1. What is Mathematics?

There is no definitive answer to this question. Indeed, the answer given by a 21st-century mathematician would differ greatly from that given by an 18th-century mathematician or a Renaissance mathematician. However, there are certain unchanging features of mathematics which distinguish it from most other activities.

Mathematics provides the basic language and logical structures which are used to describe and explain the physical world in science and engineering, or the behaviour of options, shares and economies. These objects or structures include, for example, numbers, sets, functions, spaces etc. What distinguishes the objects of mathematics is that they are governed by precise rules or relations. What distinguishes mathematics from the experimental sciences is that the only necessary tools are reason and logic, and that using these we can answer questions definitively and with a certainty that is not available in any other endeavour: The theorem that the angle in a semicircle is always a right angle follows by pure reason from the definitions and basic properties of the mathematical terms (circle, line, angle etc). We know it – because we can prove it – with the kind of certainty that no amount of measurement or experiment could ever give us. We know that it is true in our universe and in every other possible universe.

By proving mathematical statements we achieve certain knowledge and definitive answers to our questions. Even better, a good proof tells us not only that something is certainly true, but explains why it must be true.

2. The rules of logic

When reasoning in mathematics, we use terms such as: and, or, not, implies, (logically) equivalent. It is important to realise that, although these terms coincide with words in everyday language, when using them in logic or mathematics, they are precise technical terms governed by rules for use.

In this section I will use capital letters A, B, C, ..., P, Q to denote statements (mathematical or otherwise) which may be true or false. Such as:

All dogs are animals.

London is the capital of France.

---

1However, there have been some very good and entertaining attempts to answer this question: See What is Mathematics? by Courant and Robbins, or A very short introduction to Mathematics by Tim Gowers.
2 is the only even prime number.

All numbers are rational.

If A and B are statements, then the following are also statements: A and B, A or B, A implies B, A is equivalent to B. Thus the following are statements:

London is the capital of France and all dogs are animals.

2 is the only even prime number implies all numbers are rational.

A statement may be true or false (but not both).

The statement ‘A and B’ is true if and only A is true and B is true.

The statement ‘A or B’ is true if at least one of A and B is true. In particular, if ‘A and B’ is true, then ‘A or B’ is true. In other words, in logic and mathematics, or is ‘inclusive’ rather than ‘exclusive’. For example, the following statements are both true:

All dogs are animals or London is the capital of France.

2 is the only even prime number or all dogs are animals.

2.1. Negation. If A is a statement, we will denote its negation by ‘not-A’, or \( \neg A \). We can also write this as ‘It is not the case that A’. Thus, \( \neg A \) is true if A is false and is false if A is true.

For example, the negation of the statement ‘London is the capital of France’ is the statement ‘It is not the case that London is the capital of France’, or equivalently (and more simply), ‘London is not the capital of France’.

Care needs to be taken in negating statements which contain the word ‘all’.

For example, the negation of the statement ‘All numbers are rational’ is not the statement ‘All numbers are not rational’. (As it happens, both of these statements are simultaneously false. In reality, some numbers are rational and some are not.)

In order to negate the statement ‘All numbers are rational’, we ask ourselves; under what circumstances is this statement false? The correct negation is: ‘Not all numbers are rational’. This is equivalent to the statement: ‘Some numbers are not rational’, or - even better - ‘There is at least one number that is not rational’.

Similarly, the negation of

All even numbers greater than 3 can be expressed as a sum of two primes. (‘Goldbach’s conjecture’)
There is an even number greater than 3 which is not a sum of two primes.

In other words, to prove that Goldbach’s conjecture is false, it would only be necessary to find one large even number which is not a sum of two primes. Such a number, if it existed, would be a counter-example to Goldbach’s conjecture. ( Needless to say, nobody has yet found such a counter-example.)

2.2. Implication. It is important to understand the use of the term implies (the symbol we use for this notion is ‘$\implies$’).

The following all have the same meaning: ‘P implies Q’, ‘$P \implies Q$’, ‘If P then Q’, ‘Q if P’, ‘P only if Q’. In such statements, P is called the hypothesis and Q is called the conclusion.

The fundamental rule for the use of implication in logic or mathematics:

| The statement ‘P implies Q’ is false if P is true and Q is false, and is true otherwise. |

To show that the statement $P \implies Q$ is true we must show that if P is true then Q is also true. In particular, it is possible to know that $P \implies Q$ is true without knowing whether P (or Q) is true.

In practice, when asked to show that $P \implies Q$ is true, we show that Q is true on the assumption that P is true; i.e. we begin by supposing or assuming that P is true, and using this assumption we show that Q must also be true. But we are not claiming that P is true (nor are we claiming that it is false).

2.2.1. An example. For example, consider the following statement:

A: If every even number greater than 3 is a sum of two prime numbers then every number greater than 5 is a sum of three prime numbers.

Then A is the statement $P \implies Q$, where P (the hypothesis) is the statement ‘Every even number greater than 3 is a sum of two prime numbers’ and Q (the conclusion) is the statement ‘Every number greater than 5 is a sum of three prime numbers’.

It is not known whether P is true or false. P is believed by most mathematicians to be true (it is known as Goldbach’s conjecture), but so far no proof has been found. 2

However, it is not difficult to prove the statement A:

**Proof.** We assume – or suppose – that the hypothesis is true; i.e. that every even number greater than 3 is a sum of two primes.

2In fact, in a letter to the mathematician Leonhard Euler in 1742, Goldbach conjectured the statement Q, now referred to as the ‘weak Goldbach conjecture’. In his reply, Euler conjectured the statement P which is now known as Goldbach’s conjecture.
Let $N$ be any number greater than 5.

$N$ is either even or odd.

If $N$ is even, then $N - 2$ is also even, and greater than 3. By our hypothesis $N - 2 = p + q$, for some primes $p$ and $q$. But then $N = 2 + p + q$ is a sum of three primes.

On the other hand, if $N$ is odd, then $N$ is at least 7 and $N - 3$ is an even number greater than 3. By our hypothesis again, $N - 3 = r + s$ for some primes $r$ and $s$, and hence $N = 3 + r + s$.

Either way – i.e. whether $N$ is even or odd – $N$ is the sum of three primes and statement A is proved.

So we know with certainty that the statement ‘$P \implies Q$’ is true, even though we do not yet know whether $P$ is true.\(^3\)

**Exercise 2.1. Is it true that $Q$ implies $P$?**

2.3. **More on implication.** Recall that the statement

$$P \implies Q$$

is false if $P$ is true and $Q$ is false; otherwise, it is true. In particular, if $P$ is false, then the statement ‘$P \implies Q$’ is true, *whether $Q$ is true or false*. For example the statements

If pigs can fly then London is the capital of France.

and

If pigs can fly then London is the capital of England.

are both true.

In logic, a *false* statement implies any statement whatsoever.

2.4. **Truth tables.** A good way for understanding the correct use of logical connectives such as and, or and implies is via truth tables.

We use a truth table to define the conditions under which the statements $P$ and $Q$, $P$ or $Q$, $P \implies Q$ are true, given knowledge of the truth of falsity of the individual statements $P$ and $Q$.

Thus the truth table for $P$ and $Q$ is:

\(^3\)In 1937, the Russian mathematician I. M. Vinogradov proved that every sufficiently large number is a sum of three primes. Finally, in May 2013, the Peruvian mathematician Harald Helfgott found a proof of the weak Goldbach conjecture.
Thus the truth table for \( P \text{ or } Q \) is:

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P or Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Thus the truth table for \( P \text{ implies } Q \) is:

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \implies Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

2.5. **Equivalence of statements.** If \( P \) and \( Q \) are two statements, then the statement \( 'P \implies Q \text{ and } Q \implies P' \) can be written \( 'P \iff Q' \) or \( 'P \text{ if and only if } Q' \).\(^4\)

Thus, if we are asked to show that \( 'P \text{ is equivalent to } Q' \) we must prove both that \( P \implies Q \) and that \( Q \implies P \).

The statement \( 'P \text{ is equivalent to } Q' \) is true if *either* both \( P \) and \( Q \) are true *or* both \( P \) and \( Q \) are false. It is false if one of \( P \) and \( Q \) is true and the other is false.

In mathematical or logical arguments, we can always replace a statement by one which is known to be equivalent to it.

For example, note that for any statement \( A \), \( \neg\neg A \) is equivalent to \( A \).

2.6. **The converse of an implication.** The **converse** of the statement \( 'P \implies Q' \) is the statement \( 'Q \implies P' \). In other words, the converse of an implication is the statement obtained by exchanging the roles of hypothesis and conclusion.

The converse of the statement

\[ \text{If a number is prime then it is an integer.} \]

\(^4\)In fact, \( 'P \implies Q' \) has the same meaning as \( 'P \text{ only if } Q' \), while \( 'Q \implies P' \) means the same as \( 'P \text{ if } Q' \).
is the statement

If a number is an integer then it is prime.

(The first of these statements is true, simply by definition. The second is clearly false: the number 4 is a counterexample.)

In general knowing the truth or falsity of an implication tells us nothing about the truth or falsity of its converse. However, very often when we are considering an implication it is natural to ask what can be said about the truth or falsity of the converse statement.

**Example 2.2.** Let \( ABC \) be a triangle. Pythagoras’s Theorem states

If \( ABC \) is a right angle then

\[
|AB|^2 + |BC|^2 = |AC|^2.
\]

The converse statement, therefore, is:

If

\[
|AB|^2 + |BC|^2 = |AC|^2.
\]

then \( ABC \) is a right angle.

In this particular case, this converse statement can also be proved to be true.

2.7. **The contrapositive.** Given two statements \( P \) and \( Q \), observe that the following statements are equivalent: ‘\( P \implies Q \)’ and ‘\( \neg Q \implies \neg P \)’. Either of these is false if \( P \) is true and \( Q \) is false (i.e. if \( \neg Q \) is true and \( \neg P \) is false), and is true otherwise.

The statement \( \neg Q \implies \neg P \) is called the *contrapositive* of the statement \( P \implies Q \). Since these are equivalent statements, we can always replace an implication by its contrapositive in the course of an argument.

For example, the contrapositive of the statement

If a number is greater than 100 then it is positive

is the statement

If a number is not positive then it is not greater than 100.

These two statements are logically equivalent to each other.

2.8. **‘For all’ and ‘There exists’**. Often a single mathematical statement is best understood as a series of statements, one for each element of a given set.

For instance, the statement ‘The square of an odd number is odd’ can be expressed as follows:

For all integers \( n \), if \( n \) is odd then \( n^2 \) is odd.
Written this way, we see that our original statement can be understood as an infinite list of statements:

\[ \ldots \]

If \(-1\) is odd then \((-1)^2\) is odd
If 0 is odd then 0 squared is odd
If 1 is odd then 1 squared is odd
If 2 is odd then 2 squared is odd

\[ \ldots \]

Each of these statements is an implication (and each is true, as it happens). Using standard mathematical notation, we can write the original statement as follows:

\[ \forall n \in \mathbb{Z}, \ \text{If } n \text{ is odd then } n^2 \text{ is odd}. \]

or

\[ \forall n \in \mathbb{Z}, \ n \text{ is odd } \implies n^2 \text{ is odd}. \]

(The symbol \(\forall\) is read ‘For all’. In logic, it is called the universal quantifier. \(\mathbb{Z}\) is the symbol for the set of all integers.)

What is the negation of this statement? Answer:

It is not (always) the case that the square of an odd integer is odd.

This is equivalent to

There is an odd integer whose square is not odd.

This is an existential statement. (Of course, it is a false statement, but that is not our concern just now.) It asserts the existence of an integer with some specified property. In standard mathematical notation we can express it as follows:

\[ \exists n \in \mathbb{Z}, \ n \text{ is odd and } n^2 \text{ is even}. \]

(The symbol \(\exists\) is read ‘There exists’. In logic, it is called the existential quantifier.)

In general, when we negate a statement with a universal quantifier we obtain a statement with an existential quantifier, and vice versa.

For example, if we negate the statement

\[ \forall n \in \mathbb{Z}, \ n^2 > n \]

we obtain the statement

\[ \exists n \in \mathbb{Z}, \ n^2 \neq n, \]

or, equivalently,

\[ \exists n \in \mathbb{Z}, \ n^2 \leq n. \]
If we negate the statement
\[ \exists x \in \mathbb{R}, \quad x^3 = x + 2 \]
we obtain the statement
\[ \forall x \in \mathbb{R}, \quad x^3 \neq x + 2. \]

Sometimes, we combine several quantifiers in a single statement. In general, the order in which these quantifiers occur matters. Changing the order of the quantifiers may change the meaning (and hence, possibly the truth or falsity) of the statement.

Here are some examples:

The (true) statement *Every positive real number has a square root* can be expressed as

For all positive real numbers \( x \) there is a real number \( y \) whose square is \( x \).

In mathematical notation:
\[
\forall x > 0, \quad \exists y \in \mathbb{R} \text{ with } y^2 = x.
\]

In this statement, it is understood (from the order in which the terms occur) that the \( y \) whose existence is asserted will depend on the given \( x \).

Suppose that we exchange the order of the quantifiers:
\[
\exists y \in \mathbb{R} \text{ (with the property that) } \forall x > 0, \quad y^2 = x.
\]

In everyday language, this latter statement says

There is a real number \( y \) with the property that if \( x \) is any positive number then \( y^2 = x \).

Note that the meaning of the statement is entirely altered. It now asserts that *the same* number \( y \) will be a square root of *any* positive number \( x \). (This is, of course, clearly false.)

The (true, but not obvious) statement

If a prime number divides the product of two integers then it divides one or other of them

can be expressed more precisely with mathematical notation (including quantifiers):
\[
\forall p \text{ prime } (\text{and}) \forall a, b \in \mathbb{Z}, \quad p|ab \implies p|a \text{ or } p|b.
\]
2.8.1. More on contrapositives. Recall that the contrapositive of a statement is a logically equivalent statement. What is the contrapositive of the statement *The square of an odd number is odd.* Recall that this statement can be construed as a series of implications:

\[ \forall n \in \mathbb{Z}, \text{ } n \text{ is odd } \implies n^2 \text{ is odd.} \]

To obtain the contrapositive, in each implication we exchange hypothesis and conclusion and negate both:

\[ \forall n \in \mathbb{Z}, \text{ } n^2 \text{ is not odd } \implies n \text{ is not odd.} \]

Since *not odd* is the same as *even*, this can be written:

\[ \forall n \in \mathbb{Z}, \text{ } n^2 \text{ is even } \implies n \text{ is even.} \]

Thus, in everyday language, the contrapositive of the statement *The square of an odd number is odd* is the statement *If the square of an integer is even then the integer itself is even.* These two statements are entirely logically equivalent.

2.9. Proof by Contradiction. A *contradiction* is a statement of the form ‘P and \(\neg P\)’. Such a statement is necessarily false, since it can never happen that a statement and its negation are both true (or equivalently, it can never happen that a – properly-formed mathematical – statement is simultaneously true and false).

*Proof by contradiction* is a very useful stratagem, or method of proof: In order to prove the truth of a statement, we show that the negation of this statement implies something known to be false (usually a contradiction or ‘absurdity’; this method is also called *reductio ad absurdum*.)

Thus we wish to prove (the truth of statement) P. We begin by supposing \(\neg P\). (Often, to emphasize our purpose, we write ‘Suppose, *for the sake of contradiction*, that \([P \text{ is false or } \neg P \text{ is true}]\).’ We then derive a contradiction or false statement from this supposition. Once we have arrived at this contradiction, we are done, since we are forced to conclude that our original supposition (\(\neg P\)) cannot be true, and therefore P is true after all.

**Example 2.3.** Let’s prove the following:

*For all positive real numbers \(a, b, c\), if \(a = bc\) then either \(b \leq \sqrt{a}\) or \(c \leq \sqrt{a}\).*

**Proof.** Suppose, *for the sake of contradiction*, that the statement is false.

Then there exist \(a, b, c > 0\) satisfying \(a = bc\) but \(b > \sqrt{a}\) and \(c > \sqrt{a}\). It follows that

\[ bc > \sqrt{a} \cdot \sqrt{a} = a. \]

Thus \(bc > a\) and hence \(bc \neq a\). This is a contradiction (since \(a = bc\), and hence the statement is proved. \(\square\)
We will see some less elementary examples of proof by contradiction later.

The English mathematician G.H. Hardy (1877-1947) said the following about proof by contradiction (reductio ad absurdum):

Reductio ad absurdum, which Euclid loved so much, is one of a mathematician’s finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.

3. Examples of Mathematical Reasoning

3.1. Proving the ‘obvious’. In mathematics an ‘obvious’ or ‘clear’ statement is one for which we can provide a short proof, based only on definitions or already known facts. In particular, if a mathematical statement is not simply true from the meaning of the terms (a tautology: eg. ‘Any odd number is not even’) but is clearly true, then we should be able to write a proof of it. Of course, the point of serious mathematics is to discover and prove true but non-obvious statements. But first we should be confident that we can prove the obvious.

Example 3.1. Show that the sum of two even numbers is even.

We can’t begin to address a mathematical question until we know the precise definitions of the terms involved.

What does it mean to be even? First note the concepts even and odd apply only to whole numbers (integers). We cannot ask whether 57/86 or \(\sqrt{2}\) are even. Precisely:

Definition 3.2. An integer is even if it is a multiple of 2; i.e. the integer \(n\) is even if \(n = 2m\) for some integer \(m\).

The definition tells us what is required to prove that a number is even: we must show that it is of the form \(2m\) for some integer \(m\).

So what’s involved in proving that the sum of two even numbers is even?

Suppose that \(n\) and \(m\) are any two even numbers. We are required to show that \(n + m\) is even; i.e. that \(n + m = 2k\) for some integer \(k\).

What do we have to go on?

Nothing other than the fact that \(n\) and \(m\) are even. By definition this means that \(n = 2s\) and \(m = 2t\) for some integers \(s\) and \(t\).

Thus \(n + m = 2s + 2t\): so we must prove that \(2s + 2t = 2k\) for some integer \(k\).
When we spell out what is required in this way, we can’t miss the proof: by the laws of arithmetic

\[ 2s + 2t = 2(s + t) \]

and (the crucial point) each of \( s, t \) is an integer, so that \( s + t \) is also an integer. Thus \( n + m \) is twice an integer, and we have completed the proof.

Having figured all of this out, let’s write it out as a proof:

**Proposition 3.3.** The sum of two even integers is even.

**Proof.** Let \( n \) and \( m \) be any two even integers.

By definition of the term *even*, there are integers \( s \) and \( t \) such that \( n = 2s \) and \( m = 2t \).

Then

\[ n + m = 2s + 2t = 2(s + t). \]

Since each of \( s \) and \( t \) are integers, it follows that \( s + t \) is an integer. Thus, \( n + m \) is twice an integer, and so is even. \( \square \)

**Exercise 3.4.** Let \( d \) be a positive integer. We say that an integer \( n \) is divisible by \( d \) if \( n = ds \) for some integer \( s \). Prove that if two integers are each divisible by \( d \), then so is their sum or difference.

3.1.1. **What are we allowed to assume known?** Have we really *proved* that the sum of two even numbers is even? After all, in the course of the proof, we made statements which we took as known: eg. that if \( s \) and \( t \) are integers, then so is \( s + t \), or that

\[ 2s + 2t = 2(s + t) \]

for any integers \( s \) and \( t \). Since we are in the business (just for now) of proving the obvious, why not prove these statements also?

The answer is that we *could* do so. In order to do so, we would first need to know the definitions of the concepts of integer, addition of integers, multiplication of integers. These, in turn, can be expressed in terms of the more primitive concepts of *set*, *element*, *subset* etc.

But (since our time is finite) this process cannot be continued indefinitely. Whenever we prove some statement, we do so by reducing it, via the rules of logic or reasoning, to more elementary statements which we either (a) have already proved or (b) proceed to prove or (c) are willing to accept as known without proof. At some stage we have to be content to accept the truth of certain (elementary) statements without proof.

For the purpose of this course, we will take as known the basic algebraic properties of the real numbers (\( \mathbb{R} \)). For example:

(1) For all \( a, b \in \mathbb{R}, \ a + b, ab \in \mathbb{R} \)
(2) \(a + b = b + a\) and \(ab = ba\) for all \(a, b \in \mathbb{R}\)

(3) \(a + 0 = a\) for all real numbers \(a\).

(4) \(a \times 1 = a\) for all \(a\)

(5) \((a + b) + c = a + (b + c)\) and \((ab)c = a(bc)\) for all \(a, b, c\)

(6) \(a \cdot (b + c) = ab + ac\) for all \(a, b, c\)

(7) If \(a > b\) and \(b > c\) then \(a > c\) for all \(a, b, c\)

(8) For all \(a, b, c \in \mathbb{R}\), if \(a > b\) then \(a + c > b + c\)

(9) For all \(a, b, c \in \mathbb{R}\), if \(a > 0\) and \(b > c\), then \(ab > ac\).

(10) The principle of induction for positive integers (see below).

We will not assume known any properties of divisibility or prime numbers, but will develop the whole theory from its beginnings (starting in Chapter 1).

For example:

**Definition 3.5.** If \(a, b \in \mathbb{Z}\) we say that \(a\) divides \(b\) (or \(a\) is a divisor of \(b\), or \(a\) is a factor), and write \(a|b\), if there exists some integer \(c\) such that \(b = ac\).

**Remark 3.6.** It is important to note that the content of such a definition or statement is not changed if we use a different choice of letters. The statement ‘\(d|n\) if \(n = dt\) for some integer \(t\)’ has exactly the same meaning.

We will prove the following ‘obvious’ statement:

**Proposition 3.7.** If \(d, m, n \in \mathbb{Z}\) and if \(d|m\) and \(m|n\) then \(d|n\).

**Proof.** Since \(d|m\), we have \(m = ds\) for some integer \(s\).

Since \(m|n\), \(n = mt\) for some integer \(t\).

Therefore, \(n = mt = (ds)t = d(st)\) and thus \(d|n\) (since \(st \in \mathbb{Z}\)). \(\square\)

**Exercise 3.8.** Prove the following ‘obvious’ statement: If \(a, b, c, d\) are all integers and if \(a|b\) and \(c|d\) then \(ac|bd\).

3.2. **Mathematical Discovery.** As already remarked, the point of mathematics is to discover and prove or explain facts which are useful and even surprising but which are not, on the face of it, clear or obvious. However, now logic alone is not enough. To discover something worthwhile and interesting usually requires an idea, or a creative leap. (There are no rules for coming up with ideas, although there are techniques which can help the process.)
**Question 3.9.** The sequence of prime numbers begins

\[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots\]

Does it go on for ever, or is there a greatest prime number?

**Question 3.10.** Are there magnitudes (positive real numbers) which are not rational?

These are two mathematical questions whose answer is certainly not obvious. We cannot discover the answer simply by reflecting on the definitions of the terms. (Of course, we cannot discover the answer, or even address the questions, without first knowing the definitions of the terms.)

Both of these questions were answered by the mathematicians of ancient Greece. The answer to the first (which is known to us from the books of Euclid, ca. 350 BC) is one of the great achievements of that civilization. The answer to the second was a source of great surprise, and even scandal, to the mathematicians and philosophers who followed Pythagoras.

In both cases, the answer involves an idea, a creative act. We cannot answer genuine mathematical questions by simply unravelling definitions or following known procedures.

Let us consider some of the reasoning involved in answering the first question.

Of course, if we start to calculate the primes, the sequence shows no sign of stopping. Sometimes the gap to the next prime can be quite large (find the next prime after 113), but in practice, we eventually find it. Experimenting in this way is likely to lead us to guess that the sequence goes on for ever. But guessing falls far short of answering the question with the certainty that only mathematics allows.

Recall that

**Definition 3.11.** A prime number is an integer greater than 1 which has no divisors other than itself and 1.

Simply contemplating this definition is unlikely to lead us to an answer to our question.

What do we know about prime numbers to begin with?

The main fact we will require is the following: every integer great than 1 has a prime divisor. (This statement is close to being ‘obvious’, but it requires a proof. We’ll prove it below using the principle of induction.)

There are certainly infinitely many integers greater than 1. Does it follow that there are infinitely many primes? Not in any immediate or obvious
way: For example, using only the prime 2, we can make infinitely many integers whose only prime divisor is 2:

\[ 2, 2^2, 2^3, 2^4, 2^5, \ldots \]

To prove that the sequence of prime numbers goes on forever requires a good idea. In this case, the good idea (due to Euclid, or some other unknown mathematician, from around 350BC) was the following: given any finite list \( n_1, n_2, \ldots, n_t \) of integers greater than 1, it is possible to write down an integer greater than 1 which is not divisible by any of the numbers in the list. How is this done? The idea is simple, but very ingenious:

We simply multiply all the numbers together and add 1: i.e. let \( N = n_1 n_2 \cdots n_t + 1 \).

**Proposition 3.12.** \( N \) is not divisible by \( n_1 \) or \( n_2 \) or \( \ldots \) or \( n_t \).

We’ll just prove it for \( n_1 \) (since an identical proof works for all the other numbers in the list.)

(A short proof of this proposition is the following:

\( N \) is equal to a multiple of \( n_1 \) with 1 added on. Therefore \( N \) leaves remainder 1 on division by \( n_1 \), and hence is not divisible by \( n_1 \).

This proof is fine, provided we already know the theory of remainders, which in turn depends on the division algorithm, one of the main results we will meet and use this semester. Because I do not want to assume all of this theory at this stage, we will give a more elementary proof:)

**Proof.** By construction, \( N - 1 = n_1 \cdot (n_2 \cdots n_t) \). So certainly \( N - 1 \) is a multiple of \( n_1 \); i.e. \( n_1 \) divides \( N - 1 \).

Suppose now (for the sake of contradiction) that \( n_1 \) divides \( N \). Then (by Exercise 3.4) \( n_1 \) must divide the difference \( N - (N - 1) = 1 \). But \( n_1 > 1 \), and hence any multiple of \( n_1 \) is greater than 1, so this is a contradiction. Therefore \( n_1 \) cannot divide \( N \) after all.

We can now prove:

**Theorem 3.13 (Euclid).** There are infinitely many distinct prime numbers.

**Proof.** Given any finite list of primes, we can use the construction in the proposition to find a number \( N > 1 \) not divisible by any of the primes in the list. But \( N \) is divisible by some prime. Therefore there is a prime number not in the list.

This shows that no finite list of primes can contain all the primes.
4. The principle of induction

We let \( \mathbb{N} \) denote the set of positive integers (also called the set of natural numbers):

\[
\mathbb{N} := \{1, 2, 3, \ldots, \}.
\]

The principle of induction is the following statement (which tells us how to determine whether a set of natural numbers is equal to all of \( \mathbb{N} \)):

If \( S \) is a subset of \( \mathbb{N} \) with the following properties:

1. \( 1 \in S \)
2. For all \( n \), if \( n \in S \) then \( n + 1 \in S \)

then \( S = \mathbb{N} \).

(We will not prove this statement, but it is intuitively easy to understand: By (1) \( 1 \in S \). By (2) with \( n = 1 \), \( 1 + 1 = 2 \in S \). By (2) again, with \( n = 2 \), we deduce \( 3 \in S \). By (2) with \( n = 3 \) we deduce \( 4 \in S \). Continuing in this way, we can show any natural number belongs to \( S \), and hence \( S = \mathbb{N} \).)

The main application of the principle of induction is to give us the method of proof by induction: Suppose we have a sequence of statements \( P(n) \), one for each natural number \( n \). Then to prove the statement

\( P(n) \) is true for all \( n \) (i.e. \( \forall n \in \mathbb{N}, P(n) \))

it is enough to show

1. \( P(1) \) is true.
2. For any \( n \in \mathbb{N} \), if \( P(n) \) is true then \( P(n + 1) \) is true:
   i.e. \( P(n) \implies P(n + 1) \) for all \( n \in \mathbb{N} \).

(This follows from the principle of induction by taking \( S \) to be the set of natural numbers \( n \) for which \( P(n) \) is true.)

Example 4.1. Prove that

\[
\forall n \in \mathbb{N}, \quad 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.
\]

(Here \( P(n) \) is the statement \( 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \), and we wish to prove the truth of \( P(n) \) for all \( n \).)

Proof. We will prove this by induction on \( n \):

When \( n = 1 \) the statement is that \( 1 = 1 \cdot (1 + 1)/2 = 2/2 \), which is true.
Now suppose that \( P(n) \) is true for some \( n \in \mathbb{N} \) (this is called the \textit{inductive hypothesis}). Then we must prove that \( P(n+1) \) is true.\(^5\)

Now, by our inductive hypothesis,

\[
1 + 2 + \cdots + n = \frac{n(n+1)}{2}.
\]

Adding \( n + 1 \) to both sides gives us:

\[
1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1).
\]

But

\[
\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2}.
\]

Therefore we have shown

\[
1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}
\]

(which is statement \( P(n+1) \)) and we are done. \(\square\)

**Example 4.2.** \textit{Show that} \( 2^n > n \) \textit{for all} \( n \geq 1 \).

\textit{Proof.} We’ll prove thus by induction on \( n \).

When \( n = 1 \) the statement is \( 2^1 > 1 \) which is clearly true.

Suppose the statement is true for some \( n \). So

\[
2^n > n.
\]

Multiplying both sides by 2 we deduce

\[
2 \cdot 2^n = 2^{n+1} > 2n.
\]

But

\[
2n = n + n \geq n + 1 \text{ since } n \geq 1.
\]

Thus \( 2^{n+1} > n + 1 \) as required. \(\square\)

\(^5\)The statement \( P(n+1) \) is obtained by replacing \( n \) by \( n+1 \) everywhere in the statement \( P(n) \).

Thus, the statement \( P(n+1) \) is:

\[
1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.
\]

We must prove this starting from our inductive hypothesis \( P(n) \).
4.1. A variation. We often use the following variation of the principle of induction: Let \( k \) be some fixed integer (negative, 0, or positive). In order to prove that \( P(n) \) is true for all \( n \geq k \) is is enough to prove that

1. \( P(k) \) is true
2. For all \( n \geq k \), \( P(n) \implies P(n + 1) \).

(i.e. we use \( k \) as our starting point, rather than 1; this follows by replacing \( n \) by \( n + k - 1 \) in the original principle of induction).

**Example 4.3.** Prove that \( n! > n^2 \) for all \( n \geq 4 \). (Recall that \( n! := 1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n \).)

**Proof.** We’ll prove this by induction on \( n \geq 4 \).

When \( n = 4 \), the statement is \( 24 = 4! > 4^2 = 16 \), which is true.

Suppose the statement is true for some \( n \geq 4 \). So \( n! > n^2 \).

Multiplying both sides by \( n + 1 \), we get \( (n + 1) \cdot n! = (n + 1)! > (n + 1) \cdot n^2 \).

However, when \( n \geq 4 \), \( n^2 - n - 1 > n^2 - 2n - 1 = (n - 1)^2 - 2 \geq 9 - 2 > 0 \) and hence \( n^2 > n + 1 \).

Thus \( (n + 1)! > (n + 1)n^2 > (n + 1) \cdot (n + 1) = (n + 1)^2 \) as required, and we’re done. \( \square \)

4.2. Another variation: complete induction. Here is another useful variation on the principle of induction:

Suppose that \( Q(n) \) is a sequence of statements, one for each \( n \geq 1 \). In order to prove that \( Q(n) \) is true for all \( n \), we must prove:

1. \( Q(1) \) is true.
2. For any \( n \geq 1 \), if \( Q(1), Q(2), \ldots, Q(n) \) are all true, then \( Q(n + 1) \) is true.

(Note: This follows easily from the original version of proof by induction: Let \( P(n) \) be the statement ‘\( Q(1) \) and \( Q(2) \) and \( \cdots \) and \( Q(n) \)’.)

**Example 4.4.** We’ll use the complete induction to prove the following important

**Theorem 4.5.** Every integer greater than 1 is either a prime number or a product of prime numbers.

**Proof.** We’ll use complete induction. Let \( Q(n) \) be the statement that \( n \) is either prime or a product of primes.

We begin with \( n = 2 \): \( Q(2) \) is true since 2 is a prime.
Suppose now that $Q(2), \ldots, Q(n)$ are all true, for some $n > 1$.

We must prove that $Q(n+1)$ is true: If $n+1$ is prime, then $Q(n+1)$ is true. Otherwise, $n + 1 = rs$ where $r, s$ are integers satisfying $2 \leq r, s \leq n$. Thus, by our inductive hypothesis, $Q(r)$ and $Q(s)$ are both true. Thus $r$ and $s$ are each either prime of a product of primes. It follows that $n + 1 = rs$ is a product of prime numbers, and we are done.

**Remark 4.6.** In fact, we usually express the conclusion of this last Theorem by saying that every integer greater than 1 can be expressed as a product of primes; i.e., we define the phrase product of primes to include the case where the number is a prime number itself.

4.3. **The well-ordering principle for $\mathbb{N}$.** This is the following:

**Theorem 4.7.** Every nonempty set of positive integers has a least element:

If $S \subset \mathbb{N}$ and if $S \neq \emptyset$ then there exists $s \in S$ satisfying $s \leq t$ for all $t \in S$.

Note: Since $S \neq \emptyset$, either $1 \in S$ or $2 \in S$ or $3 \in S$ or ....

**Proof.** We will prove by induction on $n$ the following: If $S$ is a subset of $\mathbb{N}$ containing $n$ then $S$ has a least element.

When $n = 1$, $S$ contains 1 and hence 1 is a least element of $S$.

Suppose that the statement is true for 1, 2, \ldots, $n$. We must prove that it also holds for $n + 1$.

Suppose $n + 1 \in S$. If $S$ contains $k$ for any $k \leq n$, then $S$ has a least element by our inductive hypothesis. Otherwise, $S$ does not contain any $k \leq n$ and $n + 1$ is a least element. Either way, $S$ contains a least element and we are done.

4.4. **Equivalence of Induction and Well-ordering.** We have just used the principle of induction to prove the well-ordering principle. In fact, it is also possible to do everything the other way around: we could have started with the well-ordering principle and deduced the principle of induction:

**Proposition 4.8.** Suppose that $\mathbb{N}$ satisfies the well-ordering principle. Then the principle of induction holds.

**Proof.** We suppose that $S \subset \mathbb{N}$ satisfies

1. $1 \in S$
2. For all $n \in \mathbb{N}$, $n \in S \implies n + 1 \in S$. 

---

The content appears to be a mathematical proof involving the well-ordering principle and the principle of induction, with specific focus on proving properties of prime numbers and the expression of integers as products of primes.
We must prove that $S = \mathbb{N}$:

Let $T = \mathbb{N} \setminus S$.\(^6\) Thus, we wish to prove that $T = \emptyset$.

Suppose, for the sake of contradiction that $T \neq \emptyset$. By the well-ordering principle, $T$ has a least element, $m$ say. Now $1 \in S \implies 1 \notin T \implies m \neq 1$. So $m > 1$. Let $n = m - 1$. Since $m$ is a least element of $T$, $n \notin T$. Thus $n \in S$. But then, by our assumption about $S$, $n + 1 = m \in S$, and hence $m \notin T$. This is a contradiction, proving the proposition. \(\square\)

To conclude: We have shown each of the principle of induction and the well-ordering principle imply each other: they are logically equivalent statements.

---

\(^6\)This means that $T$ consists of all those natural numbers which do not belong to set $S$. We say that $T$ is the complement of $S$. We’ll learn more about the language of sets later in the course.