Note 2

Important Things to Note

Theorems

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

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.*

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.*

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

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

Theorem 2.6. *There are infinitely many prime numbers.*

Theorem 2.7. *$\sqrt{2}$ is irrational.*

Theorem 2.8. *There exist irrational numbers x and y such that x^y is rational.*

Theorem 2.9. *Let $n \in \mathbb{Z}^+$. If the sum of the digits of n is divisible by 9, then n is divisible by 9.*

Lemmas

Lemma 2.1. *Every natural number greater than one is either prime or has a prime divisor.*

Lemma 2.2. *If a^2 is even, then a is even.*

Lemma 2.3. *If a is an integer, then a^2 is an integer.*

Lemma 2.4. *If a and b are both integers, then ab is an integer.*

Tips to Avoid Errors

Lesson #1: When writing proofs, do not assume the claim you aim to prove.

Lesson #2: Never forget to consider the case where your variables take on the value zero.

Lesson #3: Be careful when mixing negative numbers and inequalities.

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 that 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 rules 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 proved 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.

Proof of Theorem 2.2. Let n in decimal be written as $n = abc$, i.e. $n = 100a + 10b + c$. Assume that the sum of the digits of n is divisible by 9, i.e.

$$\exists k \in \mathbb{Z} \text{ such that } a + b + c = 9k. \tag{1}$$

Adding $99a + 9b$ to both sides of Equation (1), we have

$$100a + 10b + c = n = 9k + 99a + 9b = 9(k + 11a + b).$$

We conclude that n 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 $n > k$, then 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.

Proof by Contradiction
Goal: To prove P.
Approach: Assume $\neg P$
$\vdots$
R
$\vdots$
$\neg R$
Conclusion: $\neg P \Rightarrow \neg R \wedge R$, which is a contradiction. Thus, P.

A proof by contradiction shows that $\neg P \Rightarrow \neg R \wedge R \equiv$ False. The contrapositive of this statement is hence True $\Rightarrow P$.

Theorem 2.6. *There are infinitely many prime numbers.*

Using a proof technique like direct proof seems to be very difficult. How would you construct infinitely many prime numbers? If we use contradiction instead by assuming the statement is false, i.e., there are only finitely many primes, bad things will happen.

Lemma 2.1. *Every natural number greater than one is either prime or has a prime divisor.*

Proof of Theorem 2.6. We proceed by contradiction. Suppose that Theorem 2.6 is false, i.e., there are only finitely many primes, say k of them. Then, we can enumerate them: $p_1, p_2, p_3, \ldots, p_k$.
Define number $q := p_1 p_2 p_3 \ldots p_k + 1$, which is the product of all primes plus one. We can then claim that q cannot be prime because by definition, it is larger than all the primes p_1 through p_k. By Lemma 2.1, we therefore conclude that q has a prime divisor p. This will be our statement R.

Next, because $p_1, p_2, p_3, \ldots, p_k$ are all the primes, p must be equal to one of them: thus, p divides $r := p_1 p_2 p_3 \ldots p_k$. Hence, $p \mid q$ and $p \mid r$, implying $p \mid (q - r)$. But $q - r = 1$, implying $p \leq 1$, and hence p is not prime; this is the statement $\neg R$. We thus have $R \wedge \neg R$, which is a contradiction, as desired. □

Theorem 2.7. $\sqrt{2}$ *is irrational.*

Why should contradiction be a good candidate proof technique to try here? Consider this: Theorem 2.6 and Theorem 2.7 share something fundamental – in both cases, we wish to show something doesn't exist.

For Theorem 2.6, we wished to show that a largest prime doesn't exist.
For Theorem 2.7, we wish to show that integers a and b satisfying $\sqrt{2} = a/b$ don't exist.

Lemma 2.2. *If a^2 is even, then a is even.*

Proof of Theorem 2.7. We proceed with contradiction. Assume that $\sqrt{2}$ is rational. By the definition of rational numbers, there are integers a and b with no common factor other than 1, such that $\sqrt{2} = a/b$. Let our assertion R state that a and b share no common factors.

For any numbers x and y, we know that $x = y \Rightarrow x^2 = y^2$, hence $2 = a^2/b^2$. Multiplying both sides by b^2, we have $a^2 = 2b^2$. Since b is an integer, it follows that b^2 is an integer, and thus a^2 is even. Plugging in Lemma 2.2, we hence have that a is even. In other words, there exists an integer c such that $a = 2c$.

Combining all facts together, we have that $2b^2 = 4c^2$, or $b^2 = 2c^2$. Since c is an integer, c^2 is an integer, and hence b^2 is even. Thus, again applying Lemma 2.2, we conclude that b is even.

But we have just shown that both a and b are even. In particular, this means they share the common factor 2. This implies $\neg R$. We conclude that $R \wedge \neg R$ holds; thus, we have a contradiction, as desired. □

Proof by Cases

The idea behind a proof by cases is as follows: Sometimes when we wish to prove a claim, we don't know which a set of possible cases is true, but we know that at least one is true. What we can do then is to prove the result in both cases; then , clearly the general statement must hold.

Theorem 2.8. *There exist irrational numbers x and y such that x^y is rational.*

Proof of Theorem 2.8. We proceed by cases. Note that the statement of the theorem is quantified by an existential quantifier. Thus, to prove our claim, it suffices to demonstrate a single x and y such that x^y is rational. To do so, let $x = \sqrt{2}$ and $y = \sqrt{2}$. Let us divide our proof into two cases, exactly one of which must be true:

(a) $\sqrt{2}^{\sqrt{2}}$ is rational, or

(b) $\sqrt{2}^{\sqrt{2}}$ is irrational.

Case (a). Assume first that $\sqrt{2}^{\sqrt{2}}$ is rational. But this immediately yields our claim, since x and y are irrational numbers such that x^y is rational.

Case (b). Assume now that $\sqrt{2}^{\sqrt{2}}$ is irrational. This obviously means that x^y is not rational, so our first guess for x and y was not right, so let's set $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Then,

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2,$$

where the second equality follows from the axiom $(x^y)^z = x^{yz}$. But now we again started with two irrational numbers x and y and obtained rational x^y.

Since one of case (a) or case (b) must hold, we thus conclude that the statement of Theorem 2.8 is true. □

This is also an example of a **non-constructive** proof: We've proven that some object X exists but without explicitly revealing what X itself is. What were the actual numbers x and y satisfying the claim of Theorem 2.8? Were they $x = \sqrt{2}$ and $y = \sqrt{2}$? Or $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$? Since we did a case analysis, it's not clear which of the two choices is actually the correct one.

Common Errors When Writing Proofs

Claim: $-2 = 2$.

Proof? Assume $-2 = 2$. Squaring both sides, we have $(-2)^2 = 2^2$, or $4 = 4$, which is true. We conclude that $-2 = 2$, as desired. ♠

The theorem is obviously false, so what did we do wrong? Our arithmetic is correct, and each step rigorously follows from the previous step. So, the error must lie in the very beginning of the proof, where we made a brazen assumption: That $-2 = 2$. In other words, to prove the statement $P \equiv$ "$-2 = 2$", we just proved that $P \Rightarrow$ True, which is not the same as proving P.

Lesson #1: When writing proofs, do not assume the claim you aim to prove.

Lesson #2: Never forget to consider the case where your variables take on the value zero. Otherwise, this can happen:

Claim: $1 = 2$.

Proof? Assume that $x = y$ for integers $x, y \in \mathbb{Z}$. Then,

$$\begin{aligned} x^2 - xy &= x^2 - y^2 && \text{(since } x = y\text{)} \\ x(x-y) &= (x+y)(x-y) \\ x &= x + y && \text{(divide both sides by } x - y\text{)} \\ x &= 2x \end{aligned}$$

Setting $x = y = 1$ yields the claim. ♠

In deriving the third equality, we divided by $(x - y)$. Since $x = y$, the value of $(x - y)$ in our setting is zero. Dividing by zero is not well-defined; thus the third equality does not hold.

Lesson #3: Be careful when mixing negative numbers and inequalities. For example:

Claim: $4 \leq 1$.

Proof? We know that $-2 \leq 1$; squaring both sides of this inequality yields $4 \leq 1$. ♠

Unfortunately, the answer isn't very satisfactory when there are opposite signs on the ends of an inequality. In this case, the claim and proof is obviously not true, but let's provide a counterexample: We know that $2 > -1$. This time, squaring both sides of the inequality yields $4 > 1$, which is still true.

In general, if an inequality holds and there are positive signs on both ends, then the inequality holds after squaring. If they are both negative, then flipping the sign after squaring maintains the inequality.

In addition, do not forget that multiplying an inequality by a negative number flips the direction of the inequality. For example, multiplying both sides of $-2 < 5$ by -1 yields $2 > -5$, as you would expect.

Style and Substance in Proofs

Get in the habit of thinking carefully before you write down the next sentence of your proof. If you cannot explain clearly why the step is justified, you are making a leap and you need to go back and think some more.

In theory, each step in a proof must be justified by appealing to a definition or general axiom. In practice, the depth to which one must do this is a matter of taste.

For example, we could break down the step, "Since a is an integer, $(2a^2 + 2a)$ is an integer," into several more steps.

Lemma 2.3. *If a is an integer, then a^2 is an integer.*

Lemma 2.4. *If a and b are both integers, then ab is an integer.*

Proof. Per Lemma 2.3, a^2 is an integer. Per Lemma 2.4, $2a^2$ and $2a$ are integers, so $(2a^2 + 2a)$ is an integer. □

A justification can be stated without proof only if you are absolutely confident that (1) it is correct and (2) the reader will automatically agree that it is correct.

It is often a good idea to break down a long proof down into several lemmas. Furthermore, make each lemma as general as possible so it can be reused elsewhere. Notice that in the proof that $\sqrt{2}$ is irrational, we used the result "For any integer n, if n^2 is even then n is even," twice. This suggests that it is a good candidate to becoming a lemma, since it is useful in more complex proofs.

Remember, theorems are propositions that you want to "export" from the paper to the rest of the world, whereas lemmas are propositions used locally in the proofs of your theorems.

Exercises

1. Generalize the proof of Theorem 2.2 so that it works for any positive integer n. (Hint: Suppose n has k digits, and write a_i for the digits of n, so that $n = \sum_{i=0}^{k-1}(a_i \cdot 10^i)$.)

Theorem 2.9. *Let $n \in \mathbb{Z}^+$. If the sum of the digits of n is divisible by 9, then n is divisible by 9.*

2. Prove Lemma 2.2. (Hint: First try a direct proof. Then, try contraposition. Which proof approach is better suited to proving this lemma?)

Lemma 2.2. *If a^2 is even, then a is even.*