Elementary Number Theory by Underwood Dudley: Notes and Problem Solutions

Kedar Mhaswade

March 12, 2025

Abstract

This document contains the author's notes and solutions to problems from Underwood Dudley's [[1]] accessible introduction to Number Theory.

In the *Preface*, Dudley writes, "Number Theory problems can be difficult because inspiration is sometimes necessary to find a solution, and inspiration cannot be had to order. A student should not expect to be able to conquer all of the problems and should not feel discouraged if some are baffling. There is benefit in trying to solve problems whether a solution is found or not."

We have all experienced the frustration and exaltation of solving problems. And, in arithmetic–the queen of mathematics–there is no dearth of beautiful and difficult problems. We should keep trying as long as doing so calmly feels worth the effort. Destructive perfectionism is not needed. The author undertook this project almost purely as a labor of love[1].

Every theorem in the book and its proof are provided. A table of theorems (proved or researched) is compiled here [A].

[1] He also wanted to become a better programmer, but before he could solve the amazing *Project Euler* problems a bit more efficiently, he wanted to feel more comfortable with arithmetic!

Contents

Chapter 1

Integers

Note: **A roman letter in italics, like, for example, p, denotes an integer, unless specified otherwise.**

Definition (Least-Integer Principle)**.** A nonempty finite set of integers contains a *smallest element.*

Definition (Divides)**.** We say "a divides b" and write $a \mid b$ if and only if there is an integer d such that $ad = b$.

Thus, $a \mid b \iff \exists d \in \mathbb{Z}$ such that $ad = b, a, b \in \mathbb{N}$

A few lemmas follow:

Lemma 1.1. *If $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.*

Lemma 1.2. *If $d \mid a_1, d \mid a_2, \cdots, d \mid a_n$, then $d \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n)$.*

Definition (GCD)**.** We say d is the "greatest common divisor" of a and b (not both zero) and write "$d = \gcd(a, b)$" if and only if

1. $d \mid a$ and $d \mid b$, and
2. ($c \mid a$ and $c \mid b$) $\implies c \leq d$

It follows that $\gcd(a, b) \geq 1$.

Theorem 1.1. *If* $\gcd(a, b) = d$, *then* $\gcd(a/d, b/d) = 1$.

Proof. We use proof by contradiction.

If $\gcd(a, b) = d$, then $\exists p, q \in \mathbb{Z}$ such that

$$a = pd \implies a/d = p \tag{1.1}$$

$$b = qd \implies b/d = q \tag{1.2}$$

From definition[1], it follows that the GCD of any two natural numbers is greater than or equal to 1.

Let us assume that $\gcd(p, q) = m > 1$.

It then follows that $p = mx, q = my$ for some integers x, y.

From equations (1.1) and (1.2), we get:

$$a = mxd$$

and

$$b = myd$$

Then, $\gcd(a, b) = md$. Since $m > 1$, $\gcd(a, b) > d$.

This is a contradiction because we had $\gcd(a, b) = d$. Therefore, our assumption $\gcd(p, q) = m > 1$ is incorrect and we must have $\gcd(p, q) = \gcd(a/d, b/d) = 1$. ■

Definition (Relatively Prime)**.** We say that a and b are *relatively prime* if and only if $\gcd(a, b) = 1$.

Theorem 1.2. *Given positive integers a and b, there exist two unique integers q and $r, 0 \leq r < b$ such that*

$$a = bq + r$$

Chapter 2

Project Details

Describe important project steps, e.g., the rationale of the chosen architecture or technology stack, design decisions, algorithms used, interesting challenges faced on the way, lessons learned etc.

Chapter 3

System Documentation

Give a well-structured description of the architecture and the technical design of your implementation with sufficient granularity to enable an external person to continue working on the project.

Chapter 4

Summary

Give a concise (and honest) summary of what has been accomplished and what not. Point out issues that may warrant further investigation.

Appendix A

Table of Theorems

Table A.1: Theorems in the Book.

Begin List of Theorems		
Theorem	Chapter/Theorem	Notes
Theorem [1.1]	Chapter 1 Theorem 1	Regarding $\gcd(a/d, b/d)$.
End List of Theorems		

References

[1] Underwood Dudley. *Elementary Number Theory*. 2nd ed. Dover Publications, 2008 (cit. on p. 1).

[2] Nicholas J. Higham. *Handbook of Writing for the Mathematical Sciences*. 3rd ed. Philadelphia: Society for Industrial and Applied Mathematics (SIAM), 2020. URL: https://nhigham.com/handbook-of-writing-for-the-mathematical-sciences/.