Introduction to Number Theory and Algorithms

Christian J. Rudder

August 2024

Contents

This page is left intentionally blank.

Preface

This is a Distillation of:
A Computational Introduction to Number Theory and Algebra
(Version 2), by Victor Shoup.

See https://shoup.net/ntb/ for the original text and practice problems.

— 1 —

Prerequisites

Definition 0.1: Well-Ordering Principle

Every non-empty set of positive integers has a least element.

Definition 0.2: "Without Loss of Generality"

A phrase that indicates that the proceeding logic also applies to the other cases. i.e., For a proposition not to lose the assumption that it works other ways as well.

— 2 —

Basic properties of Integers

2.1 Divisibility

a divides b, i.e., $\left(\frac{b}{a}\right)$, means b is reached by a, when a is multiplied by **some integer**.

Definition 1.1: Division

Let $a, b, x \in \mathbb{Z}$: $\left(\frac{b}{a}\right)$ means $b = ax$.

Denoted: $a|b$,
read a divides b, and a doesn't divide b is, $a \nmid b$.

Examples:

- $3 \mid 6$ because $6 = 3 \cdot 2$.
- $3 \nmid 5$ because $5 \neq 3 \cdot x$ for any $x \in \mathbb{Z}$.
- $2 \mid 0$ because $0 = 2 \cdot 0$.
- $0 \nmid 2$ because $2 \neq 0 \cdot x$ for any $x \in \mathbb{Z}$.

Note: $a, b, x \in \mathbb{Z}$ for, $\left(\frac{b}{a}\right)$ or $b = ax$ are labeled, a: divisor, b: dividend, x: quotient.

Tip: Many problems will involve manipulating equation like $b = ax$. Whether it's substituting b for ax or vice-versa, or adding/subtracting/multiplying/dividing.

Many definitions and theorems will build off one another. It's crucial to understand what concepts mean rather than memorizing them. This means having the ability to prove theorems and definitions from scratch.

Observe the following:

Theorem 1.1: Properties of Divisibility

For all $a, b, c \in \mathbb{Z}$:

(i) $a \mid a$, $1 \mid a$, and $a \mid 0$

(ii) $0 \mid a \iff a = 0$

(iii) $a \mid b \iff -a \mid b \iff a \mid -b$

(iv) $a \mid b \wedge a \mid c \implies a \mid (b + c)$

(v) $a \mid b \wedge b \mid c \implies a \mid c$

Try to prove these properties before reading the proof below.

Proof 1.1: Properties of Divisibility

Proof. For all $a, b, x, y \in \mathbb{Z}$:

(i)
- $a \mid a$ means $a = ax$, choosing $x = 1$ always satisfies.
- $1 \mid a$ because $a = 1 \cdot a$
- $a \mid 0$ because $0 = a \cdot 0$

(ii)
- If $0 \mid a$ then $a = 0 \cdot x$, 0 times any integer is 0, so $a = 0$
- If $a = 0$ then $0 = 0 \cdot x$, x can be any integer.

(iii) Proving $a \mid b \iff -a \mid b$:

- If $a \mid b$ then $b = ax = (-a)(-x)$, $-x$ is some integer, say x'.
  So $b = (-a)x'$ then $-a \mid b$
- If $-a \mid b$ then $b = (-a)x$, choose x to be some negative integer.

Proving $-a \mid b \iff a \mid -b$:

- If $-a \mid b$ then $b = (-a)x$, choose x positive integer.
- If $a \mid -b$ then $-b = ax$, choose x to be some negative integer.

(iv) If $a \mid b$ and $a \mid c$ then $b = ax$ and $c = ay$. Add both equations, $b + c = ax + ay$ factor, $b + c = a(x + y)$, $(x + y)$ is some integer. So $a \mid (b + c)$

(v) If $a \mid b$ and $b \mid c$ then $b = ax$ and $c = by$. Substitute b in c, $c = (ax)y$
shift terms, $c = a(xy)$, (xy) is some integer. So $a \mid c$.

■

Theorem 1.2: Reflexive Divisibility

For all $a, b \in \mathbb{Z}$: $a \mid b \wedge b \mid a \iff a = \pm b$. Additionally, $a \mid 1 \iff a = \pm 1$.

Proof 1.2: Reflexive Divisibility

Proof. For all $a, b, x, y \in \mathbb{Z}$:

Proving $a \mid b \wedge b \mid a \implies a = \pm b$:

$$\begin{aligned} a \mid b \quad b \mid a \qquad & \textit{Given} \\ b = ax \quad a = by \qquad & \textit{Definition of Division} \\ ab = (ax)(by) \qquad & \textit{Multiplying both equations} \\ ab = (ab)(xy) \qquad & \textit{Shift terms} \\ 1 = xy \qquad & \textit{Divide both sides by } ab \end{aligned}$$

x and y are integers, so $x = y = 1$. Substitute x and y,

$$\begin{aligned} b = a(1) \quad a = b(1) \qquad & \textit{Substitute} \\ a = b \qquad & \textit{Simplify} \end{aligned}$$

x or y could be $\pm$, so $\underline{a = \pm b.}$ Now $a = \pm b \implies a \mid b$ and $b \mid a$. From Theorem 1.1, we can use (i) to show $a \mid a$. Substitute b in for a, $\underline{a \mid b \text{ or } b \mid a.}$

Proving $a \mid 1 \implies a = \pm 1$:

$$\begin{aligned} a \mid 1 \qquad & \textit{Given} \\ 1 = ax \qquad & \textit{Definition of Division} \\ 1 = a(1) \qquad & \textit{Simplify} \end{aligned}$$

a must be 1, x could be $\pm$, so $a = \pm 1$ then $\underline{a \mid \pm 1 \text{ so } a \mid 1}$. ■

Definition 1.2: Cancellation Law

Let $a, b, c \in \mathbb{Z}$: If $ab = ac$ and $a \neq 0$ then $b = c$.

I.e., given $b = c$ multiplying both sides by a yields $ab = ac$, and still, $b = c$.

Definition 1.3: Prime Numbers

$p \in \mathbb{Z}$ is prime if $p \neq 0$ and p has no divisors other than 1 and p.

We will **only consider positive prime numbers**, in this text. Examples of primes are:

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

Definition 1.4: Composite Numbers

$n, a, b \in \mathbb{Z}$ is composite if $n = ab$ and $1 < a < n$ and $1 < b < n$.

I.e., a composite number is a number that can be factor into two integers, other than 1 and itself.
Examples:

- 4 is composite because $4 = 2 \cdot 2$.
- 6 is composite because $6 = 2 \cdot 3$.

Briefly observe the following:

Theorem 1.3: Division Algorithm

For all $a, b \in \mathbb{Z}$, $b > 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

To dissect, for all $a, b, q, r \in \mathbb{Z}$, $b > 0$, q and r exist uniquely such that:

$$a = bq + r$$

Dividend = **Divisor** · **Quotient** + **Remainder**

b fits into a q times with r left over.

Examples:

- $8 = 4 \cdot 2 + 0$
- $5 = 3 \cdot 1 + 2$

Note: Theorem 1.3 is called the Division Algorithm, despite not being an algorithm.

Proof 1.3: Division Algorithm

Proof. For all $a, b \in \mathbb{Z}$, $b > 0$, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$.

The definition of division $b \mid a$ then $a = bx$, $x \in \mathbb{Z}$. Subtract bx from both sides, $a - bx = 0$, working out evenly to 0. Freeze a and b, and vary x, yields a set of outputs, S:

$$S = \{a - bx : x \in \mathbb{Z}\}$$

"What's left of a after taking b, x times." E.g., $a = 6$, $b = 2$:

x	$a - bx$	
0	0	$= 6 - 2 \cdot 0$
1	4	$= 6 - 2 \cdot 1$
2	2	$= 6 - 2 \cdot 2$
3	0	$= 6 - 2 \cdot 3$
4	-2	$= 6 - 2 \cdot 4$

Let r be outputs of S and $q := x$ then $a - bq = r$ add bx to both sides, $\underline{a = bq + r}$.

Intuitively: I cut a cake of size a into pieces of b width for q people. Leftovers r can't exceed the size of the original cake: it's between nothing left or nothing shared, i.e., $\underline{0 \leq r < b}$.

We found our lower bound: $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$.

Formally: By the Well-Ordering Principle (0.1), there exists a smallest element in S, say r. To show S is not empty, choose $x = 0$ then $a - b(0) = a$, we are left with $0 \leq a$.

Without loss of generality, also assume $a < 0$. To satisfy $a - bx \geq 0$ choose $x = a$ yielding $a - ba = a(1 - b)$. Then $(1 - b) \leq 0$ as $(0 \leq r < b)$ so $(1 \leq b)$. Hence $a(1 - b) \geq 0$ as $(n < 0) \cdot (m \leq 0) = (h \geq 0)$ for some $n, m, h \in \mathbb{Z}$. So $\underline{S \text{ is not empty.}}$

• $\mathbf{r < b}$, say $r \geq b$, $\underline{r \text{ is the smallest element.}}$ Then $r = a - bq \geq b$. Subtract b from both sides, $(r - b = a - bq - b) \geq (b - b = 0)$ factoring we see $r - b = a - b(q + 1)$. Since $q + 1$ is some integer say q', $r - b = a - bq'$. There exists some b, $\underline{(r - b) < r \text{ contradicting our assumption.}}$

• $\mathbf{q, r}$ **uniqueness**, say there's another pair q', r' such that $a = (bq' + r') = (bq + r)$ and $0 \leq r' < b$. Without loss of generality, assume $r' \geq r$. Re-arrange both sides, $r' - r = bq - bq'$ factor, $r' - r = b(q - q')$. Then $b \mid (r' - r)$, but $(0 \leq r' - r < b)$ so $(r' - r) = 0$ therefore $r' = r$, showing $\underline{r \text{ is unique}}$. $b(q - q') = 0$ therefore $(q - q') = 0$ hence $q = q'$ showing $\underline{q \text{ is unique}}$. ■

2.2 Modular Arithmetic & Residues

Remember: For $a \in \mathbb{R}$, $a \in [0, 1)$ is a range, i.e., including decimals from 0 to 1 (excluding 1).

Definition 2.1: Floor & Ceiling

For $x \in \mathbb{R}$ and $m, n \in \mathbb{Z}$. Functions map $\mathbb{R} \to \mathbb{Z}$,

Floor x, $\lfloor x \rfloor$, is the largest m such that $m \leq x < m + \varepsilon$, where $\varepsilon \in [0, 1)$.
i.e., round down to the nearest integer.

Ceiling x, $\lceil x \rceil$, is the smallest n such that $n - \varepsilon < x \leq n$, where $\varepsilon \in [0, 1)$.
i.e., round up to the nearest integer.

Definition 2.2: Mod Operator

Let $a, b \in \mathbb{Z}$, $b > 0$: The remainder of a divided by b. I.e., $a - b \left\lfloor \frac{a}{b} \right\rfloor$.

Denoted: "a mod b" or "$a \,\%\, b$".

Examples: $8 \bmod 3 = 2$, and $5 \bmod 2 = 1$

Proof 2.1: Mod Operator

The Division Algorithm (1.3) only works for $b > 0$. To generalize for $b < 0$,

$$\begin{aligned} a &= bq + r && \textit{Given} \\ a/b &= q + r/b && \textit{Divide both sides by } b \end{aligned}$$

We know $0 \leq r < b$, dividing b yielded $0 \leq \dfrac{r}{b} < 1$, so

$$\frac{r}{b} \in [0, 1) \in \mathbb{R}$$

We notice $q = \left\lfloor \dfrac{a}{b} \right\rfloor$, as q is the largest integer that fits into a, b times. ■

Tip: $q = \left\lfloor \dfrac{a}{b} \right\rfloor$ is similar to integer division in programming, and $\dfrac{a}{b} = c$ implies $c \in \mathbb{R}$.

Theorem 2.1: Division Algorithm Extended

Let $a, b \in \mathbb{Z}$ with $b > 0$, and let $x \in \mathbb{R}$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, x + b)$.

$r \in [x, x + b)$ allows us to work with negative numbers and different intervals. Let's try to build some intuition about division and remainders:

$a, b, r \in \mathbb{Z}$ and $S = \{r = a - bq : q \in \mathbb{Z}\}$, $a = 6$, $b = 2$:

(0)

x	$a - bx$	
0	0	$= 6 - 2 \cdot 0$
1	4	$= 6 - 2 \cdot 1$
2	2	$= 6 - 2 \cdot 2$
3	0	$= 6 - 2 \cdot 3$
4	-2	$= 6 - 2 \cdot 4$
5	-4	$= 6 - 2 \cdot 5$
6	-6	$= 6 - 2 \cdot 6$
7	-8	$= 6 - 2 \cdot 7$

Dividing two numbers varying the divisor:

(1)

b	3 mod b
1	0
2	1
3	0
4	3
5	3
6	3
7	3
8	3

b	9 mod b
1	0
2	1
3	0
4	1
5	4
6	3
7	2
8	1
9	0
10	9

b	7 mod b
1	0
2	1
3	1
4	3
5	2
6	1
7	0
8	7

Grouping them by the remainder:

(2)

r	3 mod b
0	1, 3
1	2
3	4, 5, 6, …

r	9 mod b
0	1, 3, 9
1	2, 4, 8
3	5, 6, 7
9	10, 11, 12, …

r	7 mod b
0	1, 7
1	2, 6
2	5
3	4
7	8, 9, 10, …

Let's try the other way around.

(3)

a	a mod 3
0	0
1	1
2	2
3	0
4	1
5	2
6	0
7	1
8	2
9	0

a	a mod 9
0	0
1	1
2	2
3	3
…	…
9	0
10	1
11	2
…	…
18	0
19	1

a	a mod 7
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	0
8	1
9	2

Grouping them by the remainder:

(4)

r	a mod 3
0	0, 3, 6, 9
1	1, 4, 7
2	2, 5, 8

r	a mod 9
0	0, 9, 18
1	1, 10, 19
2	2, 11
3	3, 12
4	4, 13
5	5, 14
6	6, 15
7	7, 16
8	8, 17

r	a mod 7
0	0, 7
1	1, 8
2	2, 9
3	3
4	4
5	5
6	6

(5) **Table with increments of 3**

a	$a+1$	$a+2$
0	1	2
3	4	5
6	7	8
9	10	11
12	13	14
15	16	17
...	...	...

What is multiplication but repeated addition? What is division but repeated subtraction?

Column a in (5)-(7) shows multiples of b, which is example (4) transposed (highlighted). We can think of the width of a table as a's period.

Add 10 to 8, yields numbers always ending in 8. Add 5 to 8, yields numbers ending in 3 or 8. Then there are periods like (3).

We can see from the table (3), if we keep adding 3 to 2, we get 5, 8, 11, 14, etc.

(6) **Table with increments of 7**

a	$a+1$	$a+2$	$a+3$	$a+4$	$a+5$	$a+6$
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
35	36	37	38	39	40	41
...	...	...	...	...	...	...

(7) **Table with increments of 9**

a	$a+1$	$a+2$	$a+3$	$a+4$	$a+5$	$a+6$	$a+7$	$a+8$
0	1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35
36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53
...	...	...	...	...	...	...	...	...

We can represent these periods by $[x, x+b)$. Expanding the Division Algorithm (1.3) beyond $b > 0$, allows us to represent intervals no matter where we start on the number line.

We formally group (5)-(7)'s column headers into classes, which we call ***residues.***

Definition 2.3: Residue

Let $a, n \in \mathbb{Z}$, $n > 0$.

Set $R = \{a \bmod n : n \in \mathbb{Z}, n \neq 0\}$ produces remainders $r \in [0, n-1]$.
Each remainder r is a **residue** of a modulo n.

Definition 2.4: Residue Class

The set of numbers produced by a residue.

Denoted: $[a]_n$ or $a (\bmod n)$, a is the residue under modulo n.

Note: If modulo n has already been defined, $[a]_n$, then $[a]$ might be used.

Definition 2.5: Representative

If $x \in [a]$, x is a representative of $[a]$.

2.3 Ring Theory

We will primarily focus on **ideals** and the behavior of primes; Though to understand ideals, is to understand **groups** , **rings**, and **fields**.

Definition 3.1: Group

A *group* is a set G that is closed under one operation, say '$*$', that satisfies four properties:

- **Closure:** For all $a, b \in G$, $a * b \in G$.
- **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- **Identity:** There exists an element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.
- **Inverse:** $\forall a \, \exists \, a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a$ equates to the identity.

Examples: The following are groups:

- Set $S = \{-1, 1\}$ closed under multiplication.
  - **Closure:** $-1 \cdot -1 = 1 \in S$.
  - **Associativity:** $(-1 \cdot 1) \cdot -1 = 1 \cdot -1 = -1$ and $-1 \cdot (1 \cdot -1) = -1 \cdot 1 = -1$.
  - **Identity:** 1, as $1 \cdot -1 = -1 \cdot 1 = -1$.
  - **Inverse:** -1 as $-1 \cdot -1 = 1 =$ the identity.
- Set $I = \mathbb{Z}$ closed under addition.
  - **Closure:** $a + b \in I$ for all $a, b \in I$.
  - **Associativity:** $(a + b) + c = a + (b + c)$ for all $a, b, c \in I$.
  - **Identity:** 0, as $a + 0 = 0 + a = a$ for all $a \in I$.
  - **Inverse:** $-a$ for all $a \in I$, as $a + (-a) = (-a) + a = 0$.

Definition 3.2: Abelian Group

An *Abelian group* is a group that also satisfies the commutative property, i.e., for all $a, b \in G$, $a * b = b * a$. for some operation '$*$'.

Definition 3.3: Ring

A *ring* is a non-empty set R that is closed under additive ($+$) and multiplicative ($\cdot$) operations, such that:

- **Additive Group:** (R) is an Abelian group.
- **Multiplicative Closure:** For all $a, b \in R$, $a \cdot b \in R$.
- **Distributive Property:** For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

Examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings standard addition and multiplication.

Note: Operations aren't literally addition and multiplication. For example, the set of 2×2 matrices with $\mathbb{R}$ entries forms a ring.

Tip: Numbers and symbols are just placeholders for the concepts they represent. 1,2 or ($\div$) don't have inherent properties; they are just symbols, changing meaning in different contexts.

Definition 3.4: Ideal

An *ideal* I, is a special subset of a ring R, such that for all $a, b \in I$ and $r \in R$:

- **Additive:** $a + b \in I$.
- **Multiplicative under the ring:** $a \cdot r \in I$ or $r \cdot a \in I$.
- **Additive inverse:** $-a \in I$.
- **Additive identity:** $a, a' \in I$ such that $a + a' = a' + a = a'$.

Example: The set of all multiples of 2, $2\mathbb{Z}$, is an ideal of $\mathbb{Z}$.

- **Additive:** $(2 \cdot a) + (2 \cdot b) = 2(a + b) \in 2\mathbb{Z}$.
- **Multiplicative:** $(2 \cdot a) \cdot r = 2(a \cdot r) \in 2\mathbb{Z}$.
- **Additive inverse:** $-2 \in 2\mathbb{Z}$.
- **Additive identity:** $0 \in 2\mathbb{Z}$.

Definition 3.5: Field

A *field* is a ring $\mathbb{F}$ with additional properties:

- **Additive Structure:** $(\mathbb{F}, +)$ forms an Abelian group.
- **Multiplicative Structure:** $(\mathbb{F}, \cdot)$ forms an Abelian group excluding 0:
- **Distributive:** For all $a, b, c \in \mathbb{F}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example: $\mathbb{Q}$, the set of rational numbers:

- **Multiplicative identity:** $1 \in \mathbb{Q}$ as $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Q}$.
- **Multiplicative inverse:** $a^{-1} = \frac{1}{a}$ as $a \cdot \frac{1}{a} = 1$.
- **Excludes 0:** As 0 has no multiplicative inverse, i.e., $\frac{1}{0}$ is undefined.

Tip: A **group** defines operations, an **abelian group** ensures commutativity, a **ring** has an abelian group $(+)$, multiplication $(\cdot)$, and distribution, an **ideal** $I \subseteq R$ ring, such that $a \in I, r \in R, a \cdot r \in I$, and a **field** is a ring excluding 0 in its multiplicative abelian group.

2.4 Ideals & Primality

We will use $\mathbb{Z}$ as an ideal to explore the behavior of primes and divisibility.

Definition 4.1: Generator

An element or set of elements that can be used to *generate* a structure by repeated application of that structure's operations.

Definition 4.2: Integer Ideal Generator

The ideal generated by an integer a in $\mathbb{Z}$, denoted $a\mathbb{Z}$, is the set of all multiples of a:

$$a\mathbb{Z} = \{a \cdot x : x \in \mathbb{Z}\} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}.$$

Also Denoted: $\langle a \rangle$ when the generator is clear.

Example: The ideal generated by 2, $\langle 2 \rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$.

Proof 4.1: Proof that $a\mathbb{Z}$ is an Ideal

Let $a\mathbb{Z}$ be the ideal generated by $a \in \mathbb{Z}$, and let $az, az' \in a\mathbb{Z}$,$z'' \in \mathbb{Z}$, and $r \in \mathbb{R}$.

- **Additive Closure:** $az + az' = a(z + z') \in a\mathbb{Z}$.
- **Multiplicative Closure:** $az \cdot r = a(z \cdot r)$, then $(z \cdot r) \in \mathbb{Z}$ therefore $a(z \cdot r) \in a\mathbb{Z}$.
- **Additive Inverses:** $-az = a(-z) \in a\mathbb{Z}$.
- **Additive Identity:** $a \cdot 0 = 0 \in a\mathbb{Z}$.

Therefore, $a\mathbb{Z}$ is an ideal of $\mathbb{Z}$. ■

Definition 4.3: Principal Ideal

For ring R and $a \in R$, if $\langle a \rangle = \{r \cdot a : r \in R\}$ and $\langle a \rangle$ is an ideal of R, then $\langle a \rangle$ is a *principal ideal*.

Since $\mathbb{Z}$ forms a ring, for $a \in \mathbb{Z}$, $\langle a \rangle$ is a principal ideal of $\mathbb{Z}$. It also follows that $\langle a \rangle \subseteq \mathbb{Z}$.

Definition 4.4: Ideal Operations

Let I and J be ideals of a ring R.

- **Sum:** The sum of two ideals $I + J$ is defined as:

$$I + J = \{i + j : i \in I, j \in J\}.$$

  Since I and J are both have multiplicative closures of R, their sum is too.

$$(i \cdot r) \in I \text{ and } (j \cdot r) \in J \text{ then } (i \cdot r) + (j \cdot r) = (i + j) \cdot r \in I + J.$$

- **Product:** The product of two ideals $I \cdot J$ is defined as:

$$I \cdot J = \left\{ \sum i \cdot j : i \in I, j \in J \right\}.$$

  We need $\sum$ to show additive closure. We represent our product as sums alike $I + J$: For $i' \in I$:

$$(i \cdot j) + (i' \cdot j) = (i + i') \cdot j = i \cdot j \in I \cdot J.$$

This follows from the properties of ideals in $\mathbb{Z}$ and can be generalized to any ring R.

Example: Consider ideals in $\mathbb{Z}$:

$$I = 2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \quad \text{(the even integers)}$$

and

$$J = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \quad \text{(the multiples of 3)}.$$

The product $I \cdot J$ is not just the set of all individual products like $2 \cdot 3 = 6$. Instead, it is the set of all sums of products of elements from I and J, including sums like:

$$2 \cdot 3 + (-2) \cdot 3 = 6 - 6 = 0$$

or

$$2 \cdot 3 + 4 \cdot 3 = 6 + 12 = 18.$$

Thus, the product of I and J is:

$$I \cdot J = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\} = 6\mathbb{Z}.$$

Therefore, the product of $2\mathbb{Z}$ and $3\mathbb{Z}$ is $6\mathbb{Z}$, the set of multiples of 6. Illustrating $I \cdot J$ as the sums of products ensures the additive and multiplicative closure properties of ideals.

Theorem 4.1: Ideal Properties

For ideals in the integers $\mathbb{Z}$, and all $a, b \in \mathbb{Z}$:

- $b \in a\mathbb{Z}$ if and only if $a \mid b$.
- For every ideal $I \subseteq \mathbb{Z}$, $b \in I$ if and only if $b\mathbb{Z} \subseteq I$.
- Combining the above observations: $b\mathbb{Z} \subseteq a\mathbb{Z}$ if and only if $a \mid b$.

Proof 4.2: Proof of Ideal Properties

- $b \in a\mathbb{Z}$, let a be the smallest positive integer, then b must be 0, a, or some multiple of a, thus $a \mid b$. If $a \mid b$, then $b \in a\mathbb{Z}$, as $a\mathbb{Z}$ generates multiples of a.
- $b \in I$, then $b\mathbb{Z} \subseteq I$ as I upholds multiplicative closure. I.e., $q \in I$ then $bq \in I$.
- $a \mid b$, then $b \in a\mathbb{Z}$, $a\mathbb{Z}$ is an ideal, thus $b\mathbb{Z} \subseteq a\mathbb{Z}$. If $b\mathbb{Z} \subseteq a\mathbb{Z}$, then $b \in a\mathbb{Z}$, and $a \mid b$.

■

Theorem 4.2: Ideal Generator Existance of $\mathbb{Z}$

Let I be an ideal of $\mathbb{Z}$. Then there exists a unique non-negative integer d such that $I = d\mathbb{Z}$.

Proof 4.3: Proof of Generator Ideal equality of $\mathbb{Z}$

- **Existence:** $I = \{0\}$, then $d = 0$.
- $\mathbf{I \neq \{0\}}$: Let d be the smallest positive integer in I. If $a \in I$, then $d \mid a$, because $a = dq + r$ for some $q, r \in \mathbb{Z}$, where $0 \leq r < d$ (1.3). Since d is the smallest positive integer, $r = 0$, hence $d \mid a$.
- $\mathbf{I \subseteq d\mathbb{Z}}$, as $d \mid a$ and $a \in I$ (4.1).
- **Uniqueness:** Let d' be another non-negative integer. If $d'\mathbb{Z} = d\mathbb{Z}$, then $d \mid d'$ and $d' \mid d$. Thus, $d = \pm d'$ (1.1). Since, $d' \geq 0$, $d = d'$.

■

2.5 Primes & Greatest/Lowest Common Divisors

Definition 5.1: Greatest Common Divisor (GCD)

For all $a, b \in \mathbb{Z}$,
The *greatest common divisor* of a and b, is the largest positive integer dividing both a and b.
I.e., $d \in \mathbb{Z} : d \mid a$ and $d \mid b$, and d is unique.
Denoted: $\gcd(a, b)$.

Proof 5.1: GCD Existence and Uniqueness

Let $a, b \in \mathbb{Z}$, and $d = \gcd(a, b)$.

- **Existence:** d exists by the Well-Ordering Principle, as it's greatest element in the set of common divisors of a and b.
- **Uniqueness:** Let there be another GCD $d' \in \mathbb{Z}$ such that $d' \mid a$ and $d' \mid b$.
  Then, $d' \mid d$ and $d \mid d'$, so $d = \pm d'$ (1.1). GCD must be positive, so $d = d'$.

■

Theorem 5.1: GCD Ideal Linear Combination of $\mathbb{Z}$

For all $a, b, d \in \mathbb{Z}$ and $d = \gcd(a, b)$: $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Proof 5.2: GCD Ideal Linear Combination of $\mathbb{Z}$

Let $I := a\mathbb{Z} + b\mathbb{Z}$. Then there exists $c \in Z$ such that $c\mathbb{Z} = I$ (4.2). Then $a, b, c \in I$, are all positive integers. We will prove facts of c:

- **Common Divisor:** $a, b \in I$ and $c\mathbb{Z} = I$. So $a, b \in c\mathbb{Z}$. Then $c \mid a$ and $c \mid b$ (4.1).
- **Linear Combination:** Since $c \in I$ and $a\mathbb{Z} + b\mathbb{Z} = I$. There exists some linear combination $as + bt = c$ for some $s, t \in \mathbb{Z}$ (4.4).
- **Greatest Divisor** Let $a, b \in I$ be the products $a = a'c'$ and $b = b'c'$, where $a', b' \in \mathbb{Z}$. Then there's a linear combination $a'c' + b'c' = c'(a' + b') = c$. So $c \mid c'$, hence c is the greatest common divisor of a and b.
- **Uniqueness:** By Lemma (5.1), c is unique.

■

This next theorem heavily relies on Definition (4.1) and the previous Proof (5.1).

Theorem 5.2: Element Linear Combinations of $\mathbb{Z}$

For all $a, b, d \in \mathbb{Z}$ and $d = \gcd(a, b)$:
There exists some $s, t \in \mathbb{Z}$, such that $as + bt = r$ if and only if $d \mid r$.

Proof 5.3: Element Linear Combinations of $\mathbb{Z}$

Let $r \in \mathbb{Z}$, and $d = \gcd(a, b)$, we have

$$\begin{aligned} as + bt = r &\iff r \in a\mathbb{Z} + b\mathbb{Z} && \text{(Ideal Multiplicative Closure (4.4))} \\ &\iff r \in d\mathbb{Z} && \text{(GCD Linear Combination (5.1))} \\ &\iff d \mid r && \text{(Property of Ideals (4.1))} \end{aligned}$$

■

Note: In $as + bt = r$, s and t are not unique, nor do they have to be positive: Example (4.4)

From above it follows that:

Definition 5.2: Reltively Prime

For all $a, b \in \mathbb{Z}$, a and b are *relatively prime* if $\gcd(a, b) = 1$.

Also known as a **coprime**.

I.e., given the equation $as + bt = r$ in (5.2), if $r = 1$, then a and b are coprime.

Examples:

- $\gcd(6, 9) = 3$, so 6 and 9 are not coprime.
- $\gcd(6, 7) = 1$, so 6 and 7 are coprime.

Tip: It's crucial to understand the reasoning behind $as + bt = r$ and it's relation to ideals generated under $\mathbb{Z}$. I.e., understand ideals (3.4), and their operations (4.4) robustly.

Theorem 5.3: Cancellation of GCD

Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$. Then $c \mid b$.

Proof 5.4: Coprime Coefficient Divisibility

Let $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ and $\gcd(a, c) = 1$. a and c are coprime (5.2). Then there exists some $s, t \in \mathbb{Z}$ such that $as + ct = 1$ (5.2).Then,

$$\begin{aligned} as + ct &= 1 \text{ (Given)} \\ abs + cbt &= b \text{ (Multiply by } b\text{)} \\ cds + cbt &= b \text{ (Sub. } ab \text{ as } c \mid ab \Rightarrow ab = cd, d \in \mathbb{Z}\text{)} \\ c(ds + bt) &= b \text{ (Factor out } c\text{).} \end{aligned}$$

Yields $(ds + bt) \in \mathbb{Z}$, say m. So $cm = b$, hence $c \mid b$. ■

Theorem 5.4: Euclid's Lemma

Let p be a prime, and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof 5.5: Euclid's Lemma

Let p be a prime, and $a, b \in \mathbb{Z}$ such that $p \mid ab$.

- If $p \mid a$, we satisfy the claim.
- If $p \nmid a$, then $\gcd(p, a) = 1$ (1.3). So by Cancellation of GCD (5.3), $p \mid b$.

■

Note: Primes only have two divisors: 1 and itself. So if $p \nmid a$, then $\gcd(p, a)$ must be 1.

Tip: Euclid is pronounced "You-clid". He was a Greek mathematician who lived around 300 BC. His work laid the foundation for number theory. He primarily worked on the properties of prime numbers, and is known for his algorithm to find the GCD of two numbers.

Our most important theorem, **The Fundamental Theorem of Arithmetic**:

Theorem 5.5: Fundamental Theorem of Arithmetic (FTA)

Every $n \in \mathbb{Z} : n > 1$ is prime or is product of primes, up to the order of the factors.

By "up to the order of the factors", we mean that the factorization is commutative.
Example: $30 = 2 \cdot 3 \cdot 5$ or $3 \cdot 2 \cdot 5$. The factorization is unique, except order (commutative).

Proof 5.6: Fundamental Theorem of Arithmetic

Let $n \in \mathbb{Z}$ be a non-zero integer.

Existence: by induction of n,

- **Base Case:** $n = 2$, which holds as 2 is prime.
- **Inductive Hypothesis:** Assume for all $n = k$, k is prime or product of primes.
- **Inductive Step:** Let $n = k + 1$.
  - If n is prime, then we're done.
  - n is not prime, then $n = ab \in \mathbb{Z}$ where $a \leq b < n$, otherwise $ab > n$. Reasoning: If $a \geq n$ or $b \geq n$, then $ab \geq n^2$, contradicting $ab = n$ unless $n = 1$, however $n \geq 2$.
  - **Recursively:** Then a and b are prime or product of primes (Inductive Hypothesis). Then n is a product of primes.

  Therefore by induction, every $n \in \mathbb{Z} : n > 1$ is prime or is product of primes.

Uniqueness: Let there be two different factorizations: $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_j$.
Both factorizations are products of primes. We divide both sides by p_1:

$$p_2 p_3 \dots p_k = \frac{q_1 q_2 \dots q_j}{p_1} \qquad (p_1)(p_2 \dots p_k) = (q_1 q_2 \dots q_j)$$

(Simplified left side) (Multiply by p_1)

Let $m := (p_1)$, $n := (p_2 \dots p_k)$, $k := (q_1 q_2 \dots q_j)$. Then $mn = k$, so $m \mid k$. Take out q_1 from k, then $m \mid q_1 \cdot k$. By Euclid's Lemma (5.5), $m \mid q_1$ or $m \mid k$ (the rest of the factors).

- If $m \mid q_1$, then $m = q_1$, by definition of prime (1.3)
- If $m \mid k$, then m equals some other prime in k.

Continuing from p_2 to p_k results in $p_i = q_i$ for all i, thus the factorization must be unique. ■

Theorem 5.6: Euclids Theorem

There are infinitely many primes.

Proof 5.7: Euclids Theorem

Say there are a finite number of primes: $p_1, p_2, \ldots, p_n$.
Let $M := p_1 \times p_2 \times \ldots \times p_n$ be the product of those primes. Let $N = M + 1$:

$$\begin{aligned} N &= M + 1 \\ N &= p_1 \times p_2 \times \ldots \times p_n + 1 \\ N &= (p_1)(p_2 \times \ldots \times p_n) + 1 \text{ (Form of Division Alg. (1.3))} \end{aligned}$$

N has remainder 1 when divided by any such prime. Thus, N is not a product of primes.
Then N must be a prime (5.5). ■

Extending the the Fundamental Theorem of Arithmetic (5.5):

Theorem 5.7: FTA Corollary

Every $n \in \mathbb{Z} : n > 1$ has a unique prime factorization, up to order and sign:

$$n = \pm p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

For $p_1, p_2, \ldots, p_k$ distinct primes, and $e_1, e_2, \ldots, e_k$ positive integers.

Proof 5.8: FTA Corollary

Let $n \in \mathbb{Z} : n > 3$ and a composite number.

- $n = ab \in \mathbb{Z}$ by definition of a composite (1.4).
- Then a and b are prime or product of primes (5.5).
- Let a and b be prime and $a = b$

Then $n = a^2$, a prime squared. ■

We'll begin to define functions—which may or may not have logic—to abstract concepts.

Function 5.1: Prime Exponents - $\mathcal{V}_p(n)$

For each prime p where $n = p^e m \in \mathbb{Z}$ and $p \nmid m$. We define $\mathcal{V}_p(n) = e$.
I.e., $\mathcal{V}_p(n)$ is the exponent of p in the prime factorization of n.

In specifying $p \nmid m$, we ensure that p^e is the highest power of p dividing n.

We'll use this to abstract the Fundamental Theorem of Arithmetic further:

Theorem 5.8: FTA Abstracted by $\mathcal{V}_p(n)$

Every $n \in \mathbb{Z} : n > 1$ has a unique prime factorization, up to order and sign:

$$n = \pm \prod_p p^{\mathcal{V}_p(n)}$$

For p distinct primes.

Note: The notation $\prod$ is to products, as $\sum$ is to sums.

To expand our theorem for clarity:

$$n = \pm \prod_p p^{\mathcal{V}_p(n)} = \pm p_1^{\mathcal{V}_{p_1}(n)} p_2^{\mathcal{V}_{p_2}(n)} \cdots p_k^{\mathcal{V}_{p_k}(n)}$$

The "$\pm$" accounts for the sign of n. Say $n = -30$, then $n = -(2 \cdot 3 \cdot 5)$.

The function $\mathcal{V}_p(n)$ help us generalize GCD and **Least Common multiple** (LCM), but first we define two other functions:

Function 5.2: Minumum & Maximum - min(), max()

For all $a, b \in \mathbb{Z}$,

- $\min(a, b)$ is the smallest of a and b.
- $\max(a, b)$ is the largest of a and b.

Theorem 5.9: Operations of $\mathcal{V}_p(n)$

For all $a, b \in \mathbb{Z}$ and p prime:

- $\mathcal{V}_p(ab) = \mathcal{V}_p(a) + \mathcal{V}_p(b)$
- $\mathcal{V}_p(a^k) = k\mathcal{V}_p(a)$
- $a \mid b \iff \mathcal{V}_p(a) \leq \mathcal{V}_p(b)$ for all primes p

Proof 5.9: Operations of $\mathcal{V}_p(n)$

For all $a, b \in \mathbb{Z}$ and p prime:

- $\underline{\mathcal{V}_p(ab) = \mathcal{V}_p(a) + \mathcal{V}_p(b).}$
  Let $a = p^e m$ and $b = p^{e'} m'$, where $p \nmid m$ and $p \nmid m'$.
  - $ab = p^e m \times p^{e'} m' = p^{e+e'} mm'$
  - $\mathcal{V}_p(ab) = e + e' = \mathcal{V}_p(a) + \mathcal{V}_p(b)$

- $\underline{\mathcal{V}_p(a^k) = k\mathcal{V}_p(a).}$
  Let $a = p^e m$, where $p \nmid m$.
  - $a^k = (p^e m)^k = p^{ke} m^k$
  - $\mathcal{V}_p(a^k) = ke = k\mathcal{V}_p(a)$

- $\underline{a \mid b \iff \mathcal{V}_p(a) \leq \mathcal{V}_p(b) \text{ for all primes } p.}$
  Let $a = p^e m$ and $b = p^{e'} m'$, where $p \nmid m$ and $p \nmid m'$.
  - If $a \mid b$, then $b = aq \in \mathbb{Z}$. Thus, $\mathcal{V}_p(a) \leq \mathcal{V}_p(b)$, i.e., $e \leq e'$, otherwise $b < aq$.
  - $\mathcal{V}_p(a) \leq \mathcal{V}_p(b)$, both refer to p. Thus $a \mid b$ as a can pull some factor p^e out of b.

■

Tip: Remember that $\mathcal{V}_p(n)$ is some arbitrary function we defined. Despite this function being *made-up*, it has very **real** implications as we'll see in the next theorem. It helps to abstract concepts, to avoid repetition and the accumulation of details.

Similar to how computers are built on binary logic, and then subsequently written in some abstracted higher-level language. Then even those languages have their own abstractions through various libraries and frameworks, all helping speed up the process of development.

Theorem 5.10: GCD abstracted $\mathcal{V}_p(n)$

For all $a, b \in \mathbb{Z}$:

$$\gcd(a,b) = \prod_p p^{\min(\mathcal{V}_p(a),\mathcal{V}_p(b))}$$

Proof 5.10: GCD abstracted by $\mathcal{V}_p(n)$

The $\gcd(a,b) = \prod_p p^{\min(\mathcal{V}_p(a),\mathcal{V}_p(b))}$ can be visualized into the following:

$a =$	$\prod$	$p_1^{e_1}$	$p_2^{e_2}$	$p_3^{e_3}$	$\dots$	$p_k^{e_k}$
$b =$	$\vdots$	$p_1^{e'_1}$	$p_2^{e'_2}$	$p_3^{e'_3}$	$\dots$	$p_k^{e'_k}$
$gcd(a,b) =$	$\vdots$	$p_1^{\min(e_1,e'_1)}$	$p_2^{\min(e_2,e'_2)}$	$p_3^{\min(e_3,e'_3)}$	$\dots$	$p_4^{\min(e_k,e'_k)}$

Separating a and b into their prime factors, taking the minimum exponent of each pair p_i, Effectively striping all unnecessary factors, leaving only and all common factors between them.

I.e., the GCD.

■