

Griffith University  
**3515ICT Theory of Computation**  
**Some sample proofs**

## Proof types

1. Proof by construction
2. Proof by equivalence
3. Proof by contradiction
4. Proof by case analysis
5. Proof by induction
6. Proof by diagonalisation
7. **Proof by some other method**

## Sample proof by construction

Call a graph *k-regular* if every node in the graph has degree  $k$ .

**Theorem.** *For every even number  $n > 2$ , there exists a 3-regular graph with  $n$  nodes.*

*Proof.* Let  $n$  be an even number greater than 2. Construct a graph  $G = (V, E)$  with  $n$  nodes as follows. Let  $V = \{0, 1, \dots, n - 1\}$ . Let  $E$  be the union of the sets  $\{(i, i + 1) \mid 0 \leq i < n - 1\}$ ,  $\{(n - 1, 0)\}$  and  $\{(i, i + n/2) \mid 0 \leq i < n/2\}$ .

Clearly, every node has an edge to its predecessor and successor on a cycle of length  $n$  and to the opposite node on the cycle. That is, every node has degree 3.  $\square$

## Sample proof by equivalence

**Theorem.** *For all numbers  $a$  and  $b$ ,*  
 $a^2 - b^2 = (a - b)(a + b)$ .

*Proof.*

$$(a - b)(a + b) = a^2 + ab - ab - b^2 = a^2 - b^2. \quad \square$$

OK, that's a bit trivial, but you get the idea.

## Sample proof by contradiction

**Theorem.** (Euclid) *There exist infinitely many prime numbers.*

*Proof.* Suppose there exist only finitely many prime numbers. Let  $p_1, p_2, \dots, p_n$  be *all* the prime numbers. Compute

$$N = p_1 \times p_2 \times \cdots \times p_n + 1.$$

As every number is the product of prime factors,  $N$  must have a prime factor  $p$ . But  $p$  cannot be one of the  $p_i$  ( $1 \leq i \leq n$ ), as each of these has remainder 1 when divided into  $N$ . Therefore  $p_1, \dots, p_n$  are not all the prime numbers, which is a contradiction. Therefore, there are infinitely many prime numbers.  $\square$

## Another proof by contradiction

**Theorem.** (Antiquity. Euclid?)  $\sqrt{2}$  is irrational.

*Proof.* Suppose  $\sqrt{2}$  is rational. Then  $\sqrt{2} = p/q$ , for some integers  $p$  and  $q \neq 0$ . Suppose, without loss of generality that  $p$  and  $q$  have no common factors. In particular,  $p$  and  $q$  are not both even. By squaring both sides,  $2q^2 = p^2$ . Therefore 2 divides  $p$ , so  $p$  is even and  $p = 2r$  for some integer  $r$ . Hence,  $2q^2 = 4r^2$ , or  $q^2 = 2r^2$ .

Therefore 2 divides  $q$ , so  $q$ , as well as  $p$ , is even. But this contradicts the fact that  $p$  and  $q$  are **not** both even. Hence,  $\sqrt{2}$  is irrational.  $\square$ .

## Sample proof by case analysis

**Theorem.** For every integer  $N \geq 0$ ,  $N(N^2 + 5)$  is divisible by 6.

*Proof.* Every integer  $N$  is congruent to 0,  $\pm 1$ ,  $\pm 2$  or 3 modulo 6. Consider each case in turn.

1. Suppose  $N \equiv 0 \pmod{6}$ . Then  $N(N^2 + 5) \equiv 0 \pmod{6}$ .
2. Suppose  $N \equiv \pm 1 \pmod{6}$ . Then  $N^2 \equiv 1 \pmod{6}$ , so  $N^2 + 5 \equiv 0 \pmod{6}$  and  $N(N^2 + 5) \equiv 0 \pmod{6}$ .
3. Suppose  $N \equiv \pm 2 \pmod{6}$ . Then  $N^2 \equiv 4 \pmod{6}$ , so  $N^2 + 5 \equiv 3 \pmod{6}$ . Thus,  $N(N^2 + 5) \equiv 0 \pmod{6}$ .
4. Suppose  $N \equiv 3 \pmod{6}$ . Then  $N^2 \equiv 3 \pmod{6}$ , so  $N^2 + 5 \equiv 2 \pmod{6}$ . Thus,  $N(N^2 + 5) \equiv 0 \pmod{6}$ .

That is, in every case,  $N(N^2 + 5) \equiv 0 \pmod{6}$ .

## Sample proof by mathematical induction

For  $n \geq 0$ , let  $F_n = 2^{2^n} + 1$ .

**Theorem.** For all  $n \geq 0$ ,  $F_n = \prod_{k=0}^{n-1} F_k + 2$ .

*Proof.* Basis.  $F_0 = 2^{2^0} + 1 = 3 = \prod_{k=0}^{0-1} F_k + 2$ .

Induction step. Suppose  $F_n = \prod_{k=0}^{n-1} F_k + 2$ . Then

$$\begin{aligned} \prod_{k=0}^n F_k + 2 &= F_n \prod_{k=0}^{n-1} F_k + 2 \\ &= F_n (F_n - 2) + 2 \text{ (ind. hyp.)} \\ &= (2^{2^n} + 1)(2^{2^n} - 1) + 1 \\ &= ((2^{2^n})^2 - 1) + 1 \\ &= 2^{2^{n+1}} + 1 \\ &= F_{n+1} \end{aligned}$$

□

## Sample proof by structural induction

A *full  $k$ -ary tree* is a  $k$ -ary tree in which every node has either 0 or  $k$  children.

**Theorem.** Let  $n$  be the number of nodes and  $l$  the number of leaves in a full  $k$ -ary tree. Then  $n = (kl - 1)/(k - 1)$ .

*Proof.* Basis. Suppose  $n = l = 1$ . Then

$1 = (k \cdot 1 - 1)/(k - 1) = 1$ . Induction step.

Suppose tree  $T$  has  $n > 1$  nodes. Then  $T$  has a root and  $k$  subtrees. Suppose the  $i$ th subtree has  $n_i$  nodes and  $l_i$  leaves, for  $1 \leq i \leq k$ . As each  $n_i < n$ , by the induction hypotheses, we may assume  $n_i = (kl_i - 1)/(k - 1)$ , for  $1 \leq i \leq k$ .

Therefore,

$$\begin{aligned} n &= 1 + n_1 + \cdots + n_k \\ &= 1 + (kl_1 - 1)/(k - 1) + \cdots + (kl_k - 1)/(k - 1) \\ &= ((k - 1) + k(l_1 + \cdots + l_k) - k)/(k - 1) \\ &= (kl - 1)/(k - 1). \quad \square \end{aligned}$$

## Another proof of Euclid's theorem

For  $n \geq 0$ ,  $F_n = 2^{2^n} + 1$  is called the  $n$ th *Fermat number*.

**Theorem.** For all  $n \geq 0$ ,  $F_n = \prod_{k=0}^{n-1} F_k + 2$ .

*Proof.* See above.

**Corollary.** There exist infinitely many prime numbers.

*Proof.* First, note that every two Fermat numbers are relatively prime, *i.e.*, they have no common factors. This follows from the theorem since, if some number  $m > 1$  divides both  $F_k$  and  $F_n$  for  $k < n$ , then  $m$  also divides 2. Hence  $m = 2$ . But  $m = 2$  is impossible, as every Fermat number is odd. Second, this implies that each successive Fermat number has new prime factors, so there are infinitely prime numbers.  $\square$

## Sample proof by diagonalisation

To be provided later...