Proving Theorems

Example proofs

- If n is odd (even) then n^2 is odd (even)
- If n^2 is odd (even) then n is odd (even)
- If $3n+2$ is odd then n is odd
- If n is an integer not divisible by 3 then $n^2 \equiv 1 \pmod 3$
- The integer n is odd if and only if n^2 is odd
- prove that $\sqrt{2}$ is irrational.
- The sum of any two even integers is even

Proving Theorems

prove:

$$p \rightarrow q$$

Ex:

prove "If n is odd then n^2 is odd"

- Trivial proof
  when q is true
  anything $\rightarrow$ T
- Vacuous proof
  when p is false
  false $\rightarrow$ anything

Prove: $p \rightarrow q$

- Direct proof

proof: Assume p is true

show that q must be true

$\therefore q$

- Indirect proof

$p \rightarrow q \iff \underbrace{\neg q \rightarrow \neg p}_{\text{Contrapositive}}$

prove $\neg q \rightarrow \neg p$

proof Assume $\neg q$ (q is false)

show that it must be $\neg p$
(p is false)

$\therefore \neg p$

– Proof by Contradiction

prove P

proof: assume $\neg P$ (P is false)

show that $\neg P \rightarrow \underset{\perp}{\underset{\equiv}{C}}$

Contradiction

$\therefore P$ (P is true)

remember the contradiction rule

$$\boxed{\begin{array}{l} P \rightarrow C \\ \therefore \neg P \end{array}}$$

Ex: $\sqrt{2}$ is irrational

- proof by Contradiction

prove $p \to q$

proof: assume $(p \to q)$ is false

p is true and q is false

$p \wedge \neg q$

$\therefore \neg q$

show that it must be $\neg p$
(p is false)

$\therefore \neg p$

Contradiction (assumption is wrong)

$\therefore p \to q$

– proof by cases (direct proof)

prove $p \rightarrow q$

proof:

$$p \Leftrightarrow p_1 \vee p_2 \vee \dots p_n$$

assume p

$\therefore\ p_1 \vee p_2 \vee \dots \vee p_n$

$$\left.\begin{array}{l} p_1 \rightarrow q \\ p_2 \rightarrow q \\ \vdots \\ p_n \rightarrow q \end{array}\right\} \text{show that at all cases } q \text{ must be true.}$$

$\therefore\ p \rightarrow q$

prove theorem in the form

$$p \longleftrightarrow q$$

p if and only if q
iff

proof:

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

prove $p \rightarrow q$

prove $q \rightarrow p$

$\therefore \; p \leftrightarrow q$

prove

$$P_1 \leftrightarrow P_2 \leftrightarrow P_3 \leftrightarrow \cdots \leftrightarrow P_n$$

proof:

$$[P_1 \leftrightarrow P_2 \leftrightarrow P_3 \leftrightarrow \cdots \leftrightarrow P_n] \leftrightarrow$$
$$[(P_1 \rightarrow P_2) \wedge (P_2 \rightarrow P_3) \wedge \cdots \wedge (P_n \rightarrow P_1)]$$

prove $P_1 \rightarrow P_2$

prove $P_2 \rightarrow P_3$

$\vdots$

prove $P_n \rightarrow P_1$

$\therefore \; P_1 \leftrightarrow P_2 \leftrightarrow \cdots \leftrightarrow P_n$

Proving Existential statements.

prove $\exists x \; P(x)$

Constructive proof of Existance

Non Constructive proof of existance

find an element a such that $P(a)$ is true

$P(a)$

$\therefore \exists x \; P(x)$

- ∃ an even integer n that can be written in two ways as a sum of two prime numbers

proof: Let $n = 10$

$10 = 5+5$

$10 = 7+3$

- Suppose that r & s are integers prove that ∃ an integer K such that

$22r + 18s = 2K$

Show that there are n consecutive composite positive integers for every positive integer n.

prove

$\forall n \; \exists x \; (x+i$ is composite for $i = 1, 2, \ldots, n)$

proof: (Euclid)

(use constructive proof of existance)

let $x = (n+1)! + 1$

Consider the integers

$x+1, x+2, \ldots, x+n$

$x+i = (n+1)! + (i+1)$ for $i = 1, 2, \ldots, n$

$x+i$ is composite since $(i+1)$ divedes $x+i$

Non constructive proof of existance

two ways : prove $\exists x \; P(x)$

a) show that the existance of a value of x that makes $P(x)$ true is guaranteed by axioms or theorems

b) by contradiction

assume $\exists x \; P(x)$ is false

(assume $\neg \exists x \; P(x)$)

$\neg \exists x \; P(x) \Leftrightarrow \forall x \; \neg P(x)$

prove $\forall x \; \neg P(x)$

(prove that for all x $P(x)$ is false)

show that for every positive integer n
there is a prime greater than n.

prove:

$\forall n \; \exists x \quad P(x)$

where $P(x)$ is "x is prime and x is greater than n"

and the universe of discourse is positive integer

proof: (sketch)

Consider the integer $n!+1$

since every integer has a prime factor

$\therefore$ there is at least one prime K dividing $n!+1$

show that K must be greater than n

Proving Universal statements

prove $\forall x \; P(x)$

$\forall x \; P(x) \to q(x)$

a) Exhaustion

check all possible x

b) Generalization from a generic particular

suppose x is a particular but arbitrarily chosen

c) by Contradiction

assume $\neg \forall x \; P(x)$

$\leftrightarrow \exists x \; \neg P(x)$

$\downarrow$ Contradiction.

prove

$\forall$ integers, if n is even and $4 \leq n \leq 30$ then n can be written as a sum of two prime numbers

proof: by exhaustion.

$4 = 2+2$

$6 = 3+3$

$8 = 3+5$

$10 = 5+5$

$12 = 5+7$

$14 = 7+7 = 11+3$

$16 = \cancel{7+9} = 11+5$

$18 = \cancel{9+11}\ 11+7$

$20 = 13+7$

$22 = 17+5$

$24 = 19+5$

$26 = 7+19$

$28 = 11+17$

$30 = 11+19$.

Theorem

The sum of any two even integers is even

proof:

Let m and n be (particular but arbitrarily chosen) even integers.

By definition

$m = 2r$ and

$n = 2s$

for some integer r, s

$\therefore m+n = 2r + 2s$
$= 2(r+s)$

Let $k = r + s$

k is integer (sum of two integers)

$\therefore m+n = 2k$

$\rightarrow m+n$ is even.

q.e.d.

Disprove by Counter example

prove that $\forall x \; P(x)$ is false

$\Leftrightarrow$ prove that $\neg \forall x \; P(x)$ is true

$\Leftrightarrow \exists x \; \neg P(x)$

proving existential statement

find a such that $P(a)$ is false

a is called counter example.

Ex.

show that the assertion

"All primes are odd" is false

Ex

Is $n^2 - n + 41$ prime for all nonnegative integers n.

Theorem

Every integer is a rational number

proof . . . .

Theorem

The sum of any two rational numbers is a rational number