CHAPTER

3 Review

3.1 Definitions in Chapter 3

3.1 Proof: An Informal Definition

3.2 Mathematical Proof

3.3 Group

3.4 The Natural Numbers

3.5 The Integers

3.6 The Rational Numbers

3.7 Irrational Numbers

3.8 Divisible

3.10 Even and Odd

3.11 Greatest Common Divisor

3.13 Least Common Multiple

3.14 Prime, Composite

3.16 Relatively Prime

3.17 Pythagorean Triple

3.18 a mod m

3.19 $a \equiv b \pmod{m}$

3.20 $n!$

3.21 Floor Function; Ceiling Function

3.40 max; min

3.42 Linear Congruence

3.43 The Inverse of a, mod m

3.56 Geometric Progression

3.57 Arithmetic Progression

3.59 0^0

3.61 Optimal

3.62 Possible

3.74 Honest

3.2 Sample Exam Questions

1. Describe the basic components of an axiomatic mathematical system.

2. Let x be an even integer and y be an odd integer. What is wrong with the following proof that $x + 2y = 3y - 1$?

Incorrect Proof
Since x is even, there is an integer, n, such that $x = 2n$. Since y is odd, there is an integer, n, such that $y = 2n + 1$. Therefore, $x + 2y = 2n + 2(2n + 1) = 6n + 2 = 3(2n + 1) - 1 = 3y - 1$. □

3. Describe how (and why) an indirect proof works.

4. Consider gcd(140, 336).

(a) What is the value of gcd(140, 336)? Show your work.

(b) Use the Quotient–Remainder theorem to find integers, s and t, such that $140s + 336t = \gcd(140, 336)$.

5. State the well-ordering principle.

6. What is the numeric limit of $\sum_{i=0}^{\infty} \left(\frac{6}{10}\right)^i$?

7. Use mathematical induction to prove that the sum of the first n odd positive integers is n^2:

$$\forall n \in \mathbb{Z} \text{ with } n \geq 1, \sum_{k=1}^{n}(2k-1) = n^2.$$

8. Let $a_1, a_2, \ldots, a_n$ be n real numbers, with $n \geq 1$. Prove:

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \leq a_j$$

for at least one $j \in \{1, 2, 3, \ldots, n\}$. [*Hint*: What is the negation of this claim?]

9. Prove or find a counterexample: $2^n + 1$ is a prime for all positive integers, n.

10. Let n be an odd integer. Prove that $n^3 + 2n^2$ is also odd.

(a) Use a direct proof.

(b) Use an indirect proof.

(c) Use a proof by contradiction.

3.3 Projects

Mathematics

1. Write a brief expository paper explaining one or two more proof strategies that were not presented in this book.

2. Consider an alternative form of induction that is a compromise between mathematical induction and complete induction. The new form can be expressed as

$$[P(1) \wedge P(2) \wedge (\forall i, P(i) \wedge P(i+1) \rightarrow P(i+2))] \\ \rightarrow [\forall k, P(k)]\,.$$

Prove that this new form and mathematical induction and complete induction are all equivalent.

3. Write a brief exposition describing the failed attempt of Girolamo Saccheri to show that Euclid's fifth postulate could be proved as a theorem using only the other four postulates.

4. Write a brief exposition describing the discovery of non-Euclidean geometries.

Computer Science

1. Use your favorite computer language to write a program that calculates the greatest common divisor of two integers. Use the algorithm based on the Quotient–Remainder theorem (as in Example 3.21).

2. Write a brief expository paper explaining the basic ideas in correctness proving for computer programs.

3. Write a brief expository paper describing the current status of theorem-proving programs.

4. Do some research on efficient algorithms for factoring integers. Then write a program that uses an algorithm that is a reasonable compromise between the goals of simplicity and efficiency.

General

1. Write a brief expository paper about inductive and deductive reasoning.

2. Compare and contrast the nature of proof in mathematics and in science.

3. Compare and contrast the nature of proof in mathematics and in a courtroom.

4. Write a brief expository paper about how the social, political, and economic climate in ancient Greece and ancient Alexandria influenced the development of axiomatic mathematics.

3.4 Solutions to Sample Exam Questions

1. The axiomatic method is a technique of deduction from prior concepts. It starts with a collection of undefined terms, some axioms that describe how those terms interact, and a system of logic and rules of inference. Definitions are used to provide a shorthand notation for commonly occurring ideas. Additional properties are then proved to be true. Assertions that have been proved are called theorems, propositions, corollaries, and lemmas. A corollary is an assertion whose proof follows in a simple fashion from some other theorem (or proposition). Lemmas are usually used to prove some messy details in the proof of some other theorem.

2. By setting $x = 2n$ and $y = 2n + 1$, the proof assumes that x and y are consecutive integers. The claim is true in that case, but it will fail for nonconsecutive integers (such as 2 and 5).

3. The logical equivalence $[P \rightarrow Q] \Leftrightarrow [(\neg Q) \rightarrow (\neg P)]$ implies that the contrapositive of a valid theorem is automatically true. Thus, if the assertion $A \rightarrow B$ needs to be proved, it is possible to show that $\neg B \rightarrow \neg A$ is true and then conclude that $A \rightarrow B$ is true.

4. (a) There are several ways to perform this calculation. One option is to factor both numbers. Since $140 = 2^2 \cdot 5 \cdot 7$ and $336 = 2^4 \cdot 3 \cdot 7$, $\gcd(140, 336) = 2^2 \cdot 7 = 28$.

(b) The two phases are quite straightforward for this problem.

Phase 1:

$$\begin{aligned} 336 &= 140 \cdot (2) + 56 & \qquad 56 &= 140 \cdot (-2) + 336 \\ 140 &= 56 \cdot (2) + 28 & 28 &= 56 \cdot (-2) + 140 \\ 56 &= 28 \cdot (2) + 0 & 0 &= 28 \cdot (-2) + 56 \end{aligned}$$

Phase 2: completed by using phase 1 equations

$$\begin{aligned} 28 &= 140 - 56 \cdot (2) \\ &= 140 - (336 - 140 \cdot (2)) \cdot (2) \\ &= 140 \cdot (5) + 336 \cdot (-2) \end{aligned}$$

Phase 2: completed by using rearranged equations

$$\begin{aligned} 28 &= 56 \cdot (-2) + 140 \\ &= (140 \cdot (-2) + 336) \cdot (-2) + 140 \\ &= 140 \cdot (5) + 336 \cdot (-2) \end{aligned}$$

5. Every nonempty set of natural numbers has a smallest element.

6. $\displaystyle\sum_{i=0}^{\infty}\left(\frac{6}{10}\right)^i = \frac{1}{1-\frac{6}{10}} = 2.5$

7. Let $P(n)$ be the claim that $\sum_{k=1}^{n}(2n-1) = n^2$.

Base Step
When $n = 1$, $\sum_{k=1}^{1}(2k-1) = 2\cdot 1 - 1 = 1 = 1^2$. Thus, $P(1)$ is true.

Inductive Step
Assume that $P(n)$ is true for some $n \geq 1$. Then

$$\begin{aligned}\sum_{k=1}^{n+1}(2k-1) &= (2(n+1)-1) + \sum_{k=1}^{n}(2k-1)\\ &= (2n+1)+n^2 \quad \text{by the inductive hypothesis}\\ &= (n+1)^2.\end{aligned}$$

Consequently, $P(n+1)$ is also true.

Conclusion
Since $P(1)$ is true, and for all $n \geq 1$, $P(n) \to P(n+1)$ is true, the theorem of mathematical induction implies that $P(n)$ is true for all $n \geq 1$.

8. Suppose, by way of contradiction, that

$$\frac{a_1+a_2+\cdots+a_n}{n} > a_j \quad \text{for all } j \in \{1, 2, 3, \ldots, n\}.$$

Then

$$\begin{aligned}\sum_{j=1}^{n} a_j &< \sum_{j=1}^{n}\left(\frac{a_1+a_2+\cdots+a_n}{n}\right)\\ &= n\cdot\left(\frac{a_1+a_2+\cdots+a_n}{n}\right) = \sum_{j=1}^{n} a_j.\end{aligned}$$

The assertion that

$$\sum_{j=1}^{n} a_j < \sum_{j=1}^{n} a_j$$

is a clear contradiction. The initial assumption must be false, so

$$\frac{a_1+a_2+\cdots+a_n}{n} \leq a_j$$

for at least one $j \in \{1, 2, 3, \ldots, n\}$ must be true for $n \geq 1$.

9. When $n = 3$, $2^n + 1 = 9$, which is not a prime. Thus, $n = 3$ is a counterexample to the claim.

10. (a) At least two simple direct proofs are possible.

i. Notice that $n^3 + 2n^2 = n^2(n+2)$. Since n is odd, $n+2$ must also be odd [there is an integer, k, such that $n = 2k+1$, so $n+2 = 2k+3 = 2(k+1)+1$ is also odd]. The product $n\cdot n\cdot(n+2)$ is a product of three odd integers. Exercise 10 on page 162 implies that the product is odd.

ii. Since n is odd, there is an integer, k, such that $n = 2k+1$. Thus, $n^3+2n^2 = (2k+1)^3+2(2k+1)^2 = (2k+3)\cdot(2k+1)^2$. This is a product of three odd integers, so it is also odd (see the previous direct proof).

(b) An indirect proof seeks a proof of the assertion: let $n \in \mathbb{Z}$ with $n^3 + 2n^2$ even. Then n is even. To establish this claim, assume that $n^3 + 2n^2$ is even. Then there exists an integer, k, with $n^3 + 2n^2 = 2k$. This is equivalent to $n^3 = 2(k - n^2)$. The right-hand side is divisible by the prime, 2, so the left-hand side must also be divisible by 2. The prime divisibility property (Proposition 3.39) implies that 2 divides n and so n is even.

(c) Suppose that n is odd, but $n^3 + 2n^2$ is even. Then there exist integers, k and m, such that $n = 2k+1$ and $n^3+2n^2 = 2m$. Thus, $(2k+1)^3+2(2k+1)^2 = 2m$. This simplifies to $(2k+3)\cdot(2k+1)^2 = 2m$. The right-hand side is divisible by the prime, 2, so the left-hand side must also be divisible by 2. The prime divisibility property (Proposition 3.39) implies that 2 divides one of the three factors on the left-hand side. But each of those factors is odd, a contradiction. The only way to resolve the contradiction is to assume that when n is odd, $n^3 + 2n^2$ is also odd.