Theorems and proofs

Formally, a *theorem* is a statement that can be shown to be true (the Fundamental Theorem of Calculus).

That is to say, it is a statement that can be deduced using rules of inference from a finite collection of statements which are assumed to be true and are called *axioms*.

Usually the name "theorem" is reserved for important statements. A less important statement is often called a *proposition*.

A *lemma* (plural: *lemmata*) is usually an auxiliary statement which is needed to deduce a more important statement. Some lemmata, however become more important than theorems they were originally supposed to help proving.

We demonstrate that a theorem is true with a *proof*. A proof is a valid argument that establishes the truth of a theorem.

Most theorems can be formulated as conditional statements depending on several variables and using nested quantifiers.

Definition

Let m and n be integers. We say that n *divides* m if there is an integer k such that $m = kn$. If n divides m we write $n \mid m$. If n does not divide m we write $n \nmid m$. If n divides m we also say that m is *divisible by* n.

Example

$3 \mid 6$ and $3 \mid 9$ because $6 = 2 \cdot 3$ and $9 = 3 \cdot 3$, but $3 \nmid 5$.

Definition

We say that an integer n is even if it is divisible by 2 and is odd otherwise.

Observations

- No integer can be odd and even at the same time
- Every integer is either odd or even
- An integer m is even if and only if $m = 2k$ for some integer k.

Theorem

If n is an even integer then so is n^2.

Formally, the domain is integers, $E(n)$ is "n is even". When our theorem is $\forall n, E(n) \to E(n^2)$.

Proof.

Suppose that n is even. Then $n = 2k$ for some integer k. Then we have

$$\begin{aligned} n^2 &= (2k)^2 \\ &= (2k) \cdot (2k) \\ &= 2(k \cdot 2k) \\ &= 2l \end{aligned}$$

where $l = k \cdot 2k = 2k^2$ is an integer. Thus, $2 \mid n^2$ and so n^2 is even. $\square$

We end a proof with the symbol $\square$ which is a shortcut for Q.E.D (*quod erat demonstrandum*, meaning "which is what had to be shown").

This is an example of a *direct proof*: we assumed $E(n)$ to be true, for an arbitrary n in the domain, and deduced from that that $E(n^2)$ is true. An important point here is that n has to be *arbitrary*.

Example

Let n be an integer. Prove that if $3n+2$ is odd then n is odd.

Proof.

Suppose that n is even. Then $n = 2k$ for some k and we can write

$$\begin{aligned} 3n+2 &= 3\cdot 2k + 2 \\ &= 2(3k+1). \end{aligned}$$

Thus, if n is even then $3n+2$ is even. So, we proved the contrapositive of the original statement. $\square$

This is an example of a proof *by contrapositive*: instead of our original statement we prove its contrapositive.

Another approach.

Suppose that $3n+2$ odd but n is even.
Then $n = 2k$ and so $3n+2 = 3(2k)+2 = 2(3k+1)$ is even.
Thus, $3n+2$ is even and odd at the same time which is a contradiction.
This means that our assumption that n is even while $3n+2$ was odd was false.
Therefore, if $3n+2$ is odd then n is also odd. $\square$

This is an example of a proof *by contradiction*.
The idea is to find a true statement r such that $\neg p \to \neg r$ is true.
Since $\neg p \to \neg r \equiv r \to p$ we can use *modus ponens* to deduce p from $r \to p$ and r.
Needless to say, to use this method we need to find the negation of the original statement.
In our case, the original statement was $\forall n, O(3n+2) \to O(n)$ where $O(n)$ means "n is odd" and the domain is "all integers". Its negation is, by De Morgan's law, $\exists n, \neg(O(3n+2) \to O(n)) \equiv \exists n, (O(3n+2) \wedge \neg O(n))$. We saw that this statement implies $O(3n+2) \wedge \neg O(3n+2)$.

Proving equivalences

Theorem

An integer n is odd if and only if there exists an integer k such that $n = 2k + 1$.

There are two statements here.

$\Longrightarrow$: if n is odd then there exists an integer k such that $n = 2k + 1$

$\Longleftarrow$: if $n = 2k + 1$ for some integer k then n is odd.

Proof

$\Longleftarrow$: Suppose that $n = 2k + 1$ and n is even. Then $n = 2m$ for some integer m and so $2k + 1 = n = 2m$. Then $1 = 2(m - k)$ which means that 2 divides 1 which is false. So, our assumption that n was even was false. Thus, n is odd.

Proof (cont.)

$\Longrightarrow$: Suppose that n is odd. First, assume that $n > 0$. Let $k \geq 0$ be the maximal integer such that $2k \leq n$. Maximal means here that if $l > k$ then $2l \not\leq n$ that is $2l > n$.
Such an integer exists because there are finitely many integers $r \geq 0$ such that $2r \leq n$.
We cannot have $2k = n$ since n is odd; so $2k < n$. By maximality of k, $2(k+1) > n$. Thus, $2k < n < 2k+2$. Since n is an integer it follows that $n = 2k+1$.
Assume now that $n \leq 0$. Since n is odd, $n < 0$. Then $-n > 0$. By the above, $-n = 2l+1$ for some integer l. Then $n = -2l-1 = -2l+1-2 = 2(-l-1)+1$. Thus, $n = 2m+1$ for some integer m. $\square$

Theorem

Let n be an integer. Then n is even if and only if n^2 is even.

Proof.

We already proved that if n is even then so is n^2.
To prove the converse (n^2 is even implies that n is even) we use the contrapositive. That is, we prove that if n is odd then n^2 is odd.
Suppose that n is odd. Then $n = 2k + 1$ for some integer k and so

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= (2k+1)(2k+1) \\ &= (2k)(2k) + 2k + 2k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2l + 1 \end{aligned}$$

where $l = 2k^2 + 2k$ is an integer. Thus, n^2 is odd. $\square$

The worst mistake in a proof: assuming, directly or indirectly, the statement that we are trying to prove. Such an argument is called *circular*. Sometimes they are very hard to recognize.
For example, consider the following argument. Suppose that $3n+2$ is odd. Let $n = 2k+1$ for some integer k. Then
$3(2k+1)+2 = 6k+5$ is odd and we are done.

Paradoxes

Example

Let us prove that $2 = 1$.
Let $a = b$
Then $a^2 = ab$
Then $a^2 - b^2 = ab - b^2$
Then $(a - b)(a + b) = b(a - b)$
Then $a + b = b$
Then $2b = b$
Thus, $2 = 1$

The problem is that we cannot cancel $a - b$ since it is zero (so, for example, $(a - b)2 = 0 = (a - b)3$, but it says nothing about the equality between 2 and 3 because any number multiplied by zero is zero).

Recursion and mathematical induction

We often need to consider *sequences* defined *recursively*, that is, the next member of a sequence is obtained from one or more preceding members.

Example

- $a_n = qa_{n-1} + d$, $n \geq 1$.
  If $q = 1$ then our sequence is called an *arithmetic sequence*. Thus, $a_1 = a_0 + d$, $a_2 = a_1 + d = a_0 + 2d$, $a_3 = a_2 + d = a_0 + 3d$ and so on.
  For example, if $a_0 = 0$ and $d = 1$, we obtain $a_0 = 0$, $a_1 = 1$, $a_2 = 2$, $\ldots$, $a_n = n$, $\ldots$
  If $d = 0$ then our sequence is called a *geometric sequence*. Thus, $a_1 = qa_0$, $a_2 = qa_1 = q^2a_0$, $a_3 = qa_2 = q^3a_0$ etc.
  For example, if $q = 2$ and $a_0 = 1$ then $a_1 = 2a_0 = 2$, $a_2 = 4$, $a_3 = 8$, $\ldots$, $a_n = 2^n$, $\ldots$
  If $a_0 = 0$, $d = 1$ and $q = 2$ we get $a_1 = 1$, $a_2 = 2a_1 + 1 = 3$, $a_3 = 2a_2 + 1 = 7$, $a_4 = 2a_3 + 1 = 15$, $\ldots$. Later we will see that $a_n = 2^n - 1$.

Example

- More generally, we can consider recursions in which the next term in a sequence depends on more than one of preceding terms.
  For example, the famous *Fibonacci sequence* is defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$, that is $F_2 = F_1 + F_0 = 1$, $F_3 = F_2 + F_1 = 2$, $F_4 = F_3 + F_2 = 3$, $F_5 = F_4 + F_3 = 5$, $F_6 = F_5 + F_4 = 8$ etc.
- If $a_0, a_1, a_2, \ldots$ is a sequence, we can make another sequence out of it: $s_0 = a_0$, $s_1 = a_0 + a_1$, $s_2 = a_0 + a_1 + a_2$, $\ldots$, $s_n = a_0 + \cdots + a_n$.
  For example, if $a_n = n$, we have $s_0 = 0$, $s_1 = 1$, $s_2 = 1 + 2 = 3$, $s_3 = 1 + 2 + 3 = 6$, $s_4 = 1 + 2 + 3 + 4 = 10$ etc.
  This is also a recursive sequence, as $s_n = s_{n-1} + a_n$.

Question

Given a sequence a_n, $n \geq 0$, find a formula for its generic term (that is, a formula which allows us to compute a_n without computing all preceding terms).

Question

If a formula is hard to find, establish properties of the sequence *without* finding a formula for its generic term. For example, determine how fast its terms grow.

Example

- If $a_n = qa_{n-1} + d$ then
$$a_n = q^n a_0 + d(1 + q + \cdots + q^{n-1})$$
If $q \neq 1$ we can also write this as follows
$$a_n = q^n a_0 + d\,\frac{q^n - 1}{q - 1}.$$
- The sequence $s_n = 1 + \cdots + n = s_{n-1} + n$, $n \geq 1$, $s_0 = 0$. Then
$$s_n = \sum_{i=1}^{n} i = \tfrac{1}{2} n(n+1).$$

It is easy to check that these formulae are correct for small values of n, but how do we know they are *always* correct?
For that we introduce a proof technique called *mathematical induction*.
It is based on an important property of non-negative integers: if n is a non-negative integer then so is $n+1$.
So, if we want to prove $\forall n P(n)$ where the domain for n is "all non-negative integers" and P is any predicate, we can do it as follows:

Weak Mathematical induction

- Prove $P(0)$ (this is called the *base of induction*)
- Prove $\forall n(P(n) \to P(n+1))$ (this is called *the inductive step*)

The assumption that $P(n)$ is true is often called "the induction hypothesis".

- Since $P(n) \to P(n+1)$ is automatically true if $P(n)$ is false, the only thing we need to prove is that if $P(n)$ is true then so is $P(n+1)$.
- We can use induction to prove that $P(n)$ holds for all $n \geq m$. In that case we replace the induction base by proving that $P(m)$ is true
- We can also use induction to prove that $P(n)$ holds for all integers n between a and b

Example

Prove that the nth term of an arithmetic sequence $a_n = a_{n-1} + d$, $n \geq 1$ is equal to $a_0 + nd$.

Proof.

$P(n)$ is "$a_n = a_0 + nd$". In particular, $P(0)$ is automatically true.
Suppose that $P(n)$ is true for some $n \geq 0$. Then

$$\begin{aligned} a_{n+1} &= a_n + d \\ &= (a_0 + nd) + d \\ &= a_0 + (n+1)d, \end{aligned}$$

that is, $P(n+1)$ is true. The inductive step is proved. □

Example

Prove that the nth term of the geometric sequence $a_n = qa_{n-1}$, $n \geq 1$ is $a_0 q^n$.

Proof.

$P(n)$ is "$a_n = a_0 q^n$". Again, $P(0)$ is automatically true.
Suppose that $P(n)$ is true for some $n \geq 0$. Then

$$\begin{aligned} a_{n+1} &= a_n q \\ &= a_0 q^n q \\ &= a_0 q^{n+1}, \end{aligned}$$

which shows that $P(n+1)$ is true and proves the inductive step. □

Example

Let $a_n = qa_{n-1} + d$, $n \geq 1$. Prove that

$$a_n = q^n a_0 + [n]_q d,$$

where

$$[n]_q = 1 + q + \cdots + q^{n-1} = \begin{cases} \frac{q^n-1}{q-1}, & q \neq 1 \\ n, & q = 1. \end{cases}$$

The induction base ($n = 0$) is easy: $q^0 a_0 + [0]_q d = a_0$ as it should.
For the inductive step, we have

$$\begin{aligned} a_{n+1} &= qa_n + d \\ &= q(q^n a_0 + [n]_q d) + d \\ &= q^{n+1} a_0 + d(q[n]_q + 1) \end{aligned}$$

So, it remains to show that $q[n]_q + 1 = [n+1]_q$.

If we use the definition $[n]_q = 1 + q + \cdots + q^{n-1}$ then this is clear

$$\begin{aligned} q[n]_q + 1 &= q(1 + q + \cdots + q^{n-1}) + 1 \\ &= 1 + q + q^2 + \cdots + q^n = [n+1]_q. \end{aligned}$$

But we also want to show that the other definition works too (this, in particular, implies that both expressions for $[n]_q$ are equal). For $q = 1$ this is clear: $1 \cdot n + 1 = n + 1$. If $q \neq 1$ then

$$\begin{aligned} q[n]_q + 1 &= q\,\frac{q^n - 1}{q - 1} + 1 \\ &= \frac{q(q^n - 1) + q - 1}{q - 1} \\ &= \frac{q^{n+1} - q + q - 1}{q - 1} \\ &= \frac{q^{n+1} - 1}{q - 1} \\ &= [n+1]_q. \end{aligned}$$

So, assuming that $a_n = q^n a_0 + [n]_q d$, we established that $a_{n+1} = q^{n+1} a_0 + [n+1]_q d$. This proves the inductive step and completes the proof. □

As an example, if $a_0 = 0$, $q = 2$ and $d = 1$ (that is, $a_n = 2a_{n-1} + 1$, $n \geq 1$, and $a_0 = 0$) we obtain $a_n = 2^n - 1$.

Example

Let $a_n = a_{n-1} + d$, $n \geq 1$ be an arithmetic sequence. Prove that

$$a_0 + \cdots + a_n = (n+1)a_0 + \tfrac{1}{2}dn(n+1).$$

In particular,

$$1 + \cdots + n = \tfrac{1}{2}n(n+1).$$

Note that the second formula indeed follows from the first one: take $a_0 = 0$ and $d = 1$.

Note the following nice consequence:

$$1 + 3 + \cdots + (2n + 1) = (n + 1)^2$$

Indeed, this is an arithmetic sequence with $a_0 = 1$ and $d = 2$. So, $a_0 + \cdots + a_n = (n + 1) + 2 \cdot \frac{1}{2} n(n + 1) = (n + 1) + n(n + 1) = (n + 1)^2$.

Exercise

Find

$$1 + 4 + 7 + \cdots + (3n + 1)$$

and

$$1 + 6 + 11 + \cdots + (5n + 1).$$

Example

Consider the sequence $f_n = f_{n-1}^2 + 3f_{n-1} + 2$, $n \geq 1$, and $f_0 = 1$.
So, $f_1 = 1^2 + 3 + 2 = 6$, $f_2 = 6^2 + 3 \cdot 6 + 2 = 56$, $f_3 = 3\,306$,
$f_4 = 10\,939\,556$, $f_5 = 11\,967\,391\,829\,580$
This sequence grows very quickly. The question is, how quickly does it grow?
Let us compare it with another fast growing sequence:
$1, 4, 16, 256, 65\,536, 4\,294\,967\,296, \ldots, 2^{2^n}, \ldots$
We claim that $f_n > 2^{2^n}$ for all $n \geq 1$.

To work with 2-step recursions (such as in *Fibonacci sequence*) and other similar questions we need

Strong induction principle

We are proving $\forall n P(n)$.

- Induction base: we prove that $P(n)$ holds for all $1 \leq n \leq m$ for some m (usually rather small).
- Induction step: Prove $\forall n((\forall(k < n)P(k)) \to P(n)$. That is, assuming that $P(k)$ is true for all $k < n$ we prove that $P(n)$ is true.

Example

We claim that $\left(\frac{3}{2}\right)^{n-2} < F_n < 2^{n-2}$, $n \geq 4$.