§ Proof Techniques

Direct and indirect proofs

$p \to q$ direct $\forall x\ P(x) \to Q(x)$

$\neg q \to \neg p$ indirect / Proof by contraposition

Proposition: $\forall\, n \in \mathbb{Z}$, n is odd $\Leftrightarrow$ $3n+5$ is even.

<u>Proof</u>: "$\Rightarrow$" $\quad n = 2k+1$

$$3n+5 = 3\times(2k+1)+5$$
$$= 6k+8 = 2(3k+4)$$

"$\Leftarrow$" $\quad n$ is not odd. n is even.

$$n = 2k$$
$$3n+5 = 3\times 2k+5 = 6k+5$$
$$= 2(3k+2)+1$$

Existence Proofs

$\exists x \; P(x)$

$\forall x \, \exists y \; P(x, y)$

constructive

non-constructive

Theorem: $\exists$ irrational numbers x, y such that x^y is rational.

Proof $z = \sqrt{2}^{\sqrt{2}}$ If z is rational, we are done

Otherwise, $z^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$

Theorem: For all positive integers n, there exists a positive integer x such that

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

are all composite.

<u>Proof</u> [Constructive]

$$x = (n+1)! + 2$$

$$x+1 = (n+1)! + 3$$

$$x+2 = (n+1)! + 4$$

$$\overline{}$$

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

Theorem: $\forall$ positive integer n, there exists a prime $> n$

Proof [non-constructive]

$n! + 1$ not divisible by any prime $\leq n$.

Any prime divisor of $n!+1$ must be $> n$.

Proof by cases

$$p_1 \vee p_2 \vee \cdots \vee p_k \to q$$

$$p_1 \to q,\ p_2 \to q,\ \ldots,\ p_k \to q$$

Theorem: $\forall$ positive integer $n > 1$, $4^n + n^4$ is composite.

Proof: Case 1: n is even

$4^n + n^4 > 2$ and is a multiple of 2.

Case 2: n is odd

$$4^n + n^4 = (2^n + n^2)^2 - 2^{n+1} n^2$$

$$= (2^n + n^2 + 2^{(n+1)/2} n)(2^n + n^2 - 2^{(n+1)/2} n)$$

Proof by contradiction

p , $p \to q$ $\qquad$ p is true

q is false

Arrive at a contradiction (like $r \wedge \neg r$)

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

<u>Proof</u>: Assume that $\sqrt{2}$ is rational.

$$\sqrt{2} = \frac{a}{b}$$

$$c = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

$$c^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$$

$$\underset{\text{odd}}{2b^2} = \underset{\text{even}}{a^2}$$

Cycle of implications

Example: For any two integers (positive) a and b, the following conditions are equivalent

(1) a is a divisor of b

(2) $\gcd(a, b) = a$

(3) $\lfloor b/a \rfloor = b/a$

$(1) \Rightarrow (2)$ a is a divisor of b

a is a divisor of a

a is a common divisor of a and b.

a is the greatest common divisor of a and b.

$(2) \Rightarrow (3)$ $\quad \gcd(a, b) = a$

a is a divisor of b

$b = ka$ for some integer k

$\frac{b}{a} = k$ is an integer

$\lfloor b/a \rfloor = \frac{b}{a} = k$

$(3) \Rightarrow (1)$ $\quad k = \lfloor b/a \rfloor = \frac{b}{a}$

$\hookrightarrow$ an integer

$b = ak \Rightarrow$ a is a divisor of b

$(1), (2), (3), (4)$

$1 \to 2 \to 3 \to 4 \to 1$

$1 \to 3 \to 2 \to 4 \to 1$

$1 \to 2 \to 3 \to 1$

$2 \to 4$

$4 \to 3$

proof by disjunction

$$p \to q \vee r$$

$$\equiv \neg p \vee q \vee r$$

$$\equiv (\neg p \vee q) \vee r$$

$$\equiv \neg (p \wedge \neg q) \vee r$$

$$\equiv p \wedge \neg q \to r$$

Theorem: Let p be a prime, and a, b be integers. If p divides ab, then p divides either a or b.

Proof: p divides ab

p does not divide a

$$\gcd(a, p) = 1 = ua + vp \quad \text{for some } u, v \in \mathbb{Z}$$

$$b = u\underbrace{ab}_{\substack{\text{divisible}\\ \text{by } p}} + v p b$$

b is a multiple of p.

Disproofs

$\forall x\, P(x)$ – it suffices to find out an x for which $P(x)$ is false (counterexample)

$\exists x\, P(x)$ – $\forall x [\neg P(x)]$

(counterexamples do not work)

Theorem: $\forall a, b \in \mathbb{R}$, $a^2 < b^2 \Rightarrow a < b$

Proof: $a = 2$, $b = -3$

$a^2 < b^2$ but $a \not< b$.

Exercise: $L_1, L_2, \ldots, L_n$ lamps 0 off
1 on

```
for (i=1; i<=n; ++i) L_i = 0;

for (i=1; i<=n; ++i)
    for (j=i; j<=n; j+=i)
        L_j = 1 - L_j ;
```

After this, which lamps are on? Why?