Elementary Number Theory by Underwood Dudley: Notes and Problem Solutions

Kedar Mhaswade

March 13, 2025

Abstract

This document contains the author's notes and solutions to problems from Underwood Dudley's [[2]] 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 and brings joy. Destructive perfectionism is not needed. The author undertook this project almost purely as a labor of love[1].

Many a theorem (and lemma) in the book and its proof are provided. Attempt has been made to provide original (author's own) proofs (not verified by others). We mention it if a proof is reproduced verbatim from the book. Author's own proofs attempt to demonstrate an audacious, yet humble, renaissance attitude in the spirit of excellent collections like [[4]] and [[1]]. Occasionally the author complements the beautifully austere nature of mathematics with modest emotional narratives.

A table of theorems (proved or researched) is compiled here [A]. We hope that the compilation proves valuable to readers.

[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*

$$a = bq + r$$

Proof. We first prove the existence of integers, q, r by cases. For positive integers a and b there are three possibilities:

1. $a < b$

   Since $a = b \cdot 0 + a$, we get $q = 0$ and $r = a$ as the two integers.

2. $a = b$

   Since $a = b = b \cdot 1 + 0$, we get $q = 1$ and $r = 0$ as the two integers.

3. $a > b$

   This means that b can be subtracted $q \geq 1$ times from a for the result of the subtraction $(a - q \cdot b)$ to remain non negative. The result would be negative if we subtracted b once more (that is, $q + 1$ times in all) from a. The result of the subtraction, $a - q \cdot b$, which we denote as r, must then be a positive integer less than b, because otherwise we could subtract b at least once more.

We have proved the existence of the two integers q and r and demonstrated how to find them in all the cases.

The above proof of existence describes a precise, deterministic procedure to find non negative integers q and r for any positive integers a and b. However, we need to prove that the pair is unique. We prove uniqueness by contradiction.

Let $q_1 \neq q$ and $r_1 \neq r$ be *another pair of non negative integers* produced by the procedure above. We have

$$a = bq + r \tag{1.3}$$

and

$$a = bq_1 + r_1 \tag{1.4}$$

From the existence proof above, $r < b$ and $r_1 < b$.

It follows from equations (1.4) and (1.3) that

$$b \cdot (q - q_1) = r_1 - r$$

From the definition (1) it then follows that $b \mid (r_1 - r)$. However, $r_1 < b \implies r_1 - r < b - r \implies r_1 - r < b$. This is a contradiction unless $r_1 - r = 0$, or $r_1 = r$. If $r_1 = r$, $q_1 = q$ proving uniqueness. ■

We call q the *quotient* and r the *remainder*. Theorem [1.2] is called an "algorithm" because it entails a precise procedure to calculate non negative integers q and r for integers a and b (not both zero). The book correctly mentions that the theorem also holds when either a or b (or both) are negative. However, when negative numbers are involved, additional care must be exercised.

Consider, for example, $a = 5$ and $b = -2$. Then, $a = b \cdot (-3) + (-1)$ giving $q = -3$ and $r = -1$. Moreover, $a = b \cdot (-2) + 1$ giving $q = -2$ and $r = 1$. Doesn't the uniqueness of division algorithm hold? For $0 \leq r$ we must reject $r = -1$, whereas for $r < b$ we must reject both $r = 1$ and $r = -1$. If we change the constraint on r to $0 \leq r < -b$ however, we allow the second case and achieve uniqueness.

The division algorithm is most commonly applied to non negative integers.

Lemma 1.3. *If* $a = bq + r$ *where* $0 \leq r < b$, *then* $\gcd(a, b) = \gcd(b, r)$

Proof. We give a straightforward deductive proof.

Consider a common divisor (not necessarily the greatest) c of a and b. Then, by definition,

$$a = c \cdot m_1$$

$$b = c \cdot m_2$$

Then, $a = b \cdot q + r \implies c \cdot m_1 = c \cdot m_2 \cdot q + r$.

$\therefore r = c \cdot (m_1 - q \cdot m_2) \implies c \mid r$

This means c is a divisor of r. The reasoning applies to all common divisors of a and b, and, therefore, it also applies to the greatest of them all–the $\gcd(a, b) = g_{ab}$.

We proved that g_{ab} is a divisor of r. We still need to prove that g_{ab} equals $\gcd(b, r) = g_{br}$.

Let us use contradiction to prove that. Let us *assume* $g_{br} > g_{ab}$. This implies that g_{br} divides b and r but does *not* divide a.

However, $a = bq + r \implies \exists x, y \in \mathbb{N} \mid a = (g_{br} \cdot x)q + g_{br} \cdot y$

$\therefore a = g_{br}(qx + y) \implies g_{br} \mid a$—a contradiction owing to our faulty assumption that $g_{br} > g_{ab}$ does not divide a.

There is no such $g_{br} > g_{ab}$. Therefore, $\gcd(a, b) = \gcd(b, r)$. ■

Reflection 1. *This–a divisor of a and b must be a divisor of r– is one of Euclid's remarkable observations. The author never solemnly paused in its admiration in grade school. Perhaps that was because loving numbers for the sake of it did not cross his mind then.*

The author's obsession for numbers is still rudimentary, but the above proof that he wrote down using a paper and a pen on an airplane gave him ineffable joy; he understood Euclid's argument better and, in that moment, like Piaget [3] observed, he momentarily became Euclid*!*

Greeks showed signs of computational excellence when finding $\gcd(a, b)$. They used the above lemma [1.3] to confidently reduce the size of the problem: to find the gcd of two numbers($a \geq b$ and b), find the remainder r by applying the division algorithm to

a, b and then the gcd of two smaller numbers($b > r$ and r)[1]! They, unlike we did in grade school, never listed all the divisors of both the numbers and chose the largest of the common ones.

We define the 'remainder operation' on two integers a and b (denoted '$a \mod b$') to return the remainder by applying the division algorithm [1.2] to a and b.

Dudley gives an *iterative* procedure for Euclid's gcd algorithm next. However, we give an arguably more expressive recursive algorithm that uses a corollary that the gcd of a non negative number a and 0 is a.

Algorithm 1.1: Euclid's $\gcd(a, b)$ Algorithm

```
if b = 0 then
    return a
else
    return gcd(b, a mod b)
```

[1] $\gcd(a, b)$ also equals $\gcd(a, r)$, but their choice–$\gcd(b, r)$–was computationally more efficient

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 $\gcd(a/d, b/d)$.
Theorem [1.2]	Chapter 1 Theorem 2	The Division Algorithm.
End List of Theorems		

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from THE Book*. 6th ed. Berlin: Springer, 2018. DOI: 10.1007/978-3-662-57265-8 (cit. on p. 1).

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

[3] Jean Piaget and George-Ann Roberts (English translator). *To Understand Is To Invent. The Future of Education*. New York: Viking Press, Inc., 1974 (cit. on p. 5).

[4] Sergei Tabachnikov. "Proofs (Not) From The Book". *The Mathematical Intelligencer* 36.2 (2014), pp. 9–14. DOI: 10.1007/s00283-013-9424-2 (cit. on p. 1).