Methods of Proof

Lecture 3: Sep 9
Now we have learnt the basics in logic.

We are going to apply the logical rules in proving mathematical theorems.

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases
Basic Definitions

An integer \( n \) is an **even** number if there exists an integer \( k \) such that \( n = 2k \).

An integer \( n \) is an **odd** number if there exists an integer \( k \) such that \( n = 2k + 1 \).
Proving an Implication

**Goal:** If $P$, then $Q$.  ($P$ implies $Q$)

**Method 1:** Write assume $P$, then show that $Q$ logically follows.

The sum of two even numbers is even.

**Proof**  
$x = 2m, \ y = 2n$  
$x+y = 2m+2n$  
$= 2(m+n)$
Direct Proofs

The product of two odd numbers is odd.

Proof
\[ x = 2m+1, \ y = 2n+1 \]
\[ xy = (2m+1)(2n+1) \]
\[ = 4mn + 2m + 2n + 1 \]
\[ = 2(2mn+m+n) + 1. \]

If \( m \) and \( n \) are perfect square, then \( m+n+2\sqrt{mn} \) is a perfect square.

Proof
\[ m = a^2 \text{ and } n = b^2 \text{ for some integers } a \text{ and } b \]
Then \[ m + n + 2\sqrt{mn} = a^2 + b^2 + 2ab \]
\[ = (a + b)^2 \]
So \( m + n + 2\sqrt{mn} \) is a perfect square.
This Lecture

• Direct proof
• Contrapositive
• Proof by contradiction
• Proof by cases
Proving an Implication

**Goal:** If P, then Q. (P implies Q)

**Method 1:** Write assume P, then show that Q logically follows.

Claim: If r is irrational, then √r is irrational.

How to begin with?

What if I prove “If √r is rational, then r is rational”, is it equivalent?

Yes, this is equivalent, because it is the *contrapositive* of the statement, so proving “if P, then Q” is equivalent to proving “if not Q, then not P”.

Yes, this is equivalent, because it is the *contrapositive* of the statement, so proving “if P, then Q” is equivalent to proving “if not Q, then not P”.
Rational Number

R is rational ⇔ there are integers a and b such that

\[
\frac{a}{b} \quad \text{and } b \neq 0.
\]

Is 0.281 a rational number? Yes, 281/1000

Is 0 a rational number? Yes, 0/1

If m and n are non-zero integers, is \((m+n)/mn\) a rational number? Yes

Is the sum of two rational numbers a rational number? Yes, \(a/b+c/d=(ad+bc)/bd\)

Is \(x=0.12121212\ldots\) a rational number? Note that \(100x-x=12\), and so \(x=12/99\).
Proving the Contrapositive

Goal: If P, then Q. (P implies Q)

Method 2: Prove the contrapositive, i.e. prove “not Q implies not P”.

Claim: If r is irrational, then √r is irrational.

Proof:

We shall prove the contrapositive - "if √r is rational, then r is rational."

Since √r is rational, √r = a/b for some integers a,b.

So r = a²/b². Since a,b are integers, a²,b² are integers.

Therefore, r is rational. Q.E.D.

(Q.E.D.) “which was to be demonstrated”, or “quite easily done”. 😊
Proving an “if and only if”

**Goal:** Prove that two statements P and Q are “logically equivalent”, that is, one holds if and only if the other holds.

**Example:** For an integer n, n is even if and only if \( n^2 \) is even.

**Method 1a:** Prove P implies Q and Q implies P.

**Method 1b:** Prove P implies Q and not P implies not Q.

**Method 2:** Construct a chain of if and only if statement.
For an integer $n$, $n$ is even if and only if $n^2$ is even.

Method 1a: Prove $P$ implies $Q$ and $Q$ implies $P$.

**Statement:** If $n$ is even, then $n^2$ is even

**Proof:** $n = 2k$

$n^2 = 4k^2$

**Statement:** If $n^2$ is even, then $n$ is even

**Proof:** $n^2 = 2k$

$n = \sqrt{2k}$

??
Proof the Contrapositive

For an integer \( n \), \( n \) is even if and only if \( n^2 \) is even.

Method 1b: Prove \( P \) implies \( Q \) and not \( P \) implies not \( Q \).

Statement: If \( n^2 \) is even, then \( n \) is even

Contrapositive: If \( n \) is odd, then \( n^2 \) is odd.

Proof (the contrapositive):

Since \( n \) is an odd number, \( n = 2k+1 \) for some integer \( k \).

So \( n^2 = (2k+1)^2 \)

\[ = (2k)^2 + 2(2k) + 1 = 2(2k^2 + 2k) + 1 \]

So \( n^2 \) is an odd number.
This Lecture

• Direct proof

• Contrapositive

• Proof by contradiction

• Proof by cases
Proof by Contradiction

\[ \overline{P} \rightarrow F \]
\[ P \]

To prove \( P \), you prove that not \( P \) would lead to ridiculous result, and so \( P \) must be true.
Proof by Contradiction

\textbf{Theorem:} $\sqrt{2}$ is irrational.

Proof (by contradiction):

- Suppose $\sqrt{2}$ was rational.
- Choose $m$, $n$ integers without common prime factors (always possible) such that $\sqrt{2} = \frac{m}{n}$
- Show that $m$ and $n$ are both even, thus having a common factor 2, a contradiction!
**Proof by Contradiction**

*Theorem:* \( \sqrt{2} \) is irrational.

Proof (by contradiction): Want to prove both \( m \) and \( n \) are even.

\[
\sqrt{2} = \frac{m}{n}
\]

\[
\sqrt{2}n = m
\]

\[
2n^2 = m^2
\]

so \( m \) is even.

so can assume \( m = 2l \)

\[
m^2 = 4l^2
\]

\[
2n^2 = 4l^2
\]

\[
n^2 = 2l^2
\]

so \( n \) is even.

Recall that \( m \) is even if and only if \( m^2 \) is even.
Infinitude of the Primes

**Theorem.** There are infinitely many prime numbers.

**Proof (by contradiction):**

Assume there are only finitely many primes.

Let $p_1, p_2, \ldots, p_N$ be all the primes.

1. We will construct a number $N$ so that $N$ is not divisible by any $p_i$.

   By our assumption, it means that $N$ is not divisible by any prime number.

2. On the other hand, we show that any number must be divided by *some* prime.

   It leads to a contradiction, and therefore the assumption must be false.

So there must be infinitely many primes.
Divisibility by a Prime

**Theorem.** Any integer \( n > 1 \) is divisible by a prime number.

- Let \( n \) be an integer.
- If \( n \) is a prime number, then we are done.
- Otherwise, \( n = ab \), both are smaller than \( n \).
- If \( a \) or \( b \) is a prime number, then we are done.
- Otherwise, \( a = cd \), both are smaller than \( a \).
- If \( c \) or \( d \) is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we have found a prime factor of \( n \).

**Idea of induction.**
Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Let $p_1, p_2, \ldots, p_N$ be all the primes.

Consider $p_1p_2\ldots p_N + 1$.

Claim: if $p$ divides $a$, then $p$ does not divide $a+1$.

Proof (by contradiction):

$a = cp$ for some integer $c$
$a+1 = dp$ for some integer $d$

$\Rightarrow 1 = (d-c)p$, contradiction because $p \geq 2$.

So, by the claim, none of $p_1, p_2, \ldots, p_N$ can divide $p_1p_2\ldots p_N + 1$, a contradiction.
This Lecture

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases
Proof by Cases

\( p \lor q \)
\( p \rightarrow r \)
\( q \rightarrow r \)
\( \therefore r \)

e.g. want to prove a nonzero number always has a positive square.

x is positive or x is negative

if x is positive, then \( x^2 > 0 \).

if x is negative, then \( x^2 > 0 \).

\( \therefore x^2 > 0. \)
The Square of an Odd Integer

\[ \forall \text{ odd } n, \exists m, n^2 = 8m + 1? \]

Idea 0: find counterexample.

\[ 3^2 = 9 = 8+1, \quad 5^2 = 25 = 3\times8+1 \quad \ldots \quad 131^2 = 17161 = 2145\times8 + 1, \ldots \ldots \]

Idea 1: prove that \( n^2 - 1 \) is divisible by 8.

\[ n^2 - 1 = (n-1)(n+1) = ??... \]

Idea 2: consider \((2k+1)^2\)

\[ (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1 \]

If \( k \) is even, then both \( k^2 \) and \( k \) are even, and so we are done.

If \( k \) is odd, then both \( k^2 \) and \( k \) are odd, and so \( k^2+k \) even, also done.
Rational vs Irrational

**Question:** If $a$ and $b$ are irrational, can $a^b$ be rational??

We (only) know that $\sqrt{2}$ is irrational, what about $\sqrt{2}^{\sqrt{2}}$?

**Case 1:** $\sqrt{2}^{\sqrt{2}}$ is rational

Then we are done, $a=\sqrt{2}$, $b=\sqrt{2}$.

**Case 2:** $\sqrt{2}^{\sqrt{2}}$ is irrational

Then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, a rational number

So $a=\sqrt{2}^{\sqrt{2}}$, $b=\sqrt{2}$ will do.

So in either case there are $a, b$ irrational and $a^b$ be rational.

We don’t (need to) know which case is true!
Summary

We have learnt different techniques to prove mathematical statements.

- Direct proof
- Contrapositive
- Proof by contradiction
- Proof by cases

Next time we will focus on a very important technique, proof by induction.