The Foundations: Logic and Proofs

Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.

- Ingredients:
  - hypotheses of the theorem
  - axioms assumed to be true
  - previously proven theorems
  - rules of inference

You get: truth of the statement being proved

Usefulness

- Computer Science
  - Verifying that computer programs are correct.
  - Establishing that operating systems are secure.
  - Making inferences in artificial intelligence.
  - Showing that system specifications are consistent.

- Mathematics
  - Defining Formalism.
  - Providing specification in a common language.
  - Justification for the results.

Definitions

1. An integer n is even if, and only if, n = 2k for some integer k.
2. An integer n is odd if, and only if, n = 2k + 1 for some integer k.
3. An integer n is prime if, and only if, n > 1 and for all positive integers r and s, if n = r·s, then r = 1 or s = 1.
4. An integer n > 1 is composite if, and only if, n = r·s for some positive integers r and s with r ≠ 1 and s ≠ 1.
5. A real number r is rational if, and only if, r= $\frac{a}{b}$ for some integers a and b with b ≠ 0.
6. If n and d are integers and d ≠ 0, then d divides n, written d|n if, and only if, n = d.k for some integers k.
7. An integer n is called a perfect square if, and only if, n = k^2 for some integer k.

Types of Proofs

- **Proving conditional Statements**
  - Direct Proofs
  - Indirect Proofs
    - **Proof by Contraposition**
    - **Proofs by Contradiction**
- **Proving Non-conditional Statements**
  - Indirect Proofs
  - If-And-Only-If Proof
  - Constructive Versus Non-constructive Proofs
  - Existence Proofs; Existence and Uniqueness Proofs
  - Disproofs (Counterexample, Contradiction, Existence Statement)
  - Proofs Involving Sets
- **Mathematical Induction**

Direct Proofs

- p →q
  - first step is the assumption that *p is true*
  - subsequent steps constructed using rules of inference.
  - final step showing that *q must also be true*

showing that if *p is true,*
then q must also be true,
so that the combination
p true and q false never occurs

Outline for Direct Proof

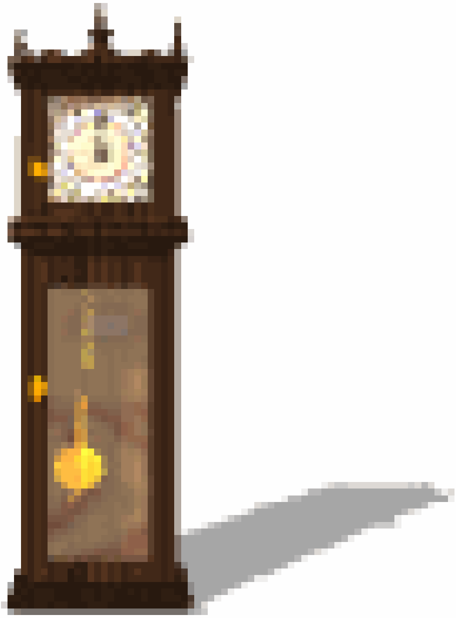
Proposition If P, then Q.

Proof. Suppose P.

$\vdots$

Therefore Q. ■

Activity Time



Prove that the sum of two odd integers is even.

Prove that the sum of two odd integers is even.

Let **m** and **n** be two odd integers. Then by definition of odd numbers

$m = 2k + 1 \quad$ for some $k \in \mathbb{Z}$

$n = 2l + 1 \quad$ for some $l \in \mathbb{Z}$

$$
\begin{aligned}
\text{Now } m + n &= (2k + 1) + (2l + 1) \\
&= 2k + 2l + 2 \\
&= 2\,(k + l + 1) \\
&= 2r \qquad \text{where } r = (k + l + 1) \in \mathbb{Z}
\end{aligned}
$$

Hence $m + n$ is even.

EXERCISE:

Prove that if n is any even integer, then $(-1)^n = 1$

SOLUTION:

Suppose n is an even integer. Then n = 2k for some integer k.

Now

$$(-1)^n = (-1)^{2k}$$
$$= [(-1)^2]^k$$
$$= (1)^k$$
$$= 1 \qquad \text{(proved)}$$

EXERCISE:

Prove that the product of an even integer and an odd integer is even.

SOLUTION:

Suppose m is an even integer and n is an odd integer. Then

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$\begin{aligned} m \cdot n &= 2k \cdot (2l + 1) \\ &= 2 \cdot k\,(2l + 1) \\ &= 2 \cdot r \qquad \text{where } r = k(2l + 1) \text{ is an integer} \end{aligned}$$

Hence $m \cdot n$ is even. (Proved)

EXERCISE:

Prove that the square of an even integer is even.

SOLUTION:

Suppose n is an even integer. Then $n = 2k$

Now

$$\begin{aligned}\text{square of } n = n^2 &= (2 \cdot k)^2 \\ &= 4k^2 \\ &= 2 \cdot (2k^2) \\ &= 2 \cdot p \quad \text{where } p = 2k^2 \in Z\end{aligned}$$

Hence, n^2 is even. (proved)

proved that if *n is an odd integer, then n^2 is an odd integer*

- We assume that the hypothesis of this conditional statement is true, namely, we assume that *n is odd*.
- By the definition of an odd integer, it follows that $n = 2k + 1$, *where k is some integer.*
- *Square both sides* $n^2 = (2k + 1)^2$
  - $4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$
- Consequently, we have proved that if *n is an odd integer, then n^2 is an odd integer*

EXERCISE:

Prove that if n is an odd integer, then $n^3 + n$ is even.

SOLUTION:

Let n be an odd integer, then $n = 2k + 1$ for some $k \in Z$

Now $n^3 + n = n(n^2 + 1)$

$= (2k + 1)((2k+1)^2 + 1)$

$= (2k + 1)(4k^2 + 4k + 1 + 1)$

$= (2k + 1)(4k^2 + 4k + 2)$

$= (2k + 1)\, 2.\, (2k^2 + 2k + 1)$

$= 2\cdot(2k + 1)(2k^2 + 2k + 1)$ $\qquad k \in Z$

= an even integer

Proposition If x is an even integer, then x^2-6x+5 is odd.

Proof. Suppose x is an even integer.

Then $x=2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2-6x+5=(2a)^2-6(2a)+5=4a^2-12a+5=4a^2-12a+4+1=2(2a^2-6a+2)+1$.

Therefore we have $x^2-6x+5=2b+1$, where $b=2a^2-6a+2 \in \mathbb{Z}$.

Consequently x^2-6x+5 is odd, by definition of an odd number.

EXERCISE:

Prove that, if the sum of any two integers is even, then so is their difference.

SOLUTION:

Suppose m and n are integers so that $m + n$ is even. Then by definition of even numbers

$$m + n = 2k \qquad \text{for some integer } k$$

$$\Rightarrow \quad m = 2k - n \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Now $m - n = (2k - n) - n$ using (1)

$= 2k - 2n$

$= 2(k - n) = 2r$ where $r = k - n$ is an integer

Hence $m - n$ is even.

EXERCISE:

Prove that the sum of any two rational numbers is rational.

SOLUTION:

Suppose r and s are rational numbers.

Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

Now

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad + bc}{bd} \\ &= \frac{p}{q} \end{aligned}$$

where $p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE:

Given any two distinct rational numbers r and s with r < s. Prove that there is a rational number x such that r < x < s.

SOLUTION:

Given two distinct rational numbers r and s such that

$r < s$ ……………………(1)

Adding r to both sides of (1), we get

$$r + r < r + s$$

$$2r < r + s$$

$\Rightarrow$

$$r < \frac{r+s}{2} \qquad \text{.........................(2)}$$

Next adding s to both sides of (1), we get

$$r + s < s + s$$

$\Rightarrow$ $r + s < 2s$

$\Rightarrow$ $$\frac{r+s}{2} < s \qquad \text{...............................(3)}$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \quad \text{..........................(4)}$$

Since the sum of two rationals is rational, therefore $r + s$ is rational. Also the quotient of a rational by a non-zero rational, is rational, therefore $\frac{r+s}{2}$ is rational and by (4) it lies between r & s.
Hence, we have found a rational number
such that $r < x < s$. (proved)

EXERCISE:

Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

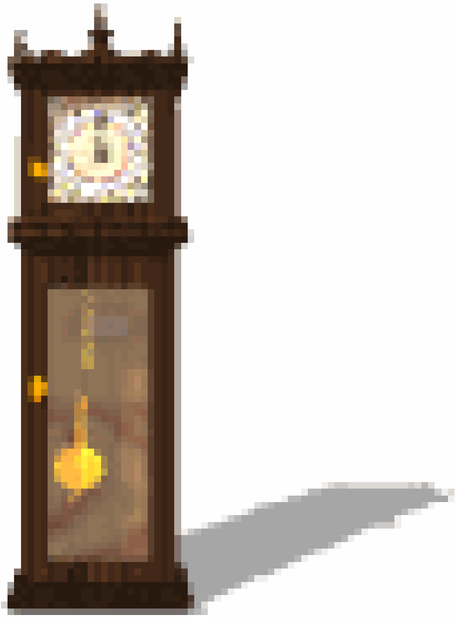
Let n, n + 1 and n + 2 be three consecutive integers.

Now

$$\begin{aligned} n + (n + 1) + (n + 2) &= 3n + 3 \\ &= 3(n + 1) \\ &= 3 \cdot k \quad \text{where } k=(n+1) \in Z \end{aligned}$$

Hence, the sum of three consecutive integers is divisible by 3.

Activity Time

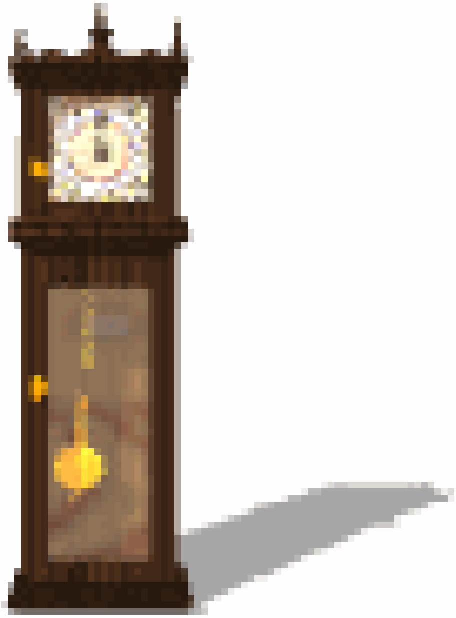


Give a direct proof that if *m and n are both perfect squares, then nm is also a perfect square.*

Proof

- We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
- By the definition of a perfect square, It follows that there are integers s and t such that $m = s^2$ and $n = t^2$.
- Multiplying both m and n to get s^2t^2.
- Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.
- By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.
- We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Activity Time



Give a direct proof that if *n is an integer and n is odd, then 3n + 2 is odd.*

Indirect Proofs

- Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.
- Attempts at direct proofs often reach dead ends
- Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

$\vdots$

Therefore $\sim P$. ■

Prove that if *n is an integer and 3n + 2 is odd, then n is odd.*

PROOF:

The contrapositive of the given conditional statement is

"if n is even then 3n + 2 is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence 3n + 2 is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2\cdot(2k^2 + 2k) + 1$

$= 2\cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore $n^2 = n.n$ is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5. Then by definition of divisibility

$$n = 5 \cdot k \qquad \text{for some integer } k$$

Squaring both sides

$$n^2 = 25 \cdot k^2 \qquad \text{where } k^2 \in Z$$

n^2 is divisible by 25

Proofs by Contradiction

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved is true.

Basic Idea

- Assume that the statement we want to prove is *false, and then show* that this assumption leads to nonsense!

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

$\vdots$

Therefore $C \wedge \sim C$. ■

We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

THEOREM:

There is no greatest integer.

PROOF:

Suppose there is a greatest integer N. Then $n \leq N$ for every integer n.

Let $M = N + 1$

Now M is an integer since it is a sum of integers.

Also $M > N$ since $M = N + 1$

Thus M is an integer that is greater than the greatest integer, which is a contradiction. Hence our supposition is not true and so there is no greatest integer.

EXERCISE:

Give a proof by contradiction for the statement:

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

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence $n = 2k + 1$ for some integer k.

Now $n^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1$

$= 2\cdot(2k^2 + 2k) + 1$

$= 2r + 1$ where $r = (2k^2 + 2k) \in Z$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

THEOREM:

The sum of any rational number and any irrational number is irrational.

PROOF:

We suppose that the negation of the statement is true. That is, we suppose that there is a rational number r and an irrational number s such that r + s is rational. By definition of ration

$$r = \frac{a}{b} \quad \ldots\ldots\ldots\ldots\ldots(1) \qquad \text{and} \qquad r + s = \frac{c}{d} \quad \ldots\ldots\ldots\ldots\ldots(2)$$

for some integers a, b, c and d with $b \neq 0$ and $d \neq 0$.

Using (1) in (2), we get

$$\frac{a}{b} + s = \frac{c}{d}$$

$$\Rightarrow \qquad s = \frac{c}{d} - \frac{a}{b}$$

$$s = \frac{bc - ad}{bd} \qquad (bd \neq 0)$$

Now bc - ad and bd are both integers, since products and difference of integers are integers. Hence s is a quotient of two integers bc-ad and bd with $bd \neq 0$. So by definition of rational, s is rational.

This contradicts the supposition that s is irrational. Hence the supposition is false and the theorem is true.

EXERCISE:

Prove that $\sqrt{2}$ is irrational.

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

$$\sqrt{2} = \frac{m}{n}$$

that

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

Or $\quad m^2 = 2n^2 \quad$ ....(1)

This implies that m^2 is even (by definition of even). It follows that m is even. Hence

$m = 2k \quad$ for some integer k $\quad$ (2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$

$$\Rightarrow \quad 4k^2 = 2n^2$$

$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

PROOF BY COUNTER EXAMPLE

Disprove the statement by giving a counter example.
For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

SOLUTION:

Suppose $a = -5$ and $b = -2$
then clearly $-5 < -2$

But $a^2 = (-5)^2 = 25$ and $b^2 = (-2)^2 = 4$

But $25 > 4$

This disproves the given statement.

EXERCISE:

Prove or give counter example to disprove the statement.

For all integers n, $n^2 - n + 11$ is a prime number.

SOLUTION:

The statement is not true

For $n = 11$

we have , $n^2 - n + 11 = (11)^2 - 11 + 11$

$$= (11)^2$$

$$= (11)(11)$$

$$= 121$$

which is obviously not a prime number.