Elementary Number Theory by Underwood Dudley: Notes and Problem Solutions

Kedar Mhaswade

April 16, 2025

Abstract

THIS is an objective, yet personal, narrative of the author's odyssey in the enchanted land of numbers. It contains his notes and solutions to problems from Professor Underwood Dudley's [3] accessible introduction to Number Theory.

There is one issue with almost all books of rigorous mathematics (of the definition-theorem-lemma-proof style): they present mathematics in the *finished* form[1]. Proofs, however clear and lucid, are presented as if they are spoken by an omniscient Oracle. It's hard to imagine real humans doing mathematics this way from scratch. Countless hours need be spent on arriving at the presentable form. The author knew that and realized it again as he was writing his proofs[2]. He has attempted to point that out where possible. Running into dead ends and admitting it may disrupt the flow of normal reading (for reading mathematics is also like reading a careful disposition), but it may be reassuring especially to a beginning (but interested and, for the lack of a better word, intelligent) reader who is assumed author's companion. Delving too much into detours may ruin an otherwise readable travelogue. The author strives to seek a balance. *Failed* proofs appear in this text with ? instead of the QED symbol ■.

In the *Preface* of his book 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

[1] We assume that such a book is free from any egregious errors, typos etc.

[2] Almost all the proofs were first attempted with a pen on a lot of paper and then typeset. We live in an affluent society; the great mathematician Srinivasa Ramanujan didn't even have access to enough paper.

project almost purely as a labor of love[3]. Doing mathematics (even established, not involving "active mathematical research") for the sake of it is sufficient because Professor Dudley has compellingly argued elsewhere (cf. [4]) that mathematics may not be necessary to find jobs, but it *is* sufficient (to live a contented life).

Many a theorem (and lemma) in the book and its proof is 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 [10] and [1]. Occasionally the author complements the beautifully austere nature of mathematics with modest emotional narratives (in the form of sidebars titled "Reflection").

A table of theorems (proved or researched) is compiled [See A]. We hope that the compilation proves valuable to readers. Readers interested only in problems and their solutions should look for the sections named "Problems" such as [1]. Not all problems are equally exhilarating and solving every problem isn't exactly fun (See [7]).

Readable and flawless mathematical typesetting is hard. It's ironic that the epitome of exact sciences breeds a degree of inexactness in notation. Like in literature, meaning sometimes depends on context not captured in notation. And yet, an encyclopedic treatment of notation at the beginning of a work like this tends to bore readers[4]. Here too, a balance needs to be sought. A few conventions are therefore in order:

- A roman letter in italics, like, for example, p, denotes an integer, unless specified otherwise.
- The so-called `\cdot`: $\cdot$ to denote multiplication is sometimes omitted. Thus, ab is equivalent (and often even preferred and ubiquitous, thanks to Euler!) to $a \cdot b$.

[3] 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!

[4] What disappointments them even more are typos and errors.

Contents

Chapter 1

Integers

Definition 1 (Least-Integer Principle)**.** A nonempty finite set of integers contains a *smallest element.*

An equivalent definition concerns the greatest element of a nonempty finite set.
Definition 2 (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 (straightforward proofs are omitted):
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 3 (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[3], 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 4 (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 (2) 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 [8] 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 find 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.

Definition 5 (The Remainder Operation)**.** 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)
```

This can also be expressed inductively using *cases*:

$$\gcd(a, b) = \begin{cases} a & \text{if } b = 0, \\ \gcd(b, a \mod b) & \text{otherwise} \end{cases}$$

We provide proofs of *correctness* of algorithms. For Algorithm [1.1], if $b = 0$, the algorithm immediately terminates, producing the correct result (a). If $b \neq 0$, then division algorithm applies and we find the gcd of b and a number less than b (because the remainder, r, is such that $0 \leq r < b$). The process continues till the second argument becomes 0. Since b is finite and the second argument is guaranteed to reduce by at least 1 every time the division algorithm applies. Such reduction must stop when the remainder becomes 0 and the algorithm terminates and returns the first argument, a, the gcd of the original numbers.

Reflection 2. *A few thoughts occurred to the author:*

1. *Is a* descent *through Euclid's* gcd *algorithm like* $(a, b) \to (b, b-1) \to (b-1, b-2) \cdots \to (1, 0)$ *possible? When does the algorithm perform the best and worst?*
2. *Are any two consecutive Fibonacci numbers relatively prime? Does an invo-*

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

cation of $\gcd(F_{n+1}, F_n)$ *always result in finding gcd of the lower Fibonacci numbers*[a].

[a] *Preliminary* tests seem to suggest so...

Theorem 1.3. *If* $\gcd(a, b) = d$, *then* $\exists x, y \in \mathbb{Z} \mid ax + by = d$.

(Informally: $\gcd(a, b)$ *can be expressed as a linear combination of* a *and* b *with integer coefficients.)*

Proof. We give an algebraic proof.

$$d = \gcd(a, b) \implies d \mid a \implies a = m_1 \cdot d; m_1 \in \mathbb{N}$$
$$d = \gcd(a, b) \implies d \mid b \implies b = m_2 \cdot d; m_2 \in \mathbb{N}$$

It follows that

$$a \cdot m_2 = b \cdot m_1$$
$$\therefore a \cdot m_2 + d = b \cdot m_1 + d$$
$$\therefore a \cdot (m_2 - 1) + a + d = b \cdot m_1 + d$$
$$\therefore a \cdot (m_2 - 1) + m_1 \cdot d + d = b \cdot m_1 + d$$

?

Reflection 3. *The author intended to achieve a proof through a simple algebraic manipulation that was not to be! His intention was to determine a deterministic procedure to express* $gcd(a, b)$ *as a linear combination* $ax + by$ *of the integers* a *and* b. *But he realized that such a manipulation was not as straightforward as he initially imangined.*

He also realized that the theorem holds only for the gcd *and not for any other common divisor. For example, for* 42 *and* 18, *whose* gcd *is 6, the theorem states that* $\exists x, y \mid 42x + 18y = 6$; *this couldn't be extended to another common divisor of* 42 *and* 18 *like* 1 *or* 3 *because we immediately run into a contradiction like* $42x + 18y = 1$ *or* $42x + 18y = 3$ *(the left hand side is an even number and the right hand side is an odd number).*

Therefore, $\gcd(a, b)$ *represents something more about* a *and* b *than what their other common divisors do.*

To prove [1.3], Dudley hints at *working backwards* from the descent of numbers a and b in a continued application of the division algorithm [1.2] as long as b remains nonzero. We attempt that below.

But first, let's consider an example: Find the gcd of $a = 222$ and $b = 60$.

$$
\begin{aligned}
222 &= \textcircled{60} \times 3 + \textcircled{42} \\
60 &= \textcircled{42} \times 1 + \textcircled{18} \\
42 &= \textcircled{18} \times 2 + \textcircled{6} \\
18 &= \textcircled{6} \times 3 + \textcircled{0}
\end{aligned}
$$

$\therefore \gcd(222, 60) = 6.$

Working backwards through the descent (and eliminating 42 and 18 in the process) we get:

$$
\begin{aligned}
6 &= 42 - \textcircled{18} \times 2 \\
6 &= 42 - (60 - 42 \times 1) \times 2 = \textcircled{42} \times 3 - 60 \times 2 \\
6 &= (222 - 60 \times 3) \times 3 - 60 \times 2 = 222 \times 3 - 60 \times 11 \\
6 &= 222 \cdot 3 + 60 \cdot (-11)
\end{aligned}
$$

$\therefore x = 3, y = -11$

Proof. Let's apply the division algorithm [1.2] continuously, starting with a and b. We know from above that this descent must eventually result in the application of the division algorithm to some integer and 0 yielding the $\gcd(a, b)$.

Let $r_n = 0$, then $r_{n-1} = d = \gcd(a, b)$.

$$
\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
r_2 &= r_3 q_4 + r_4 \\
&\vdots \\
r_{n-4} &= r_{n-3} q_{n-2} + r_{n-2} \\
r_{n-3} &= r_{n-2} q_{n-1} + d \\
r_{n-2} &= d q_n \ (r_n = 0)
\end{aligned}
$$

We start with an expression for the gcd and work backwards to eliminate one number (from the step above) at a time. Every eliminated number yields a linear combination of remaining two numbers. This process evetually stops when a and b remain. Since every expression is a linear combination of integers starting with r_{n-3} and r_{n-2} which get eliminated in steps.

Need to make the proof tighter. ■

Theorem [1.3] that $\exists x, y \in \mathbb{N} \mid ax + by = \gcd(a, b)$ is called Bézout's Identity.

Are x and y thus found unique for the given a and b?

No. For example, for $a = 42$ and $b = 18$:

$$\begin{aligned} 42 \times 1 + 18 \times (-2) = 6 &\implies (x, y) = (1, -2) \\ 42 \times (-2) + 18 \times (5) = 6 &\implies (x, y) = (-2, 5) \\ 42 \times 4 + 18 \times (-9) = 6 &\implies (x, y) = (4, -9) \\ &\vdots \end{aligned}$$

Is this (working backwards through the descent) the only way to find x and y for the given a and b?

Dudley asserts that we can devise another method to determine x and y. Let's see.

The equation $ax + by = d \mid a, b, x, y \in \mathbb{Z}$ is the so-called *Linear Diophantine Equation* [5] and is a special case of the general Diophantine equation. Solving such equations for (integer) solutions for given a, b has a rich history. See [2] for an accessible and fascinating introduction.

We have three corollaries from Bézout's Identity.
Corollary 1.3.1. *If $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$.*

(Informally: If an integer d divides the product of two integers a and b and if d and one of a and b are relatively prime, then the other must be a multiple of d.)

Proof. We give a straightforward proof[2] based on Bézout's Identity (Theorem 1.3).

Bézout's Identity when applied to the fact that d and a are relatively prime (i.e. $\gcd(d, a) = 1$) gives us

$$\exists x, y \in \mathbb{Z} \mid dx + ay = 1$$

$$\therefore d \cdot b \cdot x + a \cdot b \cdot y = b$$

But, $d \mid a \cdot b \implies a \cdot b = m_1 \cdot d,\ m_1 \in \mathbb{N}$

$$\therefore d \cdot b \cdot x + m_1 \cdot d \cdot y = b$$

and

$$d \cdot (bx + m_1 y) = b$$

This means $d \mid b$ because $bx + m_1 y$ is an integer since the set of integers is closed under addition and multiplication. ■

It's crucial that d and a are relatively prime for the corollary [1.3.1] to hold.
Corollary 1.3.2. *Let $\gcd(a, b) = d$, and suppose $c \mid a$ and $c \mid b$. Then $c \mid d$.*

(Informally: A common divisor of two integers is a divisor of their gcd*.)*

[2] Of course, other proofs, for example, one based on prime factorization of integers, are possible.

Proof. We give a rather straightforward proof based on Bézout's Identity (Theorem 1.3).

$$\exists x, y \in \mathbb{Z} \mid ax + by = d \tag{1.5}$$

Also,

$$c \mid a \implies \exists m_1 \in \mathbb{N} \mid a = m_1 \cdot c$$

and

$$c \mid b \implies \exists m_2 \in \mathbb{N} \mid b = m_2 \cdot c$$

Then, it follows from equation (1.5) that

$$m_1 cx + m_2 cy = d$$

and

$$c(m_1 x + m_2 y) = d \implies c \mid d$$

■

Corollary 1.3.3. *If $a \mid m$, $b \mid m$, and $\gcd(a, b) = 1$, then $ab \mid m$.*

(Informally: The product of two relatively prime divisors of an integer is its divisor.)

Proof. Once again we give a straightforward proof based on Bézout's Identity (Theorem 1.3). We have

$$\begin{aligned} a \mid m &\implies m = c_1 \cdot a, \\ b \mid m &\implies m = c_2 \cdot b, \\ \therefore m^2 &= c_1 c_2 ab, \end{aligned} \tag{1.6}$$

and

$$\begin{aligned} \gcd(a, b) = 1 &\implies \exists x, y \in \mathbb{Z} \mid ax + by = 1 \\ \therefore axc_1 c_2 + byc_1 c_2 &= c_1 c_2 \end{aligned}$$

From which, it follows that

$$mxc_2 + myc_1 = c_1 c_2 \implies mk = c_1 c_2 \quad (\because xc_2 + yc_1 = k) \tag{1.7}$$

From equations (1.6) and (1.7)

$$m^2 = mkab \implies m = kab \implies ab \mid m$$

■

Problems

We solve a number of problems below.

1. Calculate $\gcd(314, 159), \gcd(4144, 7696)$
We apply Euclid's gcd Algorithm (1.1).

$$\begin{aligned} 314 &= 159 \times 1 + 155 \\ 159 &= 155 \times 1 + 4 \\ 155 &= 4 \times 38 + 3 \\ 4 &= 3 \times 1 + 1 \\ 3 &= 1 \times 3 + 0 \end{aligned}$$

$\therefore \gcd(314, 159) = 1$.

$$\begin{aligned} 4144 &= 7696 \times 0 + 4144 \\ 7696 &= 4144 \times 1 + 3552 \\ 4144 &= 3552 \times 1 + 592 \\ 3552 &= 592 \times 6 + 0 \end{aligned}$$

$\therefore \gcd(4144, 7696) = 592$.

2. Calculate $\gcd(3141, 1592), \gcd(10001, 100083)$
Although nothing is exactly useless, some things can be boring and so we omit some details!

$$\begin{aligned} 3141 &= 1592 \times 1 + 1549 \\ 1592 &= 1549 \times 1 + 43 \\ &\vdots \end{aligned}$$

$\therefore \gcd(3141, 1592) = 1$ and $\gcd(10001, 100083) = 73$.

3. Find $x, y \in \mathbb{Z} \mid 314x + 159y = 1$.

We have established that $\gcd(314, 159) = 1$ above (1.), without which there would be no integral x, y that satisfy this linear Diophantine equation.

One way to get the desired solution is to work backwards through the descent:

$$\begin{aligned}
4 &= (155 - 4 \times 38) \times 1 + \boxed{1} \\
4 \times 39 - 155 \times 1 &= \boxed{1} \\
(159 - 155) \times 39 - 155 \times 1 &= \boxed{1} \\
159 \times 39 - 155 \times 40 &= \boxed{1} \\
159 \times 39 - (314 - 159) \times 40 &= \boxed{1} \\
314 \times (-40) + 159 \times (79) &= \boxed{1}
\end{aligned}$$

$\therefore x = -40, y = 79$ is a solution to the linear Diophantine equation $314x+159y = 1$.

4. Find $x, y \in \mathbb{Z} \mid 4144x + 7696y = 592$.

This 'problem' is left as an exercise to readers.

5. If $N = abc + 1$, prove that $\gcd(N, a) = \gcd(N, b) = \gcd(N, c) = 1$.

Proof. We use the division algorithm [1.2].

$$\because N = a(bc) + 1 \therefore \gcd(N, a) = \gcd(a, 1)$$

And since $1 \mid x \forall x \in \mathbb{Z}, \gcd(x, 1) = 1$.

$\therefore 1 = \gcd(a, 1) = \gcd(N, a)$.

Similar argument can be used to prove relative-primality of N, b and N, c. ■

6. Find *two different*[3] solutions of $299x + 247y = 13$.

Let's first establish that at least one (integral) solution exists. Because of [1.3], our job is easier:

$$\begin{aligned}
299 &= \boxed{247} \times 1 + \boxed{52} \\
247 &= \boxed{52} \times 4 + \boxed{39} \\
52 &= \boxed{39} \times 1 + \boxed{13} \\
39 &= \boxed{13} \times 3 + 0
\end{aligned}$$

$\because \gcd(299, 247) = 13 \therefore \exists x, y \in \mathbb{Z} \mid 299x + 247y = 13$.

Working backwards through a familiar descent we get: $x = 5, y = -6$ as one solution.

Reflection 4. *Interestingly, Dudley asks for two solutions! In a way, he's nudging us to be creative! He has said somewhere that we'll learn about finding different solutions to the linear Diophantine equation given by Bézout's Identity. However, we can try on our own.*

Are other corollaries or lemmas likely to help us?

[3] Perhaps for emphasis; "two" implies "two different".

Does another solution exist? How many solutions are there?
These are all hard questions. They express the difficulty of doing mathematics and of developing an inductive thinking, however limited in influence. For example, if we are unfamiliar with the "theory of linear Diophantine equations" what makes us take a leap of faith[a] *that another solution exists?*
We believe that try sensibly we must. We may be in dark. However, unless we, guided by established knowledge and fueled by imagination, explore the mysterious, how might we uncover new knowledge(even at a personal level)? A "solved problem" is unsolved for us until we solve it (first somehow, then by application of an established theory or technique).

[a]The author borrows this term from a lucid book, *Thinking Recursively*, by Eric Roberts [9], which introduces a "recursive leap of faith".

$$297x + 247y = 13 \implies 13(23x + 19y) = 13 \implies 23x + 19y = 1$$

The above implies that *every* solution of $23x + 19y = 1$ is a solution of $297x + 247y = 13$ and vice versa. Therefore, $(x, y) = (5, -6)$ is a solution[4] of $23x+19y = 1$. Does $23x + 19y = 1$ have *another* solution?

It's easier to try with smaller numbers. Any generalization starts with some concrete experiments. Consider an experiment tabularized below:

x	y	$23x + 19y$	Multiples of $(23 - 19)$ that yield 1 from $23x + 19y$
1	-1	4	–
1	-2	-15	$4, \text{-15} + (23 - 19) \times 4 = 1$
1	-3	-34	–
1	-4	-53	–
1	-5	-72	–
1	-6	-91	$23, \text{-91} + (23 - 19) \times 23 = 1$
⋮	⋮	⋮	⋮
1	-10	-167	$42, \text{-167} + (23 - 19) \times 42 = 1$

Table 1.1: How $23x + 19y$ Changes

Consider the first row in the Table 1.1. We observe that since $23(1) + 19(-2) = -15$, $23(1) + 19(-2) + (23 - 19)4 = 23(5) + 19(-6)$ yields 1. Only if $23x + 19y = 4k - 1, k \in \mathbb{Z}$, then we can expect $23x + 19y + k(23 - 19) = 23(k - x) + 19(y - k)$ to yield 1.

That—$x = 5$ and $y = -6$—was our first solution. Values of x and y for which $23x + 19y \neq 4k - 1$ are not of our interest. Now consider $x = 1$ and $y = -6$. Since $23(1)+19(-6) = -91$, $23(1)+19(-6)+(23-19)23 = 23(24)+19(-29)$ also yields

[4]The familiar ascent through the repeated application of the division algorithm yields the same solution.

1. Therefore, $x = 24$ and $y = -29$ is another solution. Yet another is $x = 43$ and $y = -52$.

Perhaps there is some arithmetic progression lurking here, because the next solution $(62, -75)$ will be given by the row for $x = 1, y = -14$.

This process can continue. Infinitely many solutions starting with $(5, -6)$ are possible. If (p, q) is a solution, then $(p + 19k, q - 23k)$ is also a solution of the linear Diophantine equations $23x + 19y = 1$ and $299x + 247y = 13$:

$$\begin{aligned}&(5, -6)\\&(24, -29)\\&(43, -52)\\&(62, -75)\\&\vdots\end{aligned}$$

Reflection 5. *Did we get lucky there?*
Perhaps we did.
We cannot escape a feeling that we are close to a useful generalization, a slice of a theory! We will carry that positive feeling along but curb our enthusiasm.

7. Prove that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.

Proof. We give a straightforward proof.

$$a \mid b \implies \exists c \in \mathbb{Z} \mid b = ca$$

and

$$b \mid a \implies \exists d \in \mathbb{Z} \mid a = db$$

It follows that

$$ab = cdab$$

If $a \neq 0, b \neq 0$, then

$$cd = 1$$

This is possible only if $c = 1, d = 1$ or $c = -1, d = -1$. It then follows that either $a = b$ or $b = -a$ i.e. $a = -b$. ■

8. Prove that if $a \mid b$ and $a > 0$, then $\gcd(a, b) = a$. TBD

9. Prove that $\gcd(\gcd(a, b), b) = \gcd(a, b)$.

Proof. Here's a straightforward proof.

Consider all the *common* divisors of a and b listed in an ascending order:

$$d_1 > d_2 > \cdots > d_n$$

Then, by definition, $d_1 = 1$ and $d_n = \gcd(a, b)$.

Again, by definition, $d_n \mid b$ and, trivially, $d_n \mid d_n$. Therefore, $d_n = \gcd(a, b)$ divides b and $\gcd(a, b)$. There is no greater common divisor. Therefore, $\gcd(\gcd(a, b), b) = \gcd(a, b)$.

■

10. (a) Prove that $\gcd(n, n+1) = 1 \forall n > 0$.

Proof. $\because \gcd(0, a), a > 0 = a, \therefore \gcd(0, 1) = 1$.

We argue based on the fact for $a, b \in \mathbb{Z}, ab = 1 \implies a = 1, b = 1, \text{or } a = -1, b = -1$.

Let $\gcd(n, n+1) = d$.

Then, $\exists p, q \in \mathbb{Z}$ such that

$$n = pd$$

$$n + 1 = qd$$

It follows that

$$(q - p)d = 1$$

Therefore (also since $q - p \in \mathbb{Z}$), either

$$(q - p) = 1, d = 1$$

, or

$$(q - p) = -1, d = -1$$

$$\because d > 0, \therefore d = 1, q - p = 1$$

$\therefore \gcd(n, n+1) = 1 \forall n \geq 0$.

■

Proof. We give an alternative proof using the division algorithm[5].

$$\gcd(n, n+1) = \gcd(n+1, n)$$

But $n + 1 = \textcircled{n} \cdot 1 + \textcircled{1}$.

$$\therefore \gcd(n+1, n) = \gcd(n, 1) = 1$$

■

(b) If $n > 0$, what can $\gcd(n, n+2)$ be?

It has got to be either 0 or 1.

Proof. We argue as in the above (alternative) proof (**10**.a).

$$n = \textcircled{n+2} \cdot 0 + \textcircled{n}$$

$$n + 2 = \textcircled{n} \cdot 1 + \textcircled{2}$$

$\therefore \gcd(n, n+2) = \gcd(n, 2)$.

$$\gcd(n, 2) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 2 & \text{otherwise} \end{cases}$$

■

[5] It occurred to the author at a hospital waiting room.

11. (a) Prove that $\gcd(k, n+k) = 1$ if and only if $\gcd(k, n) = 1$.
TBD

(b) Is it true that $\gcd(k, n+k) = d$ if and only if $\gcd(k, n) = d$?
TBD

12. Prove: If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
TBD

13. Prove: If $d \mid a$ and $d \mid b$, then $d^2 \mid ab$.
This 'problem' is left as an exercise to readers.

14. Prove: If $c \mid ab$ and $\gcd(c, a) = d$, then $c \mid db$.

Proof. We use straightforward manipulation based on Bézout's Identity (1.3).

$$c \mid ab \implies cp = ab$$

and

$$\gcd(c, a) = d \implies cx + by = d$$

(where $p, x, y \in \mathbb{Z}$).

$$\therefore cxb + ayb = db$$
$$\because ab = cp \therefore cxb + cpy = db \implies c(bx + py) = db$$
$$\because bx + py \in \mathbb{Z} \therefore c \mid db$$

■

Reflection 6. *Is proving theorems of Number Theory about such numerical manipulation?*
No, not for the most part, for which more creativity is essential. But such problems (that seem to have been constructed based on the more fundamental theorems like Bézout's Identity) are like exercises. Setting beautiful "problems" in books (or for math olympiads) is a also a matter of immense creativity. Problems like the above which are not exactly "fun" are aimed at giving us practice of proving (which is also needed). Of course, the author is painfully aware of the fact that writing correct[a] *and readable proofs is an art that many take time to become comfortable with.*

[a] Yes, there's such a thing as a "bogus proof"!

15. (a) If $x^2 + ax + b = 0$ has an integer root, show that it divides b.

Proof. We will use the theory of quadratic equations and combine it with what we learned in this chapter. We assume $a, b \in \mathbb{Z}$.
From the quadratic formula, the roots of the given equation,

$$x_{1,2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

We denote the *integral* root by c.

$$x_{1,2} = c \in \mathbb{Z} \implies \frac{-a \pm \sqrt{a^2 - 4b}}{2} = c$$

It then follows that

$$a^2 - 4b = (a + 2c)^2$$
$$\therefore -b = ac + c^2 \implies c \mid b$$

■

(b) If $x^2 + ax + b = 0$ has a rational root, show that it is in fact an integer.
Proof. Let the rational root be denoted by $\frac{m}{n} \mid m, n \in \mathbb{Z}$.

$$\therefore \frac{m}{n} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$
$$\therefore (2m + an)^2 = n^2(a^2 - 4b)$$
$$\therefore 4m^2 + 4amn + \cancel{a^2n^2} = \cancel{a^2n^2} - 4bn^2$$
$$\therefore m^2 + amn + bn^2 = 0$$

We can treat this equation as a quadratic in m.

$$\therefore m = n\frac{-a \pm \sqrt{a^2 - 4b}}{2} \tag{1.8}$$

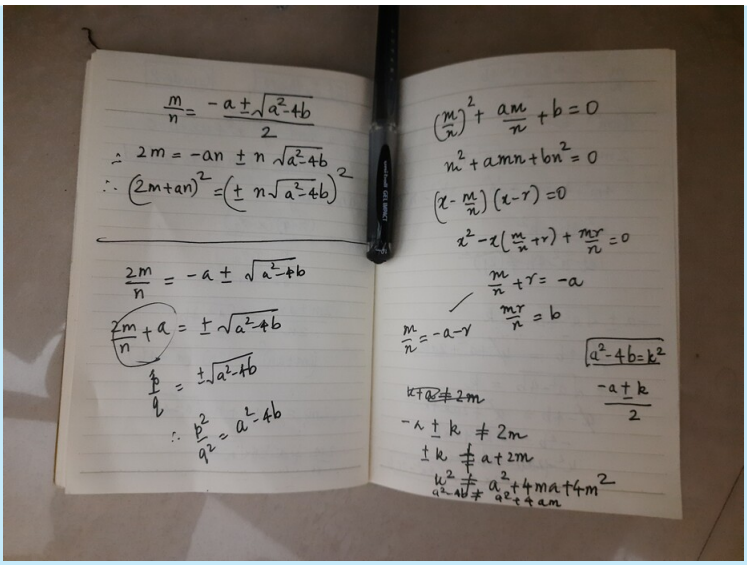
We shall show that the numerator $-a \pm \sqrt{a^2 - 4b}$ of the above fraction may not be odd because that leads to a contradiction.
Thus, we start with the assumption that the numerator (denoted by N) is odd: $\exists k \in \mathbb{Z} \mid N = 2k + 1$.

$$-a \pm \sqrt{a^2 - 4b} = 2k + 1$$
$$\therefore a^2 - 4b = ((2k + 1) + a)^2$$
$$\therefore \cancel{a^2} - 4b = (2k + 1)^2 + 2(2k + 1)a + \cancel{a^2}$$
$$\therefore -4b = 4k^2 + 4k + \textcircled{1} + 4ka + 2a$$

The left hand side of this equation is an even number and the right hand side odd. A contradiction!
Therefore, the numerator N in equation(1.8) must be even: $\exists k \in \mathbb{Z} \mid N = 2k$ which yields $m = n\frac{\cancel{2}k}{\cancel{2}} \implies m = kn \implies \frac{m}{n} = k$, an integer.

■

Reflection 7. *This was the last problem in the first chapter. The author was eager to "finish it off quickly." Although he succeeded in writing a satisfactory proof, it was neither quick nor without a struggle!*



A part (and only a part because there was a long pause before he wrote the quadratic equation (1.8)–how can that pause be meaningfully captured in this "finished text"?) of his struggle is captured herewith. Several ways were explored, many were abandoned. The author even doubted if he understands quadratic equations. Self-doubt reared its ugly head. But he persevered.

We all enjoy reading books of history, fiction, nonfiction, etc. and finish them in a few sittings. This author has, however, learned to be at peace with spending a few slow hours without any apparent 'gain' in the number of mathematical problems solved, proofs written, or pages of mathematics read. Progress in doing mathematics is slow and it is only good for our health that we accept its pace (or lack thereof). Keep calm and do math (slowly).

To be honest, however, "keeping calm" is only possible in the long shot or on the average (of time lived). If the author were secretly video shot during the time a satisfactory solution was not evident, a viewer (or the author himself, in retrospect) couldn't conclude that the protagonist was not agitated.

Chapter 2

Unique Factorization

Prime numbers have always fascinated us. See The Prime Pages [6] for everything about them.

Definition 6 (Prime Number[1])**.** A prime number is an integer greater than 1 that has no positive divisors other than 1 and itself.

Definition 7 (Composite Number[2])**.** A composite number is an integer greater than 1 that is not prime.

It is convenient to define 1 as neither prime or composite; we call 1 *unit*. Thus, every positive integer is either prime, composite, or unit.

The author verified (using online tools) that 170141183460469231731687303715884105727 is prime.

The aim of this chapter is to show that each positive integer can be represented uniquely as a product of primes. If two representations can be expressed as $p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_k^{n_k}$: p_i is prime and $n_i \in \mathbb{N}$, then they are *not* unique. Prime numbers can be used to build by multiplication the entire system of positive integers.

Lemma 2.1. *Every integer $n > 1$ is divisible by a prime.*

Proof. This proof is by Dudley.

Consider D, the set of divisors of n: $D = \{d : d \mid n, 1 < d < n\}$. Then, D is either empty or nonempty. If it is empty, then n is prime, by definition, and thus has a prime divisor, namely itself.

If it is nonempty, then the Least-Integer Principle (1) says D has a smallest element. Let's call it d. If d is composite, it has a divisor $dd : 1 < dd < d$. Then, from (1.2), $dd \mid n$. But that is impossible because d was the smallest divisor of n. Thus, d must be prime and n has a prime divisor, namely d.

In any case, n is divisible by a prime. ■

[1] We often use the word 'prime' as a noun; e.g., $2, 5, 7$ are the first three primes.

[2] We use 'composite' as a noun less frequently than we use 'prime' as a noun.

Lemma 2.2. *Every integer $n > 1$ can be written as a product of primes.*

Dudley gives a proof based on the above lemma [2.1].

Reflection 8. *Inductive proofs (which, according to some, are deductive proofs) can be tricky, but if we are careful, they are usually straightforward.*

Proof. We will give an inductive proof also based on that lemma.

Base Case Trivially, $2 = 2$. That is, 2 can nominally be written as a product of primes.

Inductive Hypothesis We assume that every integer $\{2, 3, 4, \ldots, k\}$ can be expressed as a product of primes. We call this proposition $P(k)$ and assume that it is `true`.

Inductive Step Here, we prove that if $P(k)$ is true, then $P(k+1)$ is also true.

Consider the number $k+1$. It is either prime or composite.

If it is prime, we are done. Nominally, $k+1 = k+1$, that is, $k+1$ can be expressed as a product of primes.

If, on the other hand, $k+1$ is composite, then, by definition, $\exists d \in \mathbb{N} : d \mid (k+1)$ where $d < k$ and the inductive hypothesis holds for d.

Let d be a product of r primes: $d = p_1 \times p_2 \times \cdots \times p_r$ and $\exists m \in \mathbb{N} : (k+1) = m \times d \implies (k+1) = m \times (p_1 \times p_2 \times \cdots \times p_r)$.

Similarly, $m < k$ is either prime, or, because of the inductive hypothesis, can be expressed as a product of primes. Since $k+1 = m \times d$, $k+1$ can be expressed as a product of primes. This makes the proposition $P(k+1)$ true.

We *assumed* that every integer up to k can be expressed as a product of primes and *showed* that $k+1$ can be so too. The domino effect thus applies to every integer without exception.

■

We now have a fundamental theorem and its elegant proof by Euclid.

Theorem 2.1. *There are infinitely many primes.*

Proof. We will prove the theorem by contradiction.

Let there be a finite number of primes represented by a finite set $P = \{p_1, p_2, p_3, \ldots, p_r\}$. Since this is a nonempty finite set, it has a greatest element (See definition [1]). Let the greatest element of P be p_r.

Consider the integer $N = p_1 \times p_2 \times p_3 \times \cdots \times p_r + 1$. N is, by definition, greater than all of the primes contained in P. Also, none of the prime numbers $p_i \in P$ divides N because $\forall p_i \in P, N \mod p_i = 1$ (See definition [5]).

If N is prime, then we have reached a contradiction because we found a prime not in P.

If N is composite, then there are two possibilities:

1. By lemma [2.1], every integer > 2 is divisible by a prime number and if P is the set of all the primes, such a prime must be a member of P. However, we just saw that N is not divisible by any of them: A contradiction!
2. By the same lemma [2.1], if there is a prime that divides N, then it must be a prime number not in P (or, in other words, a prime number $> p_r$): A contradiction again!

The source of all the contradictions above can be traced back to the faulty assumption that the set of prime numbers is finite.

Therefore, there are infinitely many prime numbers. ■

Reflection 9. *Thinking of a number $N = p_1 \times p_2 \times p_3 \times \cdots \times p_r + 1$—what a stroke of genius that is!*

Nowadays, with the help of computers (and perhaps AI), we keep finding bigger prime numbers. We are obsessed with them for a good reason.

Lemma 2.3. *If n is composite, then it has a divisor d such that $1 < d \leq \sqrt{n}$.*

Proof. We provide a direct proof.

Since n is composite, by definition [2], it has a divisor d such that $1 < d < n$:

$$d \mid n \implies \exists q \in \mathbb{Z} : d \times q = n$$

This also makes q a divisor of n.

Since $\sqrt{n} \leq n \forall n \in \mathbb{N}$, we can compare d with $\sqrt{n}$.

If $1 < d \leq \sqrt{n}$, we are done: we found a divisor we were seeking.

If, on the other hand, $d > \sqrt{n}$, then

$$\begin{aligned} d &> \sqrt{n} \\ d \times q &> \sqrt{n} \times q \\ n &> \sqrt{n} \times q \\ \sqrt{n} > q &\implies q < \sqrt{n} \end{aligned}$$

And we found q, a divisor of n between 1 and $\sqrt{n}$.

In either case, for a composite n, $\exists d : d \mid n, 1 < d \leq \sqrt{n}$.

■

Lemma 2.4. *If n is composite, then it has a prime divisor $d : 1 < d \leq \sqrt{n}$.*

Proof. ■

Chapter 3

Linear Diophantine Equations

Chapter 4

Congruences

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.
Theorem [1.1]	Chapter 1 Theorem 3	Euclid's gcd Algorithm.
Theorem [1.3]	Chapter 1 Theorem 4	Bézout Identity.
Theorem [2.1]	Chapter 2 Theorem 1	Infinitude of Primes.
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. 2).

[2] Martin Davis and Hersh Reuben. "Hilbert's Tenth Problem". *Scientific American* 229.5 (Nov. 1, 1973), pp. 84–91 (cit. on p. 10).

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

[4] Underwood Dudley. "Is Mathematics Necessary?" *The College Mathematics Journal* 28.5 (1997), pp. 360–64. DOI: 10.2307/2687064 (cit. on p. 2).

[5] *Linear Diophantine Equations*. 2010. URL: https://en.wikipedia.org/wiki/Diophantine_equation#Linear_Diophantine_equations (visited on 02/18/2025) (cit. on p. 10).

[6] Reginald McLean. *The Prime Pages*. 2025. URL: https://t5k.org/index.html (visited on 03/29/2025) (cit. on p. 20).

[7] *Paul Garrett's Answer to a Soft Question: How to Read a Book in Mathematics?* Sept. 28, 2013. URL: https://math.stackexchange.com/a/508272/83821 (visited on 03/18/2025) (cit. on p. 2).

[8] 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. 7).

[9] Eric S. Roberts. *Thinking Recursively*. 1st ed. John Wiley & Sons, Inc., 1986 (cit. on p. 14).

[10] 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. 2).