

# 1 Proof techniques

**Proof Technique 1** (Contraposition). To prove a statement of the form

$$P \implies Q$$

instead prove the statement

$$(\neg Q) \implies (\neg P).$$

**Problem 1.1.** Prove that, for any real numbers  $x$  and  $y$ , if  $xy = 0$  then  $x = 0$  or  $y = 0$ .

**Proof Technique 2** (Induction). To prove a statement of the form

$$\forall n \in \mathbb{N}, P(n)$$

prove the following statements:

- (i)  $P(0)$
- (ii)  $\forall n \in \mathbb{N}, (P(n) \implies P(n+1))$

**Problem 2.1.** Prove that  $2^n < 3^n$  for every integer  $n > 0$ .

**Problem 2.2.** Suppose that  $p$  and  $q$  are positive real numbers such that  $p < q$ . Prove that  $p^n < q^n$  for all natural numbers  $n > 1$ . You may use the following facts about the  $<$  relation: If  $x < y$  and  $0 < a < b$  then  $ax < by$ .

**Proof Technique 3** (Proof by cases). To prove a statement

$$(P \vee Q) \implies R$$

prove the two statements

$$\begin{aligned} P &\implies R \\ Q &\implies R. \end{aligned}$$

**Problem 3.1.** Prove that for any natural number  $n$  either  $n$  or  $n+1$  is divisible by 2.

**Proof Technique 4** (Strong induction). To prove a statement of the form

$$\forall n \in \mathbb{N}, P(n)$$

prove the sentence

$$\forall n \in \mathbb{N}, \left( (\forall m \in \mathbb{N}, (m < n \implies P(m))) \implies P(n) \right).$$

Here is a slightly less precise but more readable version of this sentence:

$$\forall n, \left( (\forall m < n, P(m)) \implies P(n) \right)$$

**Problem 4.1.** Prove that, for every integer  $n$ , either there is an integer  $m$  such that  $nm = 1$  or there is a prime number  $p$  such that  $p|n$ .

**Problem 4.2.** Let  $a_0, a_1, a_2, \dots$  be the sequence with the following properties:

- (i)  $a_0 = a_1 = 0$
- (ii)  $a_2 = 1$
- (iii)  $a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3}$

Prove that  $a_n = 2^n - n - 1$  for all natural numbers  $n$ .

*Solution.* We have  $2^0 - 0 - 1 = 0$  and  $2^1 - 1 - 1 = 0$  and  $2^2 - 2 - 1 = 1$ . This gives a base case.

Now assume for the sake of strong induction that  $n \geq 3$  and that  $a_m = 2^m - m - 1$  for  $m < n$ . We want to prove that  $a_n - 2^n - n - 1 = 0$ . We have

$$\begin{aligned} a_n &= 4a_{n-1} - 5a_{n-2} + 2a_{n-3} \\ &= 4 \times (2^{n-1} - n) - 5 \times (2^{n-2} - n + 1) + 2 \times (2^{n-3} - n + 2) \\ &= 2 \times 2^n - 2^n - 2^{n-2} + 2^{n-2} - 4n + 5n - 2n - 5 + 4 \\ &= 2^n - n - 1 \end{aligned}$$

exactly as desired. This proves the induction step and completes the proof.  $\square$

**Problem 4.3.** Prove that, for any natural number  $n$ , one of the numbers  $n$ ,  $n + 1$ , or  $n + 2$  is divisible by 3.

*Solution.* The proof is by induction on  $n$ . Let  $P(n)$  be the sentence “Either  $n$ ,  $n + 1$ , or  $n + 2$  is divisible by 3.” The statement is certainly true for  $n = 0$ , since 0 is divisible by 3, so we have the base case for induction.

Assume that  $n$  is an integer such that  $P(n)$  is true. We prove that  $P(n + 1)$  is true. We know from  $P(n)$  that either  $n$ ,  $n + 1$ , or  $n + 2$  is divisible by 3. If  $3|n + 1$  or  $3|n + 2$  then  $P(n + 1)$  is obviously true (after all  $P(n + 1)$  is the sentence  $3|n + 1 \vee 3|n + 2 \vee 3|n + 3$ ). The only remaining possibility is that  $3|n$ . In that case  $n = 3k$  for some integer  $k$  (by the definition of divisibility), so  $n + 3 = 3k + 3 = 3(k + 1)$ . As  $k + 1$  is an integer, this tells us that  $n + 3$  is divisible by 3, again by the definition of divisibility. Thus

$$3|n \vee 3|n + 1 \vee 3|n + 2 \implies 3|n + 1 \vee 3|n + 2 \vee 3|n + 3,$$

which proves the induction step.  $\square$

**Problem 4.4.** Prove by induction that every non-empty subset of  $\mathbb{N}$  has a least element.

*Solution.* Suppose that  $S \subset \mathbb{N}$  is a subset without a least element. We prove by strong induction that  $S = \emptyset$ . Let  $P(n)$  be the sentence  $n \notin S$ . We prove  $P(n)$  for all natural numbers  $n$  by strong induction on  $n$ .

Let  $n$  be a natural number and assume for the sake of strong induction that, for all  $m < n$ , the sentence  $P(m)$  is true. That is, for all  $m < n$ , we know that  $m \notin S$ . Therefore, if  $n$  were in  $S$  then  $n$  would be the least element of  $S$ . As  $S$  has no least element, we conclude that  $n \notin S$ . Therefore  $P(n)$  is also true. This proves the induction step, so by strong induction we conclude that  $S = \emptyset$ .  $\square$

**Proof Technique 5** (Bidirectional induction). To prove a statement of the form

$$\forall n \in \mathbb{Z}, P(n)$$

instead prove the two sentences

- (i)  $\exists n \in \mathbb{Z}, P(n)$
- (ii)  $\forall n \in \mathbb{Z}, (P(n) \iff P(n + 1))$

## 2 Other problems

**Problem 2.1.** Suppose that  $A = \{a, b, c\}$  and  $R$  is a total order on  $R$  such that

$$\begin{aligned} (a, b) &\in R \\ (b, c) &\in R \\ (c, a) &\in R. \end{aligned}$$

What is the cardinality of  $A$ ? Justify your answer.

**Problem 2.2.** Prove that  $1 + 2 + 4 + 8 + \cdots + 2^n = 2^{n+1} - 1$  for every  $n \in \mathbb{N}$ .

**Problem 2.3.** Prove that divisibility is a partial order on the natural numbers but not on the integers.