

Problem 1. Practice with the axioms of \mathbb{Z} . For the following exercises I want you to give Euclidean style proofs using the axioms of \mathbb{Z} from the handout. That is, *don't assume anything* and *justify every tiny little step*.

- (a) Given integers $a, b, c \in \mathbb{Z}$ with $a + b = a + c$, prove that $b = c$. This is called the **cancellation property** of \mathbb{Z} . [Hint: First apply axiom (A4) to the integer a .]
- (b) Axiom (A3) says that for each integer $a \in \mathbb{Z}$ there exists another integer $b \in \mathbb{Z}$ such that $a + b = 0$ (and we call this b an “additive inverse” of a). Prove that additive inverses are **unique**. That is, show that if $a + b = 0$ and $a + c = 0$ then $b = c$. [Hint: Use part (a).]

[Since the additive inverse of a is unique, we might as well give it a name. How about “ $-a$ ”?]

Problem 2. For each integer $a \in \mathbb{Z}$ we define the absolute value:

$$|a| := \begin{cases} a, & \text{if } a \geq 0, \\ -a, & \text{if } a < 0. \end{cases}$$

- (a) Prove that for all integers $a, b \in \mathbb{Z}$ we have $|ab| = |a||b|$. [Hint: You may assume the properties $(-a)(-b) = ab$ and $(-a)b = -(ab)$ without proof. We'll prove them later.]
- (b) Given integers $a, b \in \mathbb{Z}$ we say that a **divides** b (and we write $a|b$) if there exists $q \in \mathbb{Z}$ such that $b = qa$. If $a|b$ and $b \neq 0$, prove that $|a| \leq |b|$. [Hint: If $q \neq 0$ note that $|q| \geq 1$. Now use part (a).]

Problem 3. Prove that $\sqrt{3}$ is not a ratio of whole numbers, in two steps.

- (a) First prove the following **lemma**: Given a whole number n , if n^2 is a multiple of 3, then so is n . [Hint: Use the contrapositive, and note that there are two different ways for n to be not a multiple of 3. Treat each separately.]
- (b) Use the method of contradiction to prove that $\sqrt{3}$ is not a ratio of whole numbers. Quote your lemma in the proof. [Hint: Mimic the proof for $\sqrt{2}$ as closely as possible.]

Problem 4. In this exercise you will show that all of Boolean logic can be expressed using only the concepts NOT and \Rightarrow . We use the symbol \equiv to denote logical equivalence.

- (a) Use a truth table to show that “ P OR Q ” \equiv “(NOT P) \Rightarrow Q ”.
- (b) Use a truth table to show that “ P AND Q ” \equiv “NOT($P \Rightarrow$ (NOT Q))”.
- (c) Write the statement $P \Leftrightarrow Q$ using **only the symbols** P , Q , NOT and \Rightarrow (and, of course, parentheses).