1 What this course is about

This course is about mathematical reasoning. This means “reasoning about mathematical objects in a mathematical way.” To make this clear, we have to talk a little bit about

1. Mathematical objects.
2. Reasoning in general.

In Mathematics, we study mathematical objects as follows:

a. We start by specifying a class of mathematical objects (for example, the real numbers, or the integers, or sets).

b. We single out some basic concepts about these objects, that we will want to study (for example, addition and multiplication of real numbers).

c. We state some basic facts about these concepts, that will serve as the starting points of our study. (These basic facts are called “axioms”.)

d. We introduce new concepts (such as “absolute value”, or “prime number”), by defining them (i.e. explaining precisely what they mean).

e. We then prove facts about both the objects we started with and the new ones that we introduced later.

Since definitions and proofs are the main tools we use to introduce concepts and know facts about them, we will have to talk about
4. Definitions.
and
5. Proofs.

Proofs are the most important things we will study in this course. I would say that about 70% of the course is about writing proofs. But writing definitions is also very important, and maybe about 20% of the work in the course will be about them.

2 Mathematical objects

In Mathematics we study mathematical objects, exactly as in zoology we study “zoological objects”, better known as “animals”, and in sociology we study human societies.

One important difference between mathematical objects and the objects of other sciences is that mathematical objects are abstract objects, whereas many (perhaps most of) the objects studied by other sciences are concrete objects. Usually, it not hard to tell which objects are concrete and which ones are abstract, but it is quite difficult to explain this distinction precisely.

Quoting from the Stanford Encyclopedia of Philosophy:

The abstract/concrete distinction has a curious status in contemporary philosophy. It is widely agreed that the distinction is of fundamental importance, And yet there is no standard account of how it should be drawn. There is a great deal of agreement about how to classify certain paradigm cases. Thus it is universally agreed that numbers and the other objects of pure mathematics are abstract (if they exist) whereas rocks and trees and human beings are concrete. Some clear classes of abstracta [this means “abstract objects”, HJS] are classes, propositions, concepts, the letter “A”, and Dante’s Inferno. Some clear classes or concreta [this means “concrete objects”, HJS], are stars, protons, electrons, electromagnetic fields, that chalk token of the letter “A” written on a certain blackboard, and James Joyce’s copy of Dante’s Inferno.

In most other sciences, the primary objects of study are concrete objects, such as animals in zoology. But, in order to study those objects one creates abstract objects such as, in zoology, species, genera (plural of “genus”), families, orders, classes, phyla (plural of “phylum”). Objects such as packs of wolves, or colonies of ants, or teams of baseball players, or the U.S. Senate, or the U.S. Supreme Court, are clearly abstract.
It is not completely obvious what an “abstract object” is, precisely. I would say that “abstract objects” are objects we human beings invent and exist only in our minds, but yet somehow exist (or can be made to exist, by teaching people about them) in everybody’s mind, and we can talk about them, because we have developed a common language that makes communication possible. For example, instead of saying that “in this room there is a person and also a different person and nobody else”, we invent the number “two”, so we can simply say “in this room there are two people”. And the great thing is that when somebody says this, everybody else understands exactly what this means. We are able to communicate about abstract objects such as the number two, because when we say “two” we all mean exactly the same thing.

So the number two exists in our minds; it is not a concrete object, but it exists in the minds of all the people. (Or, more precisely, everybody can learn to talk about the number two and use it in conversation and in writing, with the same meaning as everybody else.)

Fortunately for us, in this course we do not need to worry about how to draw the distinction between concrete and abstract objects, because in Mathematics all the objects we work with are abstract. And we do not need to worry about the philosophical question of what it means, precisely, to be an abstract object. We will just describe the various kinds of mathematical objects that are studied by means of mathematical reasoning, and hope that, as they become more and more familiar to you, you will feel comfortable working with them.

Like the animal world that is studied in zoology, the “world of mathematical objects”, that from now on I will call \textit{WMO}, is populated by a rich and varied collection of things of lots of different kinds.

\section{A first look at \textit{WMO} (the world of mathematical objects): numbers and number systems}

We now take a first look at the mathematical objects that you are probably most familiar with, namely, numbers.

And, in passing, we will have to say a few words about some other things, such as sets, and some concepts such as divisibility.
2.1.1 The most common types of numbers

There are several different kinds of numbers, i.e., several different number systems. It is convenient to give the number systems names, and to introduce mathematical symbols to represent them. Here are some examples:

- \( \mathbb{N} \) is the set of natural numbers,
- \( \mathbb{Z} \) is the set of integers,
- \( \mathbb{Q} \) is the set of rational numbers,
- \( \mathbb{R} \) is the set of real numbers,
- \( \mathbb{C} \) is the set of complex numbers,
- there are sets \( \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_6 \), and, more generally, \( \mathbb{Z}_n \)—the set of integers modulo \( n \)—for every natural number \( n \) such that \( n \geq 2 \). (So, for example, there are the systems \( \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_{10}, \mathbb{Z}_{11}, \mathbb{Z}_{5403} \).)

Some of the above kinds of numbers should be familiar to you, and others may be less so or not at all. Do not worry if you find in our list things that you have never heard of before: we will be coming back to the list later, and discussing all the items in much greater detail.

A number can belong to different number systems, in the same way as, say, a person can belong to different associations. (For example, somebody could be a member, say, of the American Association of University Professors, the Rutgers Alumni Association, and the Sierra Club. Similarly, the number 3 belongs to lots of different number systems, such as, for example, \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \) and \( \mathbb{R} \).)

In this lecture, we will just discuss \( \mathbb{N}, \mathbb{Z}, \) and \( \mathbb{R} \), and we will do so very briefly. We will talk much more about these systems later, and we will also discuss later \( \mathbb{Q}, \mathbb{C}, \) and the \( \mathbb{Z}_n \) systems.

The symbols \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \), are special mathematical symbols. They are not the capital letters \( N, Z, Q, R, C \).

(Why do we use these special symbols? It’s because mathematicians need to use lots of letters in their proofs, so they do not want to take the letters \( C, R \), for example, and declare once and for all that they stand for “the set of all complex numbers” and “the set of all real numbers”.

For example, if they
are working with a circle, they want to have the freedom to call the circle “C”, and to say “let R be the radius of C”, and this would not be allowed if the symbols “C”, “R” already stood for something else. So they invented the special symbols C, R to stand for the set of complex numbers and the set of real numbers, so that the ordinary letters C, R, will be available to be used as variables.)

2.1.2 The natural numbers

The symbol N stands for the set of all natural numbers. (Natural numbers are also called “positive integers”, or—sometimes—”whole numbers”.) The members of this set are the numbers 1, 2, 3 ....

More precisely:

| The **natural numbers** are the numbers obtained from the number 1 by adding 1 any number of times. So, for example, the numbers 1, 1 + 1 (i.e., 2), 1 + 1 + 1 (i.e., 3), 1 + 1 + 1 + 1 (i.e., 4), are natural numbers. And so are the numbers 4, 503, 46, 902, 444, 531, 322 and 10^{10^{10^{10}}}. The symbol N stands for the set of all natural numbers. |

2.1.3 Sets and set membership

We will talk about sets in great detail later, but here are two things you should know right away:

1. Sets have *members*.

2. You can take any objects you want and create a set whose members are those objects. (This is to be contrasted with other ways of creating groups of things. For example, you can take a bunch of wolves and declare them to be a “pack”, but you cannot, say, take a wolf that lives in Yellowstone Park and another wolf that lives in Maine and put them together into a pack. For several wolves to be a pack, they have to live together, run around together, and they all have to follow one “alpha wolf”. Sets, on the other hand, can be formed in any way you like. For example, you can form the set N whose members are the natural numbers. But you could also form a “weird” set, say, a set S whose
members are (1) all the natural numbers, except for the numbers 32 and 1,047, (b) all the U.S. Senators, except those whose names start with the letter “M”, (c) all the planets of the Solar System, including Pluto\(^1\), (d) my aunt Frieda, and (e) Lady Gaga. You may think that there is no reason to put all those things together and form such a strange set. But forming such a set is permitted.

### The symbol “∈”

The symbol “∈” is read as “belongs to”, or “is a member of” (or, sometimes, as “belonging to”). So to say that a number \(n\) is a natural number we can write “\(n \in \mathbb{N}\)”, which we read as “\(n\) belongs to the set of natural numbers” or, even better, as “\(n\) is a natural number”.

More generally, if \(A\) is any set and \(x\) is any object, then “\(x \in A\)” means “\(x\) belongs to \(A\),” or “\(x\) is a member of \(A\).”

Never read “∈” as “is contained in”. The word “contained” has a different meaning, that will be discussed later.

#### 2.1.4 The integers

The symbol \(\mathbb{Z}\) stands for the set of all integers.

The members of \(\mathbb{Z}\) (i.e., the integers) are the natural numbers as well as 0 and the negatives of natural numbers, i.e., the numbers \(-1, -2, -3, \ldots\). So, to say that a number \(n\) is an integer, we can write “\(n \in \mathbb{Z}\)”, which we read as “\(n\) belongs to the set of integers” or, even better, as “\(n\) is an integer”.

Please do not say “\(\mathbb{N}\) is the natural numbers”, or “\(\mathbb{Z}\) is the integers”. When we group things together to create a set, that set is one thing, not many things. So \(\mathbb{N}\) cannot be “the natural numbers”. What you can, and should, say is: “\(\mathbb{N}\) is the set of all natural numbers.”

#### 2.1.5 Negation

To negate a statement is to assert that the statement is false. (Any such statement is called a denial of the statement.)

\(^1\)Or excluding Pluto, if you wish.
So, for example, a denial of “7 is a prime number” is “7 is not a prime number”. (But there are many other ways to write a denial of “7 is a prime number.” For example, we could write “7 is divisible by some natural number other than 1 and 7”, or “7 has more than two factors that are natural numbers.”)

The symbol “∼” (“it’s not true that”)

The symbol “∼”, put in front of a statement, is used to assert that the statement is false. So “∼” stands for “it is not the case that”, or “it is not true that”.

The symbol “∉” (“does not belong to”)

The symbol “∉” stands for “does not belong to” (or, sometimes, “not belonging to”), so, for example, \(x \notin \mathbb{N}\) means exactly the same as “∼ \(x \in \mathbb{N}\)”, and is read as “\(x\) does not belong to \(\mathbb{N}\)”, or “\(x\) is not a member of \(\mathbb{N}\)”, or, even better, as “\(x\) is not a natural number.”

So, for example, the following statements are true:

\[
\begin{align*}
35 & \in \mathbb{N} \\
35 & \in \mathbb{Z} \\
\sim & -35 \in \mathbb{N} \\
-35 & \in \mathbb{Z} \\
35 & \notin \mathbb{Z} \\
0 & \in \mathbb{Z} \\
\sim & 0 \in \mathbb{N} \\
0 & \notin \mathbb{N} \\
0.37 & \notin \mathbb{Z} \\
\pi & \notin \mathbb{Z}
\end{align*}
\]
2.1.6 The real numbers

The symbol \( \mathbb{R} \) stands for the set of all real numbers.

The real numbers are those numbers that you have used in Calculus. They can be positive, negative, or zero.

The positive real numbers have an “integer part”, and then a “decimal expansion” that may terminate after a finite number of steps or may continue forever. (So, for example, the number 4.23 is a real number, and so is the number \( \pi \). The decimal expansion of the number 4.23 terminates after two decimal figures, but the decimal expansion of \( \pi \) goes on forever. Here, for example, is the decimal expansion of \( \pi \) with 30 decimal digits:

\[
3.141592653589793238462643383279
\]

Using Google you can find \( \pi \) with one million digits. As of 2011, 10 trillion digits of \( \pi \) had been computed, and nobody has found any pattern! Even simple questions, such as whether every one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 appears infinitely many times, are unresolved.

And the negative real numbers are the negatives of the positive real numbers. So, for example, \(-4.23\) and \(-\pi\) are negative real numbers.

2.1.7 Positive, negative, nonnegative, and nonpositive numbers

In this course, “positive” means “> 0” (i.e., “greater than zero”), and “nonnegative” means “\( \geq 0 \)” (“greater than or equal to zero”). So, for example, 3 and 0.7 are positive (and nonnegative), and 0 is nonnegative but not positive.

Similarly, “negative” means “< 0”, and “nonpositive” means “\( \leq 0 \)”. So, for example, \(-3\) and \(-0.7\) are negative (and nonpositive), 0 is nonpositive but not negative.

2.1.8 Subsets

A set \( A \) is a subset of a set \( B \) if every member of \( A \) is a member of \( B \). We write \( A \subseteq B \) to indicate that \( A \) is a subset of \( B \).

For example,

a. If \( S \) is the set of all people in the world, and \( T \) is the set of all people who live in the United States, then \( T \) is a subset of \( S \). So the sentence “\( T \subseteq S \)” is true.
b. If $A$ is the set of all animals, and $G$ is the set of all giraffes, then $G$ is a subset of $A$, so the sentence “$G \subseteq A$” is true.

c. Let $S$ be the set of all people who live in the United States, and let $C$ be the set of all U.S. citizens. Is $C$ a subset of $S$? The answer is “no”, because there are U.S. citizens who do not live in the U.S., so these people are members of $C$ but not of $S$, so it’s not true that every member of $C$ belongs to $S$.

And here are some mathematical examples:

I. The following sentences are true:

\[
\begin{align*}
N & \subseteq \mathbb{Z}, \\
N & \subseteq \mathbb{R}, \\
\mathbb{Z} & \subseteq \mathbb{R},
\end{align*}
\]

because every natural number is an integer, every natural number is a real number, and every integer is a real number.

II. And the following sentences are false:

\[
\begin{align*}
\mathbb{Z} & \subseteq \mathbb{N}, \\
\mathbb{R} & \subseteq \mathbb{N}, \\
\mathbb{R} & \subseteq \mathbb{Z}.
\end{align*}
\]

(For example, it is not true that $\mathbb{Z} \subseteq \mathbb{N}$, because not every integer is a natural number since, for example, $0 \in \mathbb{Z}$ but $0 \notin \mathbb{N}$.)

2.1.9 The word “number”, in isolation, is too vague

As we have seen, there are different kinds of numbers. So, if you just say that something is a “number”, without specifying what kind of number it is, then this is too vague. In other words,

Never say that something is a “number”, unless you have made it clear in some way what kind of “number” you are talking about.

For example, suppose you are asked to define “divisible”, and you write:
A number $a$ is divisible by a number $b$ if we can write
\[ a = bc \]
for some number $c$.

This is too vague! What kind of “numbers” are we talking about? Could they be real numbers?. If this was the case, then 3 would be divisible by 5, because $3 = 5 \cdot z$, if we take $z = 3/5$. But we do not want 3 to be divisible by 5. And we want the “numbers: we are talking about to be integers.

So here is a fairly correct (but not yet perfect!) definition of “divisible”:

**Divisibility of integers:** We say that an integer $a$ is divisible by an integer $b$ (or that $a$ is a multiple of $b$, or that $b$ is a factor of $a$, or that $b$ divides $a$), if we can write
\[ a = bc \]
for some integer $c$. □

For example, the following sentences are true:

- 3 divides 6,
- $-3$ divides 6,
- 6 is divisible by 3,
- 6 is a multiple of 3,
- 3 is a factor of 6.

### 2.1.10 Existential statements

In the definition of divisibility given above, we have used the words “we can write”. This language makes it sound as though, in order to decide whether, say, 3 divides 6, we need to have somebody there who “can write” things. This should not be necessary: “3 divides 6” would be a true sentence even if there was nobody around to do any writing. So it is much better to use a more impersonal language:
Divisibility of integers

**DEFINITION.** An integer $a$ is divisible by an integer $b$ (or $a$ is a multiple of $b$, or $b$ is a factor of $a$, or $b$ divides $a$), if there exists an integer $c$ such that

$$a = bc.$$ 

The sentence “there exists an integer $c$ such that $a = bc$” is an example of an existential sentence, i.e., a sentence that asserts that an object of a certain kind exists. Later, when we learn to write mathematics in formal language (that is, using only formulas), we will see that this sentence can be written as follows:

$$(\exists c \in \mathbb{Z})a = bc. \quad (2.1.1)$$

The symbol “$\exists$” is the existential quantifier symbol, and the expression “$(\exists c \in \mathbb{Z})$” is an existential quantifier, and is read as “there exists an integer $c$ such that”.

So Sentence (2.1.1) is read as “there exists an integer $c$ such that $a = bc$”. And it can also be read as “$a = bc$ for some integer $c$”, or “it is possible to pick an integer $c$ such that $a = bc$”. (I recommend the “it is possible to pick ...” reading.)

### 2.2 Other mathematical objects

In addition to numbers, there are all kinds of other mathematical objects. Here is a list of some of them:

- sets,
- finite lists,
- operations,
- functions,
- relations,
arrays of various kinds and, in particular, matrices,

- linear spaces (such as \( \mathbb{R}^2 \), \( \mathbb{R}^3 \), \( \mathbb{R}^4 \), and many others),

- geometric objects of various kinds, such as lines, planes, curves, surfaces,

- algebraic structures, such as groups, rings, fields, algebras, linear spaces, modules, and dozens more,

- metric spaces,

- topological spaces,

- manifolds,

and hundreds of other things.

Some of these kinds of objects will be discussed later in the course, but most of them belong to more advanced courses such as Linear Algebra, Algebra, Topology, or Differential Geometry.

3 Reasoning

Reasoning is what we do every time we have some information and then, by thinking, we arrive at conclusions that were not already part of the information we had to begin with.

Example. In an episode of the TV series *Columbo*, Inspector Columbo is investigating a murder, and he observes that the victim was found in his office, lying on the sofa, with his eyeglasses propped up on his forehead, and that he had been shot by someone who had walked into the room and was about 20 feet away from the door when he/she fired.

From this, the Inspector concludes that the murderer was someone that the victim knew, because if someone he didn’t know had walked into his office, he would have lowered his glasses in order to take a look at the stranger.

The fact that the killer was someone known to the victim was not part of the information that Inspector Columbo had been given. It was a conclusion that he inferred from the given information, by using a mental process called deduction.

And deduction is what reasoning consists of.
As one dictionary puts it: “Reasoning is the process of reaching conclusions by connected thought.”

In other words, reasoning proceeds by formulating *arguments*, i.e., chains of steps each of which is a consequence of the preceding ones. (“We know this; therefore we can conclude that..., and then it follows that ...” and so on.) One starts with some “known facts” (called “prenisses”), and from them one *infers* (i.e., deduces) new facts, and keeps doing this until one reaches a *conclusion*.

### 3.1 Mathematical Reasoning

*Mathematical reasoning* is a special kind of reasoning. It differs from general reasoning in the following two ways:

I. Mathematical reasoning does not start from any observed facts about concrete objects, such as the ones that Columbo used to draw the conclusion that the victim must have known the killer. It proceeds from mathematical statements to mathematical statements, with no “inputs” at all from the real world.

II. In mathematical reasoning, the conclusions follow with absolute certainty. In real life, when we deduce things from other things, all we can say is that the conclusion is very likely to be true if the premisses are true, but one cannot be one hundred percent sure. (For example, in our Columbo story, there could have been a different reason explaining why the victim’s glasses were propped up on his forehead. Maybe the killer had said to the victim “if you touch your glasses I’ll kill you”.)

### 3.2 Proofs

A connected sequence of steps, each one of which follows from the previous ones, is called a **proof**. If the steps of the proof are all mathematical statements, then the proof is a **mathematical proof**. And mathematical proofs are the stuff mathematical reasoning is made of. So a **major part of this course is going to be about how to write mathematical proofs.**
How convincing does a proof have to be?

Proofs are used in many other areas, not just in Mathematics. And the criteria for how convincing a proof varies from area to area. For example, in criminal trials, guilt has to be proved beyond reasonable doubt. And in civil trials the only requirement is the preponderance of evidence, which is much weaker. (This is why O.J. Simpson was acquitted in 1995 of the murder of Nicole Brown Simpson and Ronald Goldman, but in 1997 a civil court awarded a judgement against him for the wrongful deaths of Brown and Goldman. In the criminal trial, the jury felt that the prosecution had failed to prove guilt beyond reasonable doubt, but in the civil trial, under the much less demanding “preponderance of evidence” criterion, Simpson was found guilty.) For mathematical proofs, the criterion for validity is absolute certainty. Not just “beyond reasonable doubt”, but beyond any conceivable doubt, that is, so convincing that no doubt is possible.

3.3 The conclusion of a proof

In a proof, you move from true statement to true statement. And when you get to the end, the last statement in the proof is called the conclusion. The word “conclusion” means two things: (a) the “conclusion” is what comes at the end, and (b) the “conclusion” is something that follows from what was said before.

Examples. If I say “my conclusion from what I have heard you say is that you don’t like me very much”, the word “conclusion” means “something I deduce (or infer) from what you said”.

On the other hand, the last scene of a movie or a play is often called the “conclusion”, meaning just that it is the last scene. □

In a proof, the conclusion is a “conclusion” in both senses: it comes at the end, and it follows logically from everything else.
If $P$ is a proof whose conclusion is Statement $S$, then we say that $P$ is a proof of $S$, or that $P$ proves $S$.

3.4 How can absolute certainty be attained?

Here is how, in Mathematics, we achieve absolute certainty.

First, we construct our proofs so that:

1. Each proof consists of clear, precise, steps.

2. Each step makes a clear, precise statement (except for some steps that just amount to introducing new names for things, or introducing an assumption).

3. Every step either
   
   a. is something that we already know is true,

   or

   b. follows logically from previous steps.

   or

   c. introduces some new notation or assumption.

The key point in the above is “follows logically from previous steps”. This requires a lot of elaboration, and a large part of the course will be devoted to explaining it. The study of how statements “follow logically” from other statements is called Logic, and we will do some Logic in the course, so that by the end of the course you will know what “follows logically” means, and how to work with this notion.

At this point, what you need to know is this: If a statement $Q$ follows logically from other statements $P_1, P_2, \ldots, P_n$, and if $P_1, P_2, \ldots, P_n$ are true, then $Q$ is true.

So, in a proof, we can be sure (if the proof is correct, of course) that every step is true, because if one step—say, Step 46—was not true, then there would be a first step $S$ that is not true, but then all the previous steps must be true, and then Step 46 would also be true, because it follows logically from all the previous steps.
4 An example of a proof: Euclid’s proof that there are infinitely many prime numbers

We will have a lot more to say about proofs throughout the course.

But at this point, rather than go on explaining what a mathematical proof is, I want us to look at specific example of such a proof, so that you will see how a proof works.

Later in the course, we will spend quite a bit of time analyzing in great detail this particular proof and several other proofs, so that you will understand why proofs are written the way they are, and you will know how to write proofs by yourself.

5 What Euclid’s proof is about

You probably know what a “prime number” is. (If you do not know, do not worry; I will explain it to you pretty soon.) Here are the first few prime numbers:

\[ 2, 3, 5, 7, 11, 13, 17, 19 \ldots \]

Does the list of primes stop there? Of course not. It goes on:

\[ 23, 29, 31, 37, 41, 43, 47, 53, 59, 61 \ldots \]

And it doesn’t stop there either. It goes on:

\[ 67, 71, 73, 79, 83, 89, 97, 101, 103 \ldots \]

Does the list go on forever? If you go on computing primes, you would find more and more of them. And mathematicians have actually done this, and found an incredibly large number of primes.

The largest known prime

As of February 5, 2013, the largest known prime was

\[ 2^{57,885,161} - 1. \]

(That is, 2 multiplied by itself 57,885,161 times, minus one.) This is a huge number! It has 17,425,170 decimal digits.
Is it possible that the list of primes stops here, that is, that there are no primes larger than $2^{57,885,161} - 1$?

Before we answer this, just ask yourself: suppose it was indeed true that the list stops with this prime number. How would you know that? If you think about it for a minute, you will see that there is no way to know. You could go on looking at natural numbers larger than $2^{57,885,161} - 1$, and see if among these numbers you find one that is prime. But if you don’t find any it doesn’t mean there aren’t any. It could just be that you haven’t gone far enough in your computation, and if you went farther you would find one.

In fact, no matter how many primes you may compute, you will never know whether the largest prime you have found is indeed the largest prime there is, or there is a larger one.

Can we know in some way, other than by computing lots of primes, whether the list of primes goes on forever or there is a prime number which is the largest one?

It turns out that this question can be answered by means of reasoning. And, amazingly, the answer is “yes, the list of primes goes on forever”! This was discovered, in the year 300 B.C., approximately, by the great Greek mathematician Euclid. Euclid’s 3,000-year old proof is a truly remarkable achievement, the first result of what we would now call “number theory”, one of the most important areas of Mathematics.

5.1 Statement of Euclid’s theorem

I will give you a version that is not exactly Euclid’s, but is based essentially on the same idea.

First, here is Euclid’s result:

THEOREM. The set of prime numbers is infinite.

And now we discuss the proof.

5.2 Preliminaries for Euclid’s proof

Before we present Euclid’s proof, we need to prepare the ground by explaining all the concepts that play a role in it.

In the proof, there appear:
1. infinite sets,
2. finite sets,
3. factors,
4. prime numbers.

So we have to explain what all these things mean.

“Factors” have already been explained in the definition on Page 11. So we now need to explain what a prime number is, and what it means for a set to be finite or infinite.

**DEFINITION 1.** A prime number is a natural number $p$ such that

I. $p > 1$,

II. There do no exist natural numbers $j, k$ such that $j > 1$, $k > 1$, and $p = jk$. □

**DEFINITION 2.** A finite set is a set $S$ for which it is possible to write a list $(s_1, s_2, \ldots, s_n)$, for some natural number $n$, such that all the members of $S$ occur in the list. (This last sentence means: “every member $s$ of $S$ is equal to $p_j$ for some $j$”.) □

**DEFINITION 3.** An infinite set is a set $S$ which is not finite. □

**EXAMPLE 1.** Let $S$ be the set of all people who are or have been U.S. presidents, as of now (i.e., 2015). Then we can write a list $L = (p_1, p_2, p_3, \ldots, p_{44})$ of all the members of $S$, by letting

$$p_j = \text{the } j\text{-th U.S. president}, \quad \text{for } j = 1, 2, \ldots, 44.$$  

(So, for example, $p_1 =$George Washington, $p_2 =$John Adams, and so on, until we get to $p_{44} =$Barack Obama.)

This list contains all the U.S. presidents so far. So $S$ is a finite set. Q.E.D.

**EXAMPLE 2.** The set $\mathbb{N}$ is infinite. **PROOF:** Suppose $\mathbb{N}$ was a finite set. Then we would be able to write a list $L = (a_1, a_2, \ldots, a_n)$, for some $n \in \mathbb{N}$, that would contain all the natural numbers. But, if $L$ is any such list, then the sum $a = a_1 + a_2 + \ldots + a_n$ is a natural number larger than all the $a_j$, $j = 1, 2, \ldots, n.$ So $a$ is not on the list. Hence $L$ is not, after all, a list of all the members of $\mathbb{N}$. So $\mathbb{N}$ is infinite. Q.E.D.
5.3 A theorem on existence of prime factors

In the proof of Euclid's Theorem, we are going to use an important fact, so we present this fact first.

THEOREM. If $a$ is any natural number such that $a > 1$, then $a$ has a prime factor. (That is, there exists a prime number $p$ such that $p$ is a factor of $a$, i.e., equivalently, $p$ divides $a$.)

PROOF. If the number $a$ is prime, then it has a prime factor (because $a = a.1$, so $a$ is a factor of $a$).

If $a$ is not prime, then we can pick smaller natural numbers $j, k$ such that $a = j.k$. Then $j$ is a factor of $a$.

If $j$ is prime, then $j$ is a prime factor of $a$, so $a$ has a prime factor.

If $j$ is not prime, then we can pick smaller natural numbers $j_1, j_2$ such that $j = j_1.j_2$. Then $j_1$ is a factor of $j$ so $j_1$ is a factor of $a$ (because $a = j.k = (j_1.j_2).k = j_1.(j_2.k)$).

If $j_1$ is prime, then $j_1$ is a prime factor of $a$, so $a$ has a prime factor.

If $j_1$ is not prime, then we can pick smaller natural numbers $j_{11}, j_{12}$ such that $j_1 = j_{11}.j_{12}$. Then $j_{11}$ is a factor of $j$ so $j_{11}$ is a factor of $a$ (because $a = j_1.(j_2.k) = (j_{11}.j_{12}).(j_2.k) = j_{11}.(j_{12}.j_2.k)$).

And we can go on until this process stops. And the process can only stop when we get a prime factor of $a$. So $a$ has a prime factor. Q.E.D.

A MORE ELEGANT PROOF. Let $S$ be the set of all natural numbers that are factors of $a$ and are greater than 1.

Then $S$ is a finite set. (Reason: All the members of $S$ are natural numbers between 2 and $a$. If we let $L$ be the list of all natural numbers between 2 and $a$, that is, $L = (2, 3, 4, \ldots, a)$, then $L$ is a finite list. If we delete from this list all the numbers that are not factors of $a$, we are left with a finite list of all the members of $S$. So $S$ is finite.)

Now, every finite set of real numbers has a smallest member. (This is easy to prove, and we will prove it later.) So $S$ has a smallest member. Call this smallest number $s$. Then $s$ is a natural number, $s > 1$, and $s$ is a factor of $a$ (because $s \in S$).

Now we show that $s$ is prime.

Suppose $s$ was not prime. Then we would be able to write $s = u.v$, with $u, v$ natural numbers greater than 1. Then $u < s$ (because $s = u.v$ and $v > 1$). And $u$ is a factor of $a$ (because, if we write $a = s.k$, $k \in \mathbb{N}$, then $a = (u.v).k = u.(v.k)$).
So $u \in S$, and $u < s$. But $s$ was the smallest member of $S$, so “$u \in S$ and $u < s$” is impossible.

So $s$ is prime. And then $s$ is a prime factor of $a$. Q.E.D.

**What does “Q.E.D.” mean?**

“Q.E.D.” stands for the Latin phrase *quod erat demonstrandum*, meaning “which is what was to be proved”. It is used to indicate the end of a proof.

### 5.4 An analogy: twin primes

Before I give you the proof of Euclid’s Theorem, let me tell you about another, very similar problem, for which the situation is completely different.

A pair of twin primes is a pair $(p, q)$ of prime numbers such that $q = p + 2$. So, for example, here are the first few pairs of twin primes:

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103).$$

And we can ask the same question that we asked for primes: does the list go on forever, or does it stop at some largest pair of twin primes?

In other words,

**Are there infinitely many pairs of twin primes?**

This looks very similar to the question whether there are infinitely many primes. And yet, the situation in this case is completely different:

Nobody knows whether there are infinitely many pairs of twin primes. Mathematicians have been trying for more than 2,000 years to solve this problem, by proving that there are infinitely primes, or that that there aren’t, and so far they haven’t been successful.

The twin prime conjecture is the statement that there are infinitely many pairs of twin primes. It was formulated by Euclid, about 2,300 years ago, and it is still an open problem.
5.5 The proof of Euclid’s Theorem

Let $S$ be the set of all prime numbers.

We want to prove that $S$ is an infinite set.

Suppose $S$ is not infinite, so $S$ is a finite set.

Let $L = (p_1, p_2, \ldots, p_n)$ be a list\(^2\) of all the members of $S$.

Let $M = p_1, p_2, \cdots, p_n$. (That is, $M$ is the product of all the entries of the list $L$.)

Let $N = M + 1$.

Then $N$ has a prime factor.

Pick a prime number which is a factor of $N$, and call it $q$.

We will show that the prime number $q$ is not on the list $L$.

Suppose $q$ was one of the entries of the list $L$.

Then we may pick $j$ such that $j \in \mathbb{N}$, $1 \leq j \leq n$, and $q = p_j$.

Then $q$ is a factor of the number $M$, because $p_j$ is a factor of the product $p_1, p_2, \cdots, p_n$.

But $q$ is also a factor of $N$.

So $q$ is a factor of $N - M$, i.e. $q$ is a factor of 1 (because $N - M = 1$).

But $q$ is a prime number, so $q$ cannot be a factor of 1.

The two previous statements contradict each other. So we have derived a contradiction.

Hence the assumption that $q$ is one of the entries of the list $L$ is impossible. So $q$ is not an entry of $L$.

But $q$ is a prime number.

Hence $L$ is not a list of all the primes.

But we have assumed that $L$ is a list of all the primes.

So we have established a contradiction. This contradiction arose from assuming that $S$ is a finite set.

So $S$ is an infinite set.

\[ \text{Q.E.D.} \]

\(^2\)I say “a list” rather than “the list”, because you can list the primes in different ways, for example: in increasing order, or in decreasing order.