

Learning Objectives

By the end of this worksheet, you will:

- Practice writing proofs and disproofs of statements.
- Prove statements using the techniques of simple induction and contradiction.

1. **Induction.** Consider the following statement:

$$\forall n \in \mathbb{N}, n \leq 2^n$$

- (a) Suppose we want to prove this statement using induction. Write down the full statement we'll prove (it should be an **AND** of the base case and induction step). Consult your notes if you aren't sure about this!

Solution

$$0 \leq 2^0 \wedge (\forall k \in \mathbb{N}, k \leq 2^k \Rightarrow k + 1 \leq 2^{k+1})$$

- (b) Prove the statement using induction. We strongly recommend reviewing the induction proof template from lecture before working on a proof here.

Hint: $2^{k+1} = 2^k + 2^k$.

Solution

Proof. We will prove this statement using induction on n .

Base case: let $n = 0$.

Then $2^n = 1$, and $n = 0$, so $n \leq 2^n$.

Induction step: let $k \in \mathbb{N}$, and assume that $k \leq 2^k$. We want to prove that $k + 1 \leq 2^{k+1}$.

Since $0 \leq k$, we know that $1 \leq 2^k$ (raising 2 to the power of either side). Then we can add this inequality to our assumption $k \leq 2^k$ to get:

$$k + 1 \leq 2^k + 2^k$$

$$k + 1 \leq 2^{k+1}$$

□

2. **A proof by contradiction.** Consider the following statement:¹

$$\forall x, y \in \mathbb{Z}^+, x^2 - y^2 \neq 1$$

Prove this statement using a proof by contradiction. Make sure you clearly identify the following two things (which are specific to proofs by contradiction):

- What you're assuming (the negation of the original statement).
- The contradiction that is made (this should be the last line of the proof).

For this question, you can use external facts you have already seen in this course (in previous worksheets, for example).

¹ In English, we would say that "the equation $x^2 - y^2 = 1$ has no positive integer solutions."

Solution

Proof. Assume the negation of this statement, i.e., that there exist $x, y \in \mathbb{Z}^+$ such that $x^2 - y^2 = 1$.

Then we can factor the left-hand side to get $(x + y)(x - y) = 1$. By the definition of divisibility, we can conclude that $(x + y) \mid 1$. Since x and y are positive integers, $x \geq 1$ and $y \geq 1$, so $x + y \geq 2$. However, by an external fact from last time, we know that if $(x + y) \mid 1$, then $x + y \leq 1$.

So then we have deduced both $x + y \geq 2$ and $x + y \leq 1$, which is our contradiction. \square

[Comment: there's lots of possible contradictions here! Another one might be to prove that $x < 1 \vee y < 1$, which contradicts the statement that $x, y \in \mathbb{Z}^+$.]

3. **Linear combinations and divisibility.** Let $x, y \in \mathbb{Z}$. A **linear combination** of x and y is a number that can be written in the form $px + qy$, where p and q are some integers.

- (a) Show how to define the predicate $LinComb(x, y, z)$, which says that z is a linear combination of x and y , where $x, y, z \in \mathbb{Z}$.

Solution

$$LinComb(x, y, z) : \exists p, q \in \mathbb{Z}, z = px + qy$$

- (b) Translate the following statement into predicate logic:

For every pair of even integers x and y , every linear combination of x and y is also even.

Use the divisibility predicate in the form $2 \mid x$ to express the fact that x is even.

Solution

$$\forall x, y \in \mathbb{Z}, 2 \mid x \wedge 2 \mid y \Rightarrow (\forall z \in \mathbb{Z}, LinComb(x, y, z) \Rightarrow 2 \mid z)$$

- (c) Prove the statement from part (b). Do not use any external facts about divisibility in your proof.

Solution

Proof. Let $x, y \in \mathbb{Z}$, and assume $2 \mid x$ and $2 \mid y$. By the definition of divisibility, there exist $k_1, k_2 \in \mathbb{Z}$ such that $x = 2k_1$ and $y = 2k_2$. Let $z \in \mathbb{Z}$ and assume z is a linear combination of x and y . By the definition of linear combination, there exist $p, q \in \mathbb{Z}$ such that $z = px + qy$. We want to prove that $2 \mid z$, i.e., that there exists $k_3 \in \mathbb{Z}$ such that $z = 2k_3$.

We leave the rest of the proof as an exercise; find the correct value of k_3 in your rough work, and then show that $z = 2k_3$. \square

- (d) *Extra.* Generalize the statement from part (b) by replacing “is even” by “is divisible by d ” (for an arbitrary $d \in \mathbb{N}$). Then, prove it!