Note 2

Proofs

A mathematical proof provides a means for guaranteeing that a statement is true.

So what is a proof? A proof is a finite sequence of steps, called **logical deductions**, which establishes the truth of a desired statement. In particular, the power of a proof lies in the fact hat using finite means, we can guarantee the truth of a statement with infinitely many cases.

A proof is typically structured as follows:

1. Recall that there are certain statements, called **axioms** or **postulates**, that we accept without proof.
2. From these axioms, a sequence of logical deductions follows.
3. Each statement follows the previous one where each successive statement is necessarily true if the previous statement is true.

The rule of logic are a formal distillation of laws that were thought to underlie human thinking. They play a central role in the design of computers, starting with digital logic design or the fundamental principles behind the design of digital circuits.

Notation and Basic Facts

Let $\mathbb{Z}$ denote the set of integers, i.e., $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, and $\mathbb{N}$ the set of natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$.

Recall that the sum or product of two integers is an integer, i.e., the set of integers is closed under addition and multiplication. The set of natural numbers is also closed under addition and multiplication.

Given integers a and b, we say a divides b (denoted $a \mid b$) iff there exists an integer q such that $b = aq$. For example, $2 \mid 10$ because there exists an intger $q = 5$ such that $10 = 5 \cdot 2$. We say a natural number $p \geq 2$ is prime if it is divisible only by 1 and itself.

Finally, we use the notation $:=$ to indicate a definition. For example, $q := 6$ defines variable q as having value 6.

Direct Proof

Theorem 2.1. *For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Direct Proof
Goal: To prove $P \Rightarrow Q$
Approach: Assume P
$\vdots$
Therefore Q

For each x, the proposition we are trying to prove is of the form $P(x) \Rightarrow Q(x)$. A direct proof of this starts by assuming $P(x)$ for a generic value of x and eventually concludes $Q(x)$ through a chain of implications.

Proof of Theorem 2.1. Assume that $a \mid b$ and $a \mid c$, i.e., there exist integers q_1 and q_2 such that $b = q_1 a$ and $c = q_2 a$. Then, $b + c = q_1 a + q_2 a = (q_1 + q_2)a$. Since the $\mathbb{Z}$ is closed under addition, we conclude that $(q_1 + q_2) \in \mathbb{Z}$, and so $a \mid (b + c)$, as desired.

The key insight is that the proof did not assume any specific values for a, b, and c; our proof holds for arbitrary $a, b, c \in \mathbb{Z}$. Thus, we have prove the desired claim.

Theorem 2.2. *Let $0 < n < 1000$ be an integer. If the sum of the digits of n is divisible by 9, then n is divisible by 9.*

Observe that this statement is equivalent to

$$(\forall n \in \mathbb{Z}^+)(n < 1000) \Rightarrow (\text{sum of } n\text{'s digits divisible by } 9 \Rightarrow n \text{ divisible by } 9).$$

where $\mathbb{Z}^+$ denotes the set of positive integers, $\{1, 2, \dots\}$. Now the proof proceeds similarly – we start by assuming, for a generic value of n, that the sum of n's digits is divisible by 9. Then we perform a sequence of implications to conclude that n itself is divisible by 9.

Theorem 2.3 (Converse of Theorem 2.2)**.** *Let $0 < n < 1000$ be an integer. If n is divisible by 9, then the sum of the digits of n is divisible by 9.*

Proof of Theorem 2.3. Assume that n is divisible by 9. We use the same notation for the digits of n as we used in Theorem 2.2's proof.

$$\begin{aligned} n \text{ is divisible by } 9 &\Rightarrow n = 9l \text{ for } \mathbb{Z} \\ &\Rightarrow 100a + 10b + c = 9l \\ &\Rightarrow 99a + 9b + (a + b + c) = 9l \\ &\Rightarrow a + b + c = 9l - 99a - 9b \\ &\Rightarrow a + b + c = 9(l - 11a - b) \\ &\Rightarrow a + b + c = 9k \text{ for } k = l - 11a - b \in \mathbb{Z} \end{aligned}$$

We conclude that $a + b + c$ is divisible by 9.

Proof by Contraposition

Recall that any implication $P \Rightarrow Q$ is equivalent to its contrapositive $\neg Q \Rightarrow \neq P$. Sometimes $\neg Q \Rightarrow \neg P$ can be much simpler to prove than $P \Rightarrow Q$. Thus, a proof by contraposition proceeds by having $\neg Q \Rightarrow \neg P$ instead of $P \Rightarrow Q$.

Proof by Contraposition
Goal: To prove $P \Rightarrow Q$.
Approach: Assume $\neg Q$
$\vdots$
Therefore $\neg P$
Conclusion: $\neg Q \Rightarrow \neg P$, which is equivalent to $P \Rightarrow Q$.

Theorem 2.4. *Let n be a positive integer and let d divide n. If n is odd, then d is odd.*

Proof of Theorem 2.4. We proceed by contraposition (If d is even, then n is even). If we assume d is even, then, by definition, $d = 2k$ for some $k \in \mathbb{Z}$. Because $d \mid n$, then $n = dl$ for some $l \in \mathbb{Z}$. Combining these two statements, we have $n = dl = (2k)l = 2(kl)$. We conclude that n is even.

Note that the proof technique was stated as the first line. This is generally good practice.

Theorem 2.5 (Pigeonhole principle). *Let n and k be positive integers. Place n objects into k boxes. If $n > k$, the at least one box must contain multiple objects.*

Proof of Theorem 2.5. We proceed by contraposition. If all boxes contain at most one object, then the number of objects is at most the number of boxes, i.e., $n \leq k$.

Proof by Contradiction

The idea in a proof by contradiction relies crucially on the fact that if a proposition is not false, then it must be true.