemma:\footnote{Recall that a lemma is a result one proves as a preliminary towards proving a theorem.}

Lemma 1. If \( n \) is a natural number and \( S \) is a subset of \( \mathbb{N} \) such that \( n \in S \), then \( S \) has a smallest member.

Proof. We want to prove that

\[(\forall n \in \mathbb{N})(\forall S)\left((S \subseteq \mathbb{N} \land n \in S) \implies S \text{ has a smallest member}\right). \quad (4.26)\]

Let \( P(n) \) be the sentence

\[(\forall S)\left((S \subseteq \mathbb{N} \land n \in S) \implies S \text{ has a smallest member}\right) .\]

We want to prove that \((\forall n \in \mathbb{N})P(n)\). And we will do this by induction.

Basis step. We want to prove that \( P(1) \) is true. But \( P(1) \) says that if \( S \) is a subset of \( \mathbb{N} \) and \( 1 \in S \) then \( S \) has a smallest member. But this is obviously true because 1 is the smallest member of \( S \), since 1 is less than or equal to every natural number, so in particular it is less than or equal to every member of \( S \).
**Inductive step.** We want to prove that $\forall n \in \mathbb{N}(P(n) \implies P(n + 1))$.

Let $n$ be an arbitrary natural number. We want to prove that $P(n) \implies P(n + 1)$.

Assume $P(n)$. We want to prove $P(n + 1)$.

Now, $P(n + 1)$ says that $(\forall S)(S \subseteq \mathbb{N} \land n + 1 \in S) \implies S$ has a smallest member.

To prove this, let $S$ be an arbitrary set.

Assume that $S \subseteq \mathbb{N}$ and $n + 1 \in S$. We want to prove that $S$ has a smallest member.

Clearly, either $n$ belongs to $S$ or it does not.
If $n \in S$ then it follows from the inductive hypothesis $P(n)$ that $S$ has a smallest member. (Recall that $P(n)$ says that if a subset $X$ of $\mathbb{N}$ is such that $n \in X$ then $X$ has a smallest member.)
Next consider the case when $n \notin S$.
In that case, let us form a new set $T$ by adding $n$ to $S$.
That is, let us introduce a set $T$ defined by

$$T = \{x : x \in S \lor x = n\}.$$

Then $T \subseteq \mathbb{N}$ (because $S \subseteq \mathbb{N}$ and $n \in \mathbb{N}$) and $n \in T$.
So by the inductive hypothesis (which says that a subset $X$ of $\mathbb{N}$ for which $n \in X$ has a smallest member), $T$ has a smallest member. Call this smallest member $\bar{t}$.
Then $\bar{t} \in T$, and $\bar{t} \leq t$ for every $t \in T$.
In particular, $\bar{t} \leq s$ for every $s \in S$ (because every member of $S$ is a member of $T$).
There are two possibilities: $\bar{t} \in S$ or $\bar{t} \notin S$.
Assume that $\bar{t} \in S$.
Then $\bar{t}$ is a member of $S$ that is smaller than or equal to every member of $S$. So $\bar{t}$ is the smallest member of $S$. Hence $S$ has a smallest member.
Now consider the case when $\bar{t} \notin S$. Since $\bar{t} \in T$, and the only member of $T$ that can possibly not be in $S$ is $n$, it follows that $\bar{t} = n$. Hence $n \leq s$ for every $s \in S$.

Let $s$ be an arbitrary member of $S$.

Then $s \geq n$.

So $s > n$, because if $s$ was equal to $n$ then $n$ would be in $S$, and we are assuming that $n \notin S$.

But then $s \geq n + 1$. Reason: Suppose not. Then $s < n + 1$. But we have shown that $s > n$. So $n < s < n + 1$. But we know that there do not exist any natural numbers that lie between $n$ and $n + 1$. (This was proved in Theorem 15 on page 24.)

So we have shown that $s \geq n + 1$ for every member $s$ of $S$.

In addition, we are assuming that $n + 1 \in S$. Hence $n + 1$ is the smallest member of $S$.

So $S$ has a smallest member.

We have proved that $S$ has a smallest member in each of the two cases $\bar{t} \in S$ and $\bar{t} \notin S$. It then follows, using the Proof by Cases Rule, that $S$ has a smallest member.

We have proved that $S$ has a smallest member assuming that $S \subseteq \mathbb{N}$ and $n + 1 \in S$. Hence

\[(S \subseteq \mathbb{N} \land n + 1 \in S) \implies S \text{ has a smallest member}. \quad (4.27)\]

We have proved (4.27) under the assumption that $S$ was an arbitrary set. Hence

\[(\forall S)\left((S \subseteq \mathbb{N} \land n + 1 \in S) \implies S \text{ has a smallest member}\right). \quad (4.28)\]

But (4.28) is exactly statement $P(n + 1)$. So we have proved $P(n + 1)$.

We have proved $P(n + 1)$ assuming $P(n)$. It then follows that $P(n) \implies P(n + 1)$. 

We have proved that $P(n) \implies P(n+1)$ for an arbitrary $n \in \mathbb{N}$.

Hence $(\forall n \in \mathbb{N})(P(n) \implies P(n+1))$. This completes the inductive step.

It follows from the PMI that $(\forall n \in \mathbb{N})P(n)$. Q.E.D.

Having proved the lemma, the proof of the well ordering principle is easy.

**Proof of Theorem 20.** Let $S$ be a nonempty subset of $\mathbb{N}$. Then we may pick a member of $S$ and call it $n$. Then $n$ is a natural number and $n \in S$. So by the lemma $S$ has a smallest member. Q.E.D.

### 4.3 An example of a proof using well-ordering

**Theorem 21.** Every natural number $n$ such that $n \geq 2$ is a product of primes.

Before we prove the theorem, let us explain what it says.

**Clarification: What is a “product of primes”?** A natural number $n$ is a product of primes if there exist

1. a natural number $k$,

and

2. a list $p = (p_1, \ldots, p_k)$ of prime numbers,

such that

$$n = \prod_{i=1}^{k} p_i. \quad (4.29)$$

Notice that $k$ can be equal to one. That is, a single prime, such as 2, or 3, or 23, is a product of primes in the sense of our definition.

**Definition 10.** If $n$ is a natural number, then a list $p = (p_1, \ldots, p_k)$ of prime numbers such that (4.29) holds is called a prime factorization of $n$. □

**Example 5.** The following natural numbers are products of primes: 7 (because it is prime), 24 (because $24 = 2 \times 2 \times 2 \times 3$), 309 (because $309 = 3 \times 103$ and both 3 and 103 are prime). □
Outline of the strategy for proving the theorem. Call a natural number \( n \) “bad” if \( n > 1 \) and \( n \) is not a product of primes.

What we want is to prove is that there are no bad natural numbers.

The strategy is going to be this: we let \( B \) be the set of all bad numbers, so our goal is to prove that \( B \) is empty. For this purpose, we assume it is nonempty, and use the Well Ordering Principle to conclude that it has a smallest member \( b \). Then \( b \) is bad, and in addition \( b \) is the smallest bad natural number. But then \( b \) cannot be prime, because if it is prime then it is a product of primes, so \( b \) would not be bad. Since \( b > 1 \), \( b \) must be a product \( cd \) of two smaller natural numbers. But then \( c \) and \( d \) cannot be bad. So \( c \) is a product \( p_1 \times p_2 \times \cdots \times p_k \) of primes, and \( d \) is a product \( q_1 \times q_2 \times \cdots \times q_j \) of primes. So

\[
b = cd = p_1 \times p_2 \times \cdots \times p_k \times q_1 \times q_2 \times \cdots \times q_j .
\]

But then \( b \) is a product of primes, so \( b \) is not bad. But \( b \) is bad, and we got a contradiction. Hence \( B \) is empty, and that means that there are no bad numbers.

Proof of the theorem. Let \( B \) be the set of all natural numbers \( n \) such that \( n \geq 2 \) and \( n \) is not a product of primes.

We want to prove that the set \( B \) is empty. For this purpose, we assume that \( B \) is not empty and try to get a contradiction.

So assume that \( B \neq \emptyset \). By the well-ordering principle, \( B \) has a smallest member \( b \). Then \( b \in B \), so

a. \( b \) is a natural number,

b. \( b \geq 2 ,

c. \( b \) is not a product of primes.

And, in addition,

d. \( b \) is the smallest member of \( B \), that is,

\[
(\forall m)(m \in B \Rightarrow m \geq b) .
\]

Since \( b \) is not a product of primes, it follows in particular that \( b \) is not prime. (Reason: if \( b \) was prime, then \( b \) would be a product of primes according to our definition.) Then we can pick natural numbers \( j,k \) such that

\[
b = jk , \quad j > 1 , \quad \text{and} \quad k > 1 .
\]
Then \( j < b \), because \( b = jk \) and \( k > 1 \). So \( j \notin B \) (because \( b \) is the smallest member of \( B \), and \( j < b \)). And \( j \geq 2 \) (because \( j > 1 \)). This means that \( j \) is a product of primes (because if \( j \) wasn’t a product of primes it would be in \( S \)).

Similarly, \( k \) is a product of primes. So we can write \( j = \prod_{i=1}^{m} p_i \) and \( k = \prod_{\ell=1}^{\mu} q_\ell \), where the \( p_i \) and the \( q_\ell \) are primes. But then

\[
b = \left( \prod_{i=1}^{m} p_i \right) \times \left( \prod_{\ell=1}^{\mu} q_\ell \right),
\]

so \([b \text{ is a product of primes}]\). But \([b \text{ is not a product of primes}]\). So we got two contradictory statements.

This contradiction was derived by assuming that \( B \neq \emptyset \). So \( B = \emptyset \), and this proves that every natural number \( n \) such that \( n \geq 2 \) is a product of primes, which is our desired conclusion. \( \text{Q.E.D.} \)

**Remark 2.** The fundamental theorem of arithmetic (FTA). This theorem is one of the most important results in integer arithmetic. It says that every natural number greater than 2 can be written as a product of primes in a unique way. (That is, not only is the number equal to a product of primes, but there is only one way to write it as a product of primes.) We have proved a part of the FTA, namely, the assertion that if \( n \in \mathbb{N} \) and \( n \geq 2 \) then \( n \) can be written as a product of primes. What we have not proved is the uniqueness of the factorization. This is much more delicate, and we will prove it later. At this point, just notice that even defining what “uniqueness” of the factorization of \( n \) into primes means is not a trivial question. For example, we can write the number 6 as a product of primes in this way:

\[
6 = 2 \times 3,
\]

but we can also write it as

\[
6 = 3 \times 2.
\]

Are these two expressions different ways of factoring 6 as a product of primes, or are they “the same”? Obviously, they must be “the same”. because if they were different then the factorization of 6 as a product of primes would not be unique, and the FTA would not be true.

This means that we will have to be very precise, and define very carefully what “writing a number as a product of primes in a unique way” means. And this will be done later. \( \square \)
4.4 Two theorems about the Fibonacci numbers

The Fibonacci numbers \( f_n \) (for \( n \in \mathbb{N} \)) are defined as follows:

\[
\begin{align*}
    f_1 &= 1, \\
    f_2 &= 1, \\
    f_{n+2} &= f_n + f_{n+1} \quad \text{for } n \in \mathbb{N}.
\end{align*}
\]

Remark 3. The definition of the Fibonacci numbers looks very much like an inductive definition, except that, instead of defining each Fibonacci number in terms of the previous one, we define each Fibonacci number in terms of the two preceding ones. For this reason, the definition of the Fibonacci numbers is said to be a two-step inductive definition. □

Example 6. Here are the first twelve Fibonacci numbers:

\[
\begin{align*}
    f_1 &= 1, & f_2 &= 1, & f_3 &= 2, & f_4 &= 3, \\
    f_5 &= 5, & f_6 &= 8, & f_7 &= 13, & f_8 &= 21, \\
    f_9 &= 34, & f_{10} &= 55, & f_{11} &= 89, & f_{12} &= 144.
\end{align*}
\]

We now prove an upper bound and an identity for the Fibonacci numbers. In these results, there appears a very famous number, the “golden ratio”. So we first define this number.

Definition 11. The golden ratio is the real number \( \varphi \) given by

\[
\varphi = \frac{1 + \sqrt{5}}{2}.
\]

Remark 4. The golden ratio also has several other names: the golden mean, the golden section, the divine proportion, the divine section, and also the golden proportion.

If you want to find out why this number is so important and so famous, you should read something about it:

**Strongly recommended reading:** The Wikipedia article entitled “golden ratio”.

In these notes, I will just give you two results showing that the golden ratio is closely related to the Fibonacci numbers, and I will prove one of these results, leaving the other one for you to prove.

**Theorem 22.** The Fibonacci numbers $f_n$ satisfy the bound

$$f_n \leq \varphi^{n-1} \quad \text{for every } n \in \mathbb{N}, \quad (4.30)$$

where $\varphi$ is the golden ratio, that is, $\varphi = \frac{1 + \sqrt{5}}{2}$.

**Theorem 23.** (Binet’s formula) The Fibonacci numbers $f_n$ satisfy the identity

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}} \quad \text{for every } n \in \mathbb{N}, \quad (4.31)$$

where $\varphi$ is the golden ratio, that is, $\varphi = \frac{1 + \sqrt{5}}{2}$, and $\psi$ is the number given by

$$\psi = \frac{1 - \sqrt{5}}{2}.$$

**Proof of Theorem 22.** First, we observe that

$$\varphi^2 = \varphi + 1. \quad (4.32)$$

(This is a simple calculation: $\varphi^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \varphi$.)

We now prove that

$$(\forall n \in \mathbb{N}) \ f_n \leq \varphi^{n-1}. \quad (4.33)$$

We define $B$ to be the set of all natural numbers $n$ for which the inequality $“f_n \leq \varphi^{n-1}”$ is not true. That is, we let

$$B = \{n \in \mathbb{N} : f_n > \varphi^{n-1}\}.$$  

(Think of $B$ as the set of all “bad” numbers, that is, the numbers that we want to prove don’t exist at all.)

We want to prove that $B$ is the empty set. We do this by contradiction: we assume that $B \neq \emptyset$, and will try to derive a contradiction.

Since $B$ is nonempty, the well-ordering principle implies that $B$ has a smallest member $b$. Then

1. $b \in B$, so
a. \( b \in \mathbb{N} \),

and

b. \( f_b > \varphi^{b-1} \).

Furthermore, \( b \) is the smallest member of \( B \), so

2. If \( n \in \mathbb{N} \) and \( n < b \), then \( f_n \leq \varphi^{n-1} \).

Next, we observe that if \( b \geq 3 \) then \( f_b \) is given as the sum of the two preceding Fibonacci numbers, but if \( b = 1 \) or \( b = 2 \) then \( b \) is not given in that way. So it is natural to consider separately the cases \( b = 1 \), \( b = 2 \), and \( b \geq 3 \).

First, consider the case when \( b = 1 \). Then \( f_b = 1 \), and \( \varphi^{b-1} = \varphi^0 = 1 \). (Recall that \( a^0 = 1 \) for all real numbers \( a \).) So the inequality \( f_b \leq \varphi^{b-1} \) is true.

Next, consider the case when \( b = 2 \). Then \( f_b = 1 \), and \( \varphi^{b-1} = \varphi = \frac{1 + \sqrt{5}}{2} \).

Clearly, \( \frac{1 + \sqrt{5}}{2} \geq 1 \) (because \( \sqrt{5} \geq 1 \), so \( 1 + \sqrt{5} \geq 2 \) and then \( \frac{1 + \sqrt{5}}{2} \geq 1 \)). So the inequality \( f_b \leq \varphi^{b-1} \) is true in this case as well.

Finally, consider the case when \( b \geq 3 \). In this case, we know that

\[
    f_b = f_{b-2} + f_{b-1}.
\]

And we also know that the inequalities

\[
    f_{b-1} \leq \varphi^{b-2}, \tag{4.34}
\]

\[
    f_{b-2} \leq \varphi^{b-3}, \tag{4.35}
\]

hold, because \( b - 1 \) and \( b - 2 \) are smaller than \( b \), so \( b - 1 \) and \( b - 2 \) do not belong to \( B \).

If we add (4.34) and (4.35), we get

\[
    f_{b-2} + f_{b-1} \leq \varphi^{b-2} + \varphi^{b-3}. \tag{4.36}
\]

But

\[
    f_{b-2} + f_{b-1} = f_b,
\]

and

\[
    \varphi^{b-2} + \varphi^{b-3} = (\varphi + 1)\varphi^{b-3} = \varphi^2 \varphi^{b-3} = \varphi^{b-1},
\]

(using the fact that \( \varphi + 1 = \varphi^2 \)), so (4.36) implies that \( f_b \leq \varphi^{b-1} \).
So we have proved that the inequality $f_b \leq \phi^{b-1}$ holds in all three cases ($b = 1$, $b = 2$, and $b \geq 3$). It follows (using the Proof by Cases Rule) that

$$f_b \leq \phi^{b-1}. \quad (4.37)$$

But, as we established before,

$$f_b > \phi^{b-1}. \quad (4.38)$$

Inequalities (4.37) and (4.38) contradict each other. This contradiction arose from assuming that $B \neq \emptyset$. So $B$ is empty, and this proves out desired conclusion. Q.E.D.

**Proof of Theorem 23. YOU DO THIS PROOF.**

*Important observation, that will play a crucial role in your proof:* We already pointed out before that

$$\phi^2 = 1 + \phi.$$  

It turns out that the number $\psi$ also satisfies

$$\psi^2 = 1 + \psi.$$  

(You can verify this by a simple computation.)

In other words, *the numbers $\phi$, $\psi$ are the two solutions of the equation $x^2 = x + 1$.*

**Problem 4. Prove Theorem 23.**