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.

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.

— 1 —

Properties of Integers

1.1 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 $a \mid c$.

$\blacksquare$

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

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

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

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

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 1.2, we can use (i) to show $a \mid a$. Substitute b in for a, $\underline{a \mid b \text{ or } b \mid a.}$

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

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

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:

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

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: $S = \big\{a - bx : x \in \mathbb{Z}, a - bx \geq 0\big\}$.

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 $\underline{q \text{ is unique}}$. ■

1.2 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: "$a \bmod b$" 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:

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

(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 is clear from context, then $[a]_n$, becomes $[a]$.

Definition 2.5: Representative

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

1.3 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 $a * a^{-1} = a^{-1} * a = e$ 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 $-1 \cdot -1 = 1 = 1$
- 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 Structure:** (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. Multiplication is different than standard applications, though exists in some form.

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 identity:** There exists $e \in I : a + e = e + a = a$ (often 0).
- **Additive inverse:** $-a \in I : a + (-a) = -a + a = e$.

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 identity:** $0 \in 2\mathbb{Z}$.
- **Additive inverse:** For every $2a \in 2\mathbb{Z}$, its inverse is $-2a \in 2\mathbb{Z}$.

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** R consists of an abelian group $(+)$, multiplication $(\cdot)$, and distribution. An **ideal** $I \subseteq R$ is a special subset of a ring, such that for $a \in I$ and $r \in R$, $a \cdot r \in I$. Finally, a **field** is a ring where the non-zero elements form a multiplicative abelian group.

1.4 Ideals & Generators

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.

Denoted: $\langle a \rangle$, element a generating a structure.

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:

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

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 $\mathbb{Z}$. <u>It also follows that $\langle a \rangle \subseteq \mathbb{Z}$.</u>

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 $i' \in I$:

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

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 $a \mid b$.

$\blacksquare$

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, $d = \pm d'$ (1.2). Since, $d' \geq 0$, $d = d'$.

$\blacksquare$

1.5 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 $\underline{d \text{ is unique.}}$

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 $d = \pm d'$ (1.2). 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 $\underline{as + bt = c}$ 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, yielding $c = \gcd(a, b)$.

■

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

Theorem 5.2: Bezout's Identity

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 $d \mid r$. Moreover, if $d = 1$, then $as + bt = 1$.

Proof 5.3: Bezout's Identity

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

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

∎

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: Étienne Bézout was a prominent 18th-century French mathematician, known for his contributions to algebra and number theory. He is most famous for **Bézout's Identity**. Bézout also contributed to algebraic geometry, notably with **Bézout's Theorem**, which gives the maximum number of intersections between two algebraic curves.

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 $n \leq k$, 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.

$\blacksquare$

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. $\mathcal{V}_p(n)$ is no more real than $\gcd(a, b)$. It's a tool that helps us abstract.

Similar to how computers are built on binary logic, and then subsequently written in some abstracted higher-level language. 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 by $\mathcal{V}_p(n)$

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:

$$\begin{array}{rcc|c|c|c|c}
a = & \prod & p_1^{e_1} & p_2^{e_2} & p_3^{e_3} & \dots & p_k^{e_k} \\
b = & \vdots & p_1^{e'_1} & p_2^{e'_2} & p_3^{e'_3} & \dots & p_k^{e'_k} \\
\hline
gcd(a,b) = & \vdots & p_1^{\min(e_1,e'_1)} & p_2^{\min(e_2,e'_2)} & p_3^{\min(e_3,e'_3)} & \dots & p_k^{\min(e_k,e'_k)}
\end{array}$$

Separating a and b into their prime factors, taking the minimum exponent of each pair p_i, effectively intersecting all shared factors between a and b.

I.e., the GCD.

■

Definition 5.3: Least Common Multiple (LCM)

For all $a, b, n \in \mathbb{Z}$
The smallest positive integer divisible by both a and b is the *least common multiple*.
I.e., n is the smallest such integer that $a \mid n$ and $b \mid n$. $\underline{n \text{ is unique.}}$

Denoted: $\text{lcm}(a,b)$.

Proof 5.11: LCM Existence and Uniqueness

Let $a, b \in \mathbb{Z}$, and $m = \text{lcm}(a,b)$, m is the largest such integer that $a \mid m$ and $b \mid m$.

- **Existence:** m exists by the Well-Ordering Principle.
- **Uniqueness:** Let there be another smallest $m' \in \mathbb{Z} : a \mid m'$ and $b \mid m'$.
  Then, both m and m' are divisible by a and b. If m and m' are both the smallest, $m \mid m'$ and $m' \mid m$. Thus, $m = \pm m'$ (1.2). LCM must be positive, so $m = m'$.

■

Theorem 5.11: LCM abstracted by $\mathcal{V}_p(n)$

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

$$\operatorname{lcm}(a,b) = \prod_p p^{\max(\mathcal{V}_p(a), \mathcal{V}_p(b))}$$

Proof 5.12: LCM abstracted by $\mathcal{V}_p(n)$

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

$$\begin{array}{rcc|c|c|c|c}
a = & \prod & p_1^{e_1} & p_2^{e_2} & p_3^{e_3} & \dots & p_k^{e_k} \\
b = & \vdots & p_1^{e'_1} & p_2^{e'_2} & p_3^{e'_3} & \dots & p_k^{e'_k} \\
\hline
lcm(a,b) = & \vdots & p_1^{\max(e_1, e'_1)} & p_2^{\max(e_2, e'_2)} & p_3^{\max(e_3, e'_3)} & \dots & p_k^{\max(e_k, e'_k)}
\end{array}$$

Separating a and b into their prime factors, taking the maximum exponent of each pair p_i, effectively creating a union between a and b factors.

I.e., the LCM. ■

Theorem 5.12: GCD-LCM Relationship

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

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |ab|$$

which follows:

$$lcm(a,b) = \frac{|ab|}{\gcd(a,b)}$$

Proof on next page.

Proof 5.13: GCD-LCM Relationship

For every $a, b \in \mathbb{Z}$,
In Proof GCD abstracted (5.10) LCM abstracted (5.12) we showed:

- GCD creates the intersection of a and b's factors.
- LCM creates the union of a and b's factors.

LCM $\subseteq$ ab's factors. ab can be visualized as:

$$\begin{array}{rc|c|c|c|c} a = & \prod & p_1^{e_1} & p_2^{e_2} & p_3^{e_3} & \dots & p_k^{e_k} \\ b = & \vdots & p_1^{e_1'} & p_2^{e_2'} & p_3^{e_3'} & \dots & p_k^{e_k'} \\ \hline ab = & \vdots & p_1^{(e_1+e_1')} & p_2^{(e_2+e_2')} & p_3^{(e_3+e_3')} & \dots & p_k^{(e_k+e_k')} \end{array}$$

Then $\dfrac{|ab|}{\gcd(a,b)}$ would be:

$$\begin{array}{rcc|c|c} a = & \prod & p_1^{e_1} & \dots & p_k^{e_k} \\ b = & \vdots & p_1^{e_1'} & \dots & p_k^{e_k'} \\ \hline lcm(a,b) = & \vdots & p_1^{(e_1+e_1')-\min(e_1+e_1')} & \dots & p_k^{(e_k+e_k')-\min(e_k+e_k')} \end{array}$$

We are done. To further illustrate, $\max(e_i + e_i') = (e_i + e_i') - \min(e_i + e_i')$. Using $\mathcal{V}_p(n)$:

$$\operatorname{lcm}(a,b) = \prod_p p^{\mathcal{V}_p(ab) - \min(\mathcal{V}_p(a), \mathcal{V}_p(b))}$$

$\blacksquare$

Note: $\mathcal{V}_p(ab) = \mathcal{V}_p(a) + \mathcal{V}_p(b)$ as shown in Theorem (5.9).

— 2 —

Congruences

2.1 Equivalence Relations

Definition 1.1: Equivalence Relation

An **equivalence relation** on set S is a relation $\sim$ which satisfies:

1. **Reflexivity:** For all $a \in S$, $a \sim a$.
2. **Symmetry:** For all $a, b \in S$, if $a \sim b$, then $b \sim a$.
3. **Transitivity:** For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

With $a \sim a$ reading, "a is related to a."

Definition 1.2: Equivalence Class

For $\sim$ equivalence relation on set S. For each $a \in S$, the **equivalence class** of a is the set

$$[a] = \{x \in S \mid x \sim a\}.$$

Note: For $x \in [a]$, x is a **representative** of the equivalence class $[a]$ (2.5).

Theorem 1.1: Equivalence Class Uniqueness

For $\sim$ equivalence relation on set S, for all $a, b \in S$:

(i) $a \in [a]$.

(ii) $a \in [b] \implies [a] = [b]$.

Proof 1.1: Equivalence Class Uniqueness

For $a, b \in S$:

(i) Since $\sim$ is reflexive, $a \sim a$.

(ii) Suppose $a \in [b]$. Then $a \sim b$. Then for $x \in S$,

$$\begin{aligned} x \in [a] &\implies x \sim a \text{ (Definition of } [a] \text{ (1.2))} \\ &\implies x \sim b \text{ (Transitivity, } x \sim a \wedge a \sim b) \\ &\implies x \in [b] \text{ (Definition of } [b] \text{ (1.2))} \end{aligned}$$

Thus $[a] \subseteq [b]$. Similarly, $[b] \subseteq [a]$. Therefore $[a] = [b]$.

■

2.2 Modular Congruences

Continuing with the notion of residues in, we introduce the concept of modular congruences (2.3).

Definition 2.1: Modular Congruence

For $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, a is **congruent** to b modulo n if $n \mid (a - b)$, denoted as

$$a \equiv b \pmod{n}.$$

If $n \nmid (a - b)$, then $a \not\equiv b \pmod{n}$.

I.e., a and b have the same remainder when divided by n.

Note: $a \equiv b \pmod{n}$: **a** and **b** are **dividends** of **n** our **divisor**, which relate by **remainder**.

Theorem 2.1: Modular Congruence Properties

For all $a, b, c \in \mathbb{Z}$, and some positive integer n:

(i) $a \equiv a \pmod{n}$;

(ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$;

(iii) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Proof 2.1: Modular Congruence Properties

For all $a, b, c \in \mathbb{Z}$, and some positive integer n:

(i) $a \equiv a \pmod{n}$ so $n \mid (a - a)$, which holds.

(ii) $a \equiv b \pmod{n}$ so n divides $(a - b)$ and $-(a - b) = (b - a)$, then $b \equiv a \pmod{n}$.

(iii) $a \equiv b \pmod{n}$ so $n \mid (a - b)$, and $b \equiv c \pmod{n}$ is $n \mid (b - c)$. Therefore,

$$\begin{aligned} & n \mid (a-b) \quad \text{and} \quad n \mid (b-c) \\ \implies & n \mid [(a-b)+(b-c)] \\ \implies & n \mid (a-c) \\ \implies & a \equiv c \pmod{n}. \end{aligned}$$

■

Theorem 2.2: Modular Arithmetic

Let $a, a', b, b', n \in \mathbb{Z}$ with $n > 0$. If

$$a \equiv a' \pmod{n} \quad \text{and} \quad b \equiv b' \pmod{n},$$

then

$$a + b \equiv a' + b' \pmod{n} \quad \text{and} \quad a \cdot b \equiv a' \cdot b' \pmod{n}.$$

Proof 2.2: Modular Arithmatic

Addition: For $a, a', b, b', n \in \mathbb{Z}$,

- So $a \equiv a' \pmod{n}$ then $n \mid (a - a')$ means $a - a' = nx$ for some $x \in \mathbb{Z}$.
- Similarly, $b \equiv b' \pmod{n}$ then $b - b' = ny$ for some $y \in \mathbb{Z}$.
- Adding both equations, $(a - a') + (b - b') = (nx + ny)$ so $(a + b) - (a + b') = n(x + y)$.
- Therefore, $a + b \equiv a' + b' \pmod{n}$, as $n \mid (a + b) - (a' + b')$.

Multiplication: Continuing,

- If we multiply both equations, $(a - a')(b - b') = (nx)(ny)$ so $(ab) - (a'b') = n(xy)$.
- Therefore, $ab \equiv a'b' \pmod{n}$, as $n \mid (ab) - (a'b')$.

■

Theorem 2.3: Least Residue

Let $a, n \in \mathbb{Z}$ with $n > 0$. There exists unique $z \in \mathbb{Z}$ such that:

(i) $0 \leq z < n$,

(ii) $a \equiv z \pmod{n}$.

(iii) z is the **least residue** of a modulo n.

Particularly, for all $x \in \mathbb{Z}$, $z \in [x, x+n)$.

I.e., the least non-negative remainder r, which could be thought of as $r := a \bmod n$.

Note: The period $[x, x+n)$, contains possible remainders, a call back to the Division Alg. (2.1).

Proof 2.3: Least Residue

For some $a, q, n, r \in \mathbb{Z}$,
The Division Algorithm grantees existence, for $a = qn + r : 0 \leq r < n$ (2.1). Residues mod $n > 0$ are non-empty. Thus by the Well-Ordering Principle, there's a least element. ■

Example: Working to find the **set of solutions z** for $a \equiv z \pmod{n}$, i.e., find z that satisfies,

$$\begin{aligned} 3z + 4 &\equiv 6 \pmod{7} \text{ (Given)} \\ 3z &\equiv 2 \pmod{7} \text{ (Subtracting 4 from both sides)} \end{aligned}$$

We can't necessarily divide, but we can shift residue by some favorable factor.

$$\begin{aligned} 3z \cdot 5 &\equiv 2 \cdot 5 \pmod{7} \text{ (Multiply 5 to both sides)} \\ 1 \cdot z &\equiv 10 \pmod{7} \text{ (Since } 15 \equiv 1 \pmod{7}\text{)} \end{aligned}$$

Finding solution $z \equiv 10 \pmod{7}$, which we can reduce to $z \equiv 3 \pmod{7}$, as $3 \equiv 10 \pmod{7}$.
We say "integers z has solutions" as $z \in [3]_7 = \{3 + 7k : k \in \mathbb{Z}\}$ possible solutions.

Note: $[3]_7$ reads as *"the residue class 3 modulo 7."* Mentioned in (1.2).

2.3 Solving Linear Congruences

Theorem 3.1: Modular Multiplicative Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$.

(i) For every $b \in \mathbb{Z}$, the congruence $az \equiv b \pmod{n}$ has a solution $z \in \mathbb{Z}$ if and only if $d \mid b$.

(ii) For every $z \in \mathbb{Z}$, we have $az \equiv 0 \pmod{n}$ if and only if $z \equiv 0 \pmod{n/d}$.

(iii) For all $z, z' \in \mathbb{Z}$, we have $az \equiv az' \pmod{n}$ if and only if $z \equiv z' \pmod{n/d}$.

Proof 3.1: Linear Congruence Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d := \gcd(a, n)$.

(i)

$$\begin{aligned} & az \equiv b \pmod{n} \quad \text{for some } z \in \mathbb{Z} \\ \iff & az - b = ny \quad \text{for some } z, y \in \mathbb{Z} \quad \text{(Def. of congruence (2.1))} \\ \iff & az - ny = b \quad \text{for some } z, y \in \mathbb{Z} \\ \iff & d \mid b \quad \text{(By Bezout's Identity (5.2))}. \end{aligned}$$

(ii) Above is Bezout's Identity as a and n form a linear combination of b.-

$$\begin{aligned} n \mid az \iff & n/d \mid (a/d)z \text{ (Props. of Divisibility (1.1))} \\ \iff & n/d \mid z. \text{ (Cancellation of GCD: } \gcd(a/d, n/d) = 1 \text{ (5.3))} \end{aligned}$$

(iii)

$$\begin{aligned} & az \equiv az' \pmod{n} \\ \iff & a(z - z') \equiv 0 \pmod{n} \\ \iff & z - z' \equiv 0 \pmod{n/d} \quad \text{(By Part (ii))} \\ \iff & z \equiv z' \pmod{n/d}. \end{aligned}$$

■

For emphasis, as we saw above:

Definition 3.1: GCD Reduction

For $a, n \in \mathbb{Z}$, $d := \gcd(a, n)$, then $\gcd(a/d, n/d) = 1$.

Note: "$\rightarrow$" (Maps to), "$\mapsto$" (Defines the action of how a single element maps to another), "image" (the set of all outputs), and "pre-images" (the set of all inputs).

A corollary to the above theorem (3.1):

Theorem 3.2: Modular Multiplicative Map

Let $a, n \in \mathbb{Z}$ with $n > 0$, and residue classes $I_n := \{0, \ldots, n-1\}$. Then $(a \mod n) \in I_n$. Notably, for $z \in \mathbb{Z}$, $(az \mod n)$ is also in I_n.

I.e., $(az \mod n)$ is some re-ordering of the residue class $(a \mod n)$. Defining function, τ_a:

$$\tau_a : I_n \rightarrow I_n : z \mapsto az \bmod n. \tag{3.2.1}$$

The length of the image of τ_a is the number of distinct factors of n relative to a, i.e., n/d. Let the image of τ_a be:

$$E := \{az \mod n : z \in I_n\} = \{i \cdot d \mod n : i = 0, \ldots, n/d - 1\}. \tag{3.2.2}$$

The length of the pre-images of τ_a is the number of z solutions to $az \equiv b \pmod{n}$, i.e., d. Let the pre-images of τ_a be:

$$P := \{z \in I_n : az \equiv b \pmod{n}\}. \tag{3.2.3}$$

It follows that τ_a is a bijection (one-to-one and onto) if and only if $\gcd(a, n) = 1$. Then, the length of the image is n, and each pre-image has length 1.

Example: for $a = 1, 2, 3, 4, 5, 6$ and $n = 15$,

z	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2z \mod 15$	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
$3z \mod 15$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
$4z \mod 15$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
$5z \mod 15$	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
$6z \mod 15$	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9

- **Row:2** We see 2 and 15 are coprime, hence n images, $\{0, \ldots, n-1\}$.
- **Row:3** We see 3 and 15. Taking out common factors, 15/3, we get 5 distinct images.
- **Row:4** We see 4 and 15 are coprime, hence n images, $\{0, \ldots, n-1\}$.
- **Row:5** We see 5 and 15. Taking out common factors, 15/5, we get 3 distinct images.
- **Row:6** We see 6 and 15. Taking out common factors, 15/3, we get 5 distinct images.

Another corollary to the above theorem (3.1):

Theorem 3.3: Modular Congruence Cancellation

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(c, n) = 1$. If $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Example: We'll demonstrate different representations of members residue class $[2]_5$:

$$\begin{aligned} 8 &\equiv 13 \pmod{5} \quad \text{(i)} \\ 2 \cdot 4 &\equiv 3 \cdot 5 \pmod{5} \quad \text{(ii)} \\ 2 \cdot 4 &\equiv (-3) \cdot 4 \pmod{5} \quad \text{(iii)} \\ 2 &\equiv -3 \pmod{5} \quad \text{(iv)} \end{aligned}$$

Indeed $2 \equiv -3 \pmod{5}$, as $2 + 3 \equiv 3 - 3 \pmod{5}$. To show this, observe:

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2
	0	-4	-3	-2	-1	0	-4	-3	-2	-1	0	-4	-3

Think of **negative numbers** as traveling backwards within the residue class.

Definition 3.2: Modular Iverses

Let $a, n \in \mathbb{Z}$ with $n > 0$. If $az \equiv 1 \pmod{n}$, then z is the **modular inverse** of a **modulo** n and unique.

Denoted: $a^{-1} \pmod{n}$.

If inverse z modulo n exists, it is unique, as if there were another inverse z', then $z' \equiv z \pmod{n}$.

Restating (3.1) under coprime conditions:

Theorem 3.4: Coprime Modular Multiplicative Identities

Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $\gcd(a, n) = 1$.

(i) The congruence $az \equiv 1 \pmod{n}$ has a solution $z \in \mathbb{Z}$, the modular inverse.

(ii) If $az \equiv 0 \pmod{n}$, then $z \equiv 0 \pmod{n}$ (i.e., z must be a multiple of n).

(iii) If $az \equiv az' \pmod{n}$, then $z \equiv z' \pmod{n}$ (i.e., a cancels out, as long as $\gcd(a, n) = 1$).

Try to find inverses from the above table. Take an a and find solution z to $az \equiv 1 \pmod{5}$.

The Chinese Remainder Theorem

Note: $\mathbb{Z}^+$ denotes the set of positive integers, and $\{x_i\}_{i=1}^k$ is short for $\{x_1, ..., x_k\}$.

Theorem 3.5: Chinese Remainder Theorem (CRT)

Let $\{n_i\}_{i=1}^k \in \mathbb{Z}^+$ all be coprime to each other and let $\{a_i\}_{i=1}^k$ be arbitrary integers. Then there is a solution $a \in \mathbb{Z}$ to the system of congruences:

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ a &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a &\equiv a_k \pmod{n_k} \end{aligned}$$

Moreover, if a and b are solutions to the system, then $a \equiv b \pmod{\prod_{i=1}^k n_i}$.

Proof 3.2: Solving a System of Congruences (Part 1)

Let $\{n_i\}_{i=1}^k \in \mathbb{Z}^+$ all be pairwise coprime, and let $\{a_i\}_{i=1}^k$ be arbitrary integers,

Existence: (i) Construct a partial solution for each congruence. (ii) Each partial solution must not interfere with other congruences. (iii) Combine partial solutions:

We define indexes $i, j = 1, ..., k$ representing any two $e_1, ..., e_k$ integers such that:

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & \text{if } j = i, \text{ (target congruence)} \\ 0 \pmod{n_i} & \text{if } j \neq i \text{ (non-interfering).} \end{cases}$$

I.e., e_j has multiplicative identity to it's own system, and additive identity to all other systems by being some multiple. This allows us to construct:

$$\begin{aligned} e_1 \cdot a_1 &\equiv 1 \cdot a_1 \pmod{n_1} \\ e_2 \cdot a_2 &\equiv 1 \cdot a_2 \pmod{n_2} \\ &\vdots \\ e_k \cdot a_k &\equiv 1 \cdot a_k \pmod{n_k} \end{aligned}$$

Using additive identity, we close partial-solutions to $a = \sum_{i=1}^k e_i a_i$, the whole solution. ■

Proof 3.3: Solving a System of Congruences (Part 2)

To construct such $e_1, ..., e_k$, let $n := \prod_{i=1}^{k} n_i$ (the product of all moduli) and $n_i^* := n/n_i$. Then, n_i and n_i^* are coprime, meaning they have solution $n_i^* z \equiv 1 \pmod{n_i}$ for some $z \in \mathbb{Z}$.

Then $z = (n_i^*)^{-1}$, we can now define $e_i := n_i^* z$ for each $i = 1, ..., k$. Therefore, $e_i \equiv 1 \pmod{n_i}$. Since n contains shared factors, and we take n_i at congruence i, $e_i \equiv 0 \pmod{n_j}$ for $i \neq j$.

Thus, we can now construct the solution $a = \sum_{i=1}^{k} e_i a_i$.

■

Proof 3.4: Uniqueness of Solutions (Part 3)

If a and a' both satisfy the system of congruences

$$a \equiv a_i \pmod{n_i} \quad \text{and} \quad a' \equiv a_i \pmod{n_i} \quad \text{for } i = 1, \ldots, k$$

Then they must be congruent, i.e., $a \equiv a' \pmod{\prod_{i=1}^{k} n_i}$.

■

Note: **Uniqueness refers to $\mathbb{Z}_{\mathbf{n}}$** (residue classes modulo n), not just a. So there may be multiple solutions, but they congruent to each other under a unique modulus n

Example: We'll find solution a to the system of congruences:

$$a \equiv 3 \pmod 5$$
$$a \equiv 5 \pmod 7$$
$$a \equiv 2 \pmod{11}$$

Observe that $(3 \bmod 5) = \{3, 8, 13, 18, 23, 28, 33, ...\}$, and $(5 \bmod 7) = \{5, 12, 19, 26, 33, ...\}$. Sets describing $3 + 5k$ and $5 + 7k$ respectively. We see, $3 \equiv 33 \pmod 5$, and $5 \equiv 33 \pmod 7$.

Obtaining $e_1 = 7$, as $3 + 5(7) \implies 3(7) \equiv 1 \pmod 5$, and $5 + 7(7) \implies 5(7) \equiv 0 \pmod 7$.
We can take $n = 5 \cdot 7 = 35$ to construct a new system:

$$a \equiv 33 \pmod{35} = 33 + 35k = \{33, 68, ...\}$$
$$a \equiv 2 \pmod{11} = 2 + 11k = \{2, 13, 24, 35, 46, 57, 68, ...\}$$

We see that $33 \equiv 68 \pmod{35}$, and $2 \equiv 68 \pmod{11}$. Thus, $a = 68$:

$$68 \equiv 3 \pmod 5$$
$$68 \equiv 5 \pmod 7$$
$$68 \equiv 2 \pmod{11}$$

We can design a general algorithm based off this example to solve such systems.

Chinese Remainder Theorem Algorithm

Function 3.1: CRT Algorithm - `crt()`

Computes $a \in \mathbb{Z}$ satisfying a given system of congruences:

Input: Positive integers $\{n_i\}_{i=1}^k$ and integers $\{a_i\}_{i=1}^k$
Output: An integer a satisfying the system of congruences

Function *crt*($\{n_i\}_{i=1}^k, \{a_i\}_{i=1}^k$)**:**

```
a ← a_1;
N ← n_1;
for i ← 2 to k do
    while a mod n_i ≠ a_i do
        a ← a + N;
    end
    N ← N × n_i;
end
return a
```

We compute just like the example above:

1. First take a_1 and n_1 as our initial solution and modulus.
2. Then iterate starting with a_2 and n_2 to find solution $a \bmod (n_i) = a_i$.
3. If a is not congruent to a_i, we increment a by N until it is.
4. Then update N to the new product, and move to the next congruence.

2.4 Residue Classes

We've spoken before about residue classes in (2.4), but we'll go into more detail here.

Theorem 4.1: Residue Intervals

Remainders modular $n \in \mathbb{Z} : n > 1$, denoted $\mathbb{Z}_n$, is the interval $[0, (n-1)]$. As we pass $n-1$, we loop back to 0. Yielding a general interval of $[x, x+(n-1)]$ for $x \in \mathbb{Z}$.

Adding and multiplying residues shifts to some other position in the interval.

- **Addition:** $[(a+b) \bmod n] := [a] + [b] = [a+b] = [c] \iff a + b \equiv c \pmod n$
- **Multiplication:** $[(a \cdot b) \bmod n] := [a] \cdot [b] = [a \cdot b] = [c] \iff a \cdot b \equiv c \pmod n$

If n is odd, then our interval is $[-(n-1)/2, (n-1)/2]$. If even, then $[-n/2, n/2-1]$.

Example: Consider tables $\mathbb{Z}_5$ and $\mathbb{Z}_6$:

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2
	0	-4	-3	-2	-1	0	-4	-3	-2	-1	0	-4	-3

Since 5 is odd, our interval is $[-(4)/2, (4)/2] = [-2, 2]$, which could be seen as the interval $a \in [3, 7]$.

a	0	1	2	3	4	5	6	7	8	9	10	11	12
$a \mod 6$	0	1	2	3	4	5	0	1	2	3	4	5	0
	0	-5	-4	-3	-2	-1	0	-5	-4	-3	-2	-1	0

Since 6 is even, our interval is $[-6/2, 6/2-1] = [-3, 2]$, which could be seen as the interval $a \in [3, 8]$. This interval is no different than $[0, 5]$ or $[0, 6]$, this shifting of the interval captures $[x, x + (n-1)]$.

Note: We'll use α: "alpha"; β: "beta"; and such as variables when discussing residue classes.

Theorem 4.2: Residue Class Operations

Let $\alpha \in \mathbb{Z}_n$ be residue classes. Then:

- **Additive Identity:** $\alpha + [0] = \alpha$; **Additive Inverse:** $\alpha + (-\alpha) = [0]$.
- **Multiplicative Identity:** $\alpha \cdot [1] = \alpha$; **Multiplicative Inverse:** $\alpha \cdot \alpha^{-1} = [1]$.

Moreover, **Residue classes form a ring** (3.3), including distributive properties.

Theorem 4.3: Inverse Residue Classes

For $n \in \mathbb{Z} : n > 1$,
let $Z_n^* := \{\alpha \in \mathbb{Z}_n \mid \gcd(\alpha, n) = 1\}$, i.e., Z_n^* contains elements in $\mathbb{Z}_n$ where α^{-1} exists.

- If n is prime, then $Z_n^* = \mathbb{Z}_n \setminus \{[0]\}$, i.e., Z_n^* contains all elements in $\mathbb{Z}_n$ except $[0]$.
- If n is composite, then $Z_n^* \subsetneq \mathbb{Z}_n \setminus \{[0]\}$.

Moreover, Z_n^* forms a group under multiplication. Therefore for all $\beta \in Z_n^*$, we have $\alpha\beta \in Z_n^*$.

Note: The symbol $\subsetneq$ denotes a proper subset. If $A \subsetneq B$, then A is a subset of B but not equal to B.

Proof 4.1: Residue Class Inverses

Primes: The congruence $\alpha z \equiv 1 \pmod{n}$ has a solution z for all $\alpha \in \mathbb{Z}_n$ if $gcd(\alpha, n) = 1$ (3.4).

Composites: $Z_n^* \subsetneq \mathbb{Z}_n \setminus \{[0]\}$. If $d := gcd(\alpha, n) \mid n$, and $1 < d < n$, then $d \neq 0$ and $\alpha \notin Z_n^*$ (3.1). We say $d < n$, otherwise $n \equiv 0 \pmod{n}$ where $d = n$.

Multiplicative Group:

- **Inverse:** Every element in Z_n^* has an inverse.
- **Closure:** Therefore $\alpha\beta \in Z_n^*$, as $(\alpha^{-1})\alpha\beta \equiv \beta \pmod{n}$ and $(\beta^{-1})\beta\alpha \equiv \alpha \pmod{n}$.

∎

Theorem 4.4: Inverse Operations

Let $\alpha, \beta, \gamma \in \mathbb{Z}_n$ be residue classes. Then:

- **Inverse of Inverse:** $(\alpha^{-1})^{-1} = \alpha$
- **Product of Inverse:** $(\alpha \cdot \beta)^{-1} = \alpha^{-1} \cdot \beta^{-1}$
- **Inverse Division:** $\alpha/\beta = \alpha \cdot \beta^{-1}$
- **Cancellation Law:** $\alpha\beta = \alpha\gamma \implies \beta = \gamma \iff \alpha \in Z_n^*$.

Theorem 4.5: Residue Powers Identities

Powers work similarly to integers. For $\alpha, \beta \in \mathbb{Z}_n$ and $k, l \in \mathbb{Z}$, which also hold for $\alpha, \beta \in \mathbb{Z}_n^*$:

- **Zero Power:** $\alpha^0 = [1]$
- **General Powers:** $\alpha^1 = \alpha$ and $\alpha^2 = \alpha \cdot \alpha$ and so on.
- **Inverse Power:** Inverse α^k is $(\alpha^{-1})^k$.
- **Power of a Power:** $(\alpha^l)^k = \alpha^{lk} = (\alpha^k)^l$.
- **Product of Powers:** $\alpha^k \cdot \alpha^l = \alpha^{k+l}$.
- **Quotient of Powers:** $\alpha^k/\alpha^l = \alpha^{k-l}$.
- **Power of a Product:** $(\alpha\beta)^k = \alpha^k \cdot \beta^k$.

We may now generalize the Chinese Remainder Theorem (3.5) under residue classes.

Theorem 4.6: Chinese Remainder Map

Let $\{n_i\}_{i=1}^{k} \in \mathbb{Z}^+$ all be pairwise coprime, and $n := \prod_{i=1}^{k} n_i$. We define the map:

$$\begin{aligned} \theta : \mathbb{Z}_n &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \ldots, [a]_{n_k}) \end{aligned}$$

For $\mathbb{Z}_n$ (Residue classes modulo n), we can visualize:

$$\theta([a]_n) = \begin{cases} [a]_{n_1} & \text{mod } n_1 \\ [a]_{n_2} & \text{mod } n_2 \\ \vdots & \vdots \\ [a]_{n_k} & \text{mod } n_k \end{cases}$$

Where $[a]_n$ can be thought of as our a solution in the system of congruences:

$$\begin{aligned} a &\equiv a_1 \pmod{n_1} \\ a &\equiv a_2 \pmod{n_2} \\ &\vdots \\ a &\equiv a_k \pmod{n_k}, \end{aligned}$$

extending the Chinese Remainder Theorem to classes produced by a mod n, not just a.

(i) θ is unambiguous, i.e., any $[a]_n \in \mathbb{Z}_n$ has a unique image in $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

(ii) θ forms a ring isomorphism, meaning:

(a) θ is a bijection (one-to-one and onto), i.e., there's an inverse map θ^{-1}, which is the process of finding a from $[a]_n$ (The Chinese Remainder Theorem).

(b) θ preserves addition and multiplication, since residues form a ring. Thus, operating on residue classes only affects the inputs to the map (4.2).

Tip: The Chinese Remainder Map (θ) generates a system of congruences, while the Chinese Remainder Theorem solves them (θ^{-1}).

Euler's Phi Function

Tip: Leonhard Euler (1707–1783), pronounced as "oiler," was a Swiss mathematician born in Basel. He worked in St. Petersburg and Berlin, shaping calculus and number theory.

Also known as the **Euler Totient Function**:

Definition 4.1: Euler's Phi Function

For all $n \in \mathbb{Z}^+$, we define Euler's Phi Function as:

$$\varphi(n) := |\mathbb{Z}_n^*|$$

The number of inverses modulo n. Numbers coprime to n are in $\mathbb{Z}_n^*$.
Therefore, for primes p, $\varphi(p) = p - 1$.

Theorem 4.7: Chinese Remainder's Phi Function

Let $n := \prod_{i=1}^k n_i$ be the product of pairwise coprime integers. Then:

$$\varphi(n) = \prod_{i=1}^{k} \varphi(n_i) = \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_k)$$

The number of inverses in $\mathbb{Z}_n^*$ is the product of the number of inverses in $\mathbb{Z}_{n_i}^*$.

Proof 4.2: Chinese Remainder's Phi Function

Consider the Chinese Remainder Map $\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Since θ is isomorphic, it has a one-to-one correspondence. If we restrict our input to $\mathbb{Z}_n^*$, then the output will be in $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Hence, $|\mathbb{Z}_n^*| = |\mathbb{Z}_{n_1}^*| \times |\mathbb{Z}_{n_2}^*| \times \cdots \times |\mathbb{Z}_{n_k}^*| = \prod_{i=1}^k |\mathbb{Z}_{n_i}^*| = \prod_{i=1}^k \varphi(n_i)$. ■

Theorem 4.8: Euler's Phi of a Raised Prime

Let p be a prime and $e \in \mathbb{Z}^+$. Then:

$$\varphi(p^e) = p^{e-1}(p-1)$$

Proof 4.3: Euler's Phi of a Raised Prime

$\varphi(n)$ counts residue classes in $\mathbb{Z}_n$ that are coprime to n. $\mathbb{Z}_n$ represent integers $[0, n-1]$.

Examining $\mathbb{Z}_{p^e}$, to obtain coprimes, we omit members sharing common factors to p^e, i.e., multiples p, which p^e gives us e of.

Since the last factor reaches p^e, we ignore it, as it's beyond $p^e - 1$. Leaving us p^{e-1} multiples. Therefore, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$.

■

As implied by Theorem 4.7, we can generalize this to the prime factorization of n.

Theorem 4.9: Phi of Prime Factorization

Let $n := \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of n. $\{p_i^{e_i}\}$ are pairwise coprime. Then:

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$$

Expanding the product,

$$\varphi(n) = p_1^{e_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdot \cdots \cdot p_k^{e_k} \cdot \left(1 - \frac{1}{p_k}\right)$$

Which gives us:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

as n represents $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

2.5 Euler's Theorem & Fermat's Little Theorem

We know residues repeat in $\mathbb{Z}_n$ after n steps, forming a cycle. We've been used to seeing such cycles end and start at 0. However, when we restrict ourselves to $\mathbb{Z}_n^*$, 0 is excluded. We'll find that cycles in $\mathbb{Z}_n^*$ jump by powers of $\alpha \in \mathbb{Z}_n^*$, starting and ending at 1.

Definition 5.1: Multiplicative Order

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n^*$. The multiplicative order of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Theorem 5.1: Multiplicative Order Interval

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. The multiplicative order k repeats every k steps. Therefore, for every index:

- $i \in \mathbb{Z}$, $\alpha^i \equiv 1 \pmod{n} \iff k \mid i$, i.e., $i \equiv 0 \pmod{k}$.
- $i, j \in \mathbb{Z}$, $\alpha^i \equiv \alpha^j \pmod{n} \iff i \equiv j \pmod{k}$.

Example: Let $n = 7$ and take $\alpha = 1, \ldots, 6$.

- $\alpha = 1$: order 1.
- $\alpha = 2$: order 3.
- $\alpha = 3$: order 6.
- $\alpha = 4$: order 3.
- $\alpha = 5$: order 6.
- $\alpha = 6$: order 2.

i	1	2	3	4	5	6
1^i mod 7	1	1	1	1	1	1
2^i mod 7	2	4	1	2	4	1
3^i mod 7	3	2	6	4	5	1
4^i mod 7	4	2	1	4	2	1
5^i mod 7	5	4	6	2	3	1
6^i mod 7	6	1	6	1	6	1

We see that $\alpha = 2$ for $i = 3$ and $i = 6$, 3 is the smallest k such that $2^k \equiv 1 \pmod{7}$. Additionally, we see the relationship $2^i \equiv 2^j \pmod{7}$ if and only if $i \equiv j \pmod{3}$.

Note: For set S, $\prod_{\beta \in S} \beta$ is the product of all elements in S.

Theorem 5.2: Euler's Theorem

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\varphi(n)} \equiv 1 \pmod{n}$, when multiplicative order α divides $\varphi(n)$.

Proof 5.1: Euler's Theorem

For every $\beta \in \mathbb{Z}_n^*$, theres an $\alpha \in \mathbb{Z}_n^*$ such that $\alpha\beta \in \mathbb{Z}_n^*$ (4.2) $\varphi(n)$ and$\mathbb{Z}_n^*$:

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} \alpha\beta = \alpha^{\varphi(n)} \prod_{\beta \in \mathbb{Z}_n^*} \beta$$

Taking the inverse of $\prod_{\beta \in \mathbb{Z}_n^*} \beta$ results in $1 = \alpha^{\varphi(n)}$. **Note:** $\varphi(n) := |\mathbb{Z}_n^*|$ and both products β and $\alpha\beta$ produce the same set as we cycle inverse residues.

■

Theorem 5.3: Fermat's Little Theorem (FLT)

For every prime p and residue classes $\alpha \in \mathbb{Z}_p^*$: $\alpha^p \equiv \alpha \pmod{p}$.

Proof 5.2: Fermat's Little Theorem

Since p is prime, $\varphi(p) = p-1$. By Euler's Theorem, $\alpha^{p-1} \equiv 1 \pmod{p}$. Therefore, multiplying α to both sides yields, $\alpha^{p-1} \cdot \alpha \equiv 1 \cdot \alpha \pmod{p}$. Hence $\alpha^p \equiv \alpha \pmod{p}$. ■

Definition 5.2: Primitive Root

Let $n \in \mathbb{Z}^+$ and $\alpha \in \mathbb{Z}_n^*$. If the multiplicative order of α modulo n is $\varphi(n)$, then α is a primitive root modulo n.

Theorem 5.4: Multiplicative Order of Powers

If $\alpha \in \mathbb{Z}_n^*$ has multiplicative order k. Then from every new residue produced by α^m where $m \in \mathbb{Z}$, the multiplicative order of α^m is:

$$\frac{k}{\gcd(m,k)}$$

Example: Let $n = 7$ and $\alpha = 1, \ldots, 6$.

- $\alpha = 2^1 = 2$: has order $\dfrac{3}{\gcd(1,3)} = 3$.
- $\alpha = 2^2 = 4$: has order $\dfrac{3}{\gcd(2,3)} = 3$.
- $\alpha = 2^3 = 8 = 1$: has order $\dfrac{3}{\gcd(3,3)} = 1$.

i	1	2	3	4	5	6
1^i mod 7	1	1	1	1	1	1
2^i mod 7	2	4	1	2	4	1
3^i mod 7	3	2	6	4	5	1
4^i mod 7	4	2	1	4	2	1
5^i mod 7	5	4	6	2	3	1
6^i mod 7	6	1	6	1	6	1

Raising $\alpha = 2^3$ gave us 8, which is congruent to 1 modulo 7, and $\alpha = 1$ has order 1. Moreover, residues 3 and 5 are primitive roots.

We will abstract variables to emphasize α^m being some other residue after shifting by m.

Proof 5.3: Multiplicative Order of Powers

We define $\alpha^m := \beta$. Then β's multiplicative order is the smallest l such that $\beta^l \equiv 1 \pmod{n}$. Then by (5.1),

$$\alpha^{m \cdot l} \equiv 1 \,(\mathrm{mod}\ n) \iff ml \equiv 0 \,(\mathrm{mod}\ k)$$

We can drop m as a common factor by taking $\gcd(m, k)$ from k (3.1), yielding:

$$l \equiv 0 \,(\mathrm{mod}\ \frac{k}{\gcd(m,k)})$$

Thus we have $\beta^l \equiv 1 \pmod{n} \iff l \equiv 0 \,(\mathrm{mod}\ \frac{k}{\gcd(m,k)})$ satisfying the definition.

■

2.6 Quadratic Residues

Quadratic residues pertain to congruences of form $z^2 \equiv a \pmod{p}$, where p is prime. Though we start with general observations of residues produced by powers.

Definition 6.1: Residue Classes of Powers

We shall extend $\mathbb{Z}_n^*$ to powers, such that for all $\beta \in \mathbb{Z}_n^*$:

$$(\mathbb{Z}_n^*)^m := \{\beta^m \,(\mathrm{mod}\ n)\}$$

The set $(\mathbb{Z}_n^*)^m$ from $\mathbb{Z}_n^*$ at the very least holds $[1]_n$.

To illustrate our definition, we'll re-use our previous example $(\mathbb{Z}_7^*)^m$:

m	$(\mathbb{Z}_7^*)^1$	$(\mathbb{Z}_7^*)^2$	$(\mathbb{Z}_7^*)^3$	$(\mathbb{Z}_7^*)^4$	$(\mathbb{Z}_7^*)^5$	$(\mathbb{Z}_7^*)^6$
1^m mod 7	1	1	1	1	1	1
2^m mod 7	2	4	1	2	4	1
3^m mod 7	3	2	6	4	5	1
4^m mod 7	4	2	1	4	2	1
5^m mod 7	5	4	6	2	3	1
6^m mod 7	6	1	6	1	6	1

We see $(\mathbb{Z}_n^*)^1 = \{1, 2, 3, 4, 5, 6\}$, $(\mathbb{Z}_n^*)^2 = \{1, 2, 4\}$, $(\mathbb{Z}_n^*)^3 = \{1, 6\}$, annd so on.

For emphasis of our definition:

Theorem 6.1: Intersection of $\mathbb{Z}_n^*$ Powers

Let, $\alpha, \beta \in \mathbb{Z}_n^*$ and all $l, m \in \mathbb{Z}$,
If $\alpha^l \equiv \beta^m \pmod{n}$ then their residue r is in both $(\mathbb{Z}_n^*)^m$ and in $(\mathbb{Z}_n^*)^l$.

Example: As $(\mathbb{Z}_n^*)^1 = \{1, 2, 3, 4, 5, 6\}$, $(\mathbb{Z}_n^*)^2 = \{1, 2, 4\}$, both have 1,2, and 4 in common.

Theorem 6.2: Properties of Powers $(\mathbb{Z}_n^*)^m$

Let n be a positive integer, let $\alpha, \beta \in \mathbb{Z}_n^*$, and let m be any integer.

(i) If $\alpha \in (\mathbb{Z}_n^*)^m$, then $\alpha^{-1} \in (\mathbb{Z}_n^*)^m$.

(ii) If $\alpha \in (\mathbb{Z}_n^*)^m$ and $\beta \in (\mathbb{Z}_n^*)^m$, then $\alpha\beta \in (\mathbb{Z}_n^*)^m$.

(iii) If $\alpha \in (\mathbb{Z}_n^*)^m$ and $\beta \notin (\mathbb{Z}_n^*)^m$, then $\alpha\beta \notin (\mathbb{Z}_n^*)^m$.

Proof 6.1: Properties of Powers $(\mathbb{Z}_n^*)^m$

Let n be a positive integer, let $\alpha, \beta \in \mathbb{Z}_n^*$, and let m be any integer.

(i) If $\alpha \equiv \gamma^m \pmod{n}$, then $\alpha^{-1} \equiv (\gamma^{-1})^m \pmod{n}$

(ii) If $\alpha \equiv \gamma^m \pmod{n}$ and $\beta \equiv \delta^m \pmod{n}$, then $\alpha\beta \equiv (\gamma\delta)^m \pmod{n}$

(iii) Assume $\alpha \in (\mathbb{Z}_n^*)^m$, $\beta \notin (\mathbb{Z}_n^*)^m$, and $\alpha\beta \in (\mathbb{Z}_n^*)^m$. Then by (i), $\alpha^{-1} \in (\mathbb{Z}_n^*)^m$, we have by (ii), $\beta = \alpha^{-1}(\alpha\beta) \equiv \beta \pmod{n}$; However $\beta \notin (\mathbb{Z}_n^*)^m$, which is a contradiction.

■

Note: For $\alpha := [a] \in \mathbb{Z}_n$ and $b \in \mathbb{Z}$, we will often switch between $\alpha = b$ and $\alpha \equiv b \pmod{n}$, as α represents an element for which either equality or congruence holds.

Tip: Pierre de Fermat (1601-1665) was a French lawyer and mathematician. Born in Beaumont-de-Lomagne, France, Fermat is best known for his work in number theory, analytic geometry, and probability. His famous "Fermat's Last Theorem" remained unsolved for over 350 years. He claimed $an + bn = cn : n > 2$ has no integer solution.

Theorem 6.3: Coprime Powers $\mathbb{Z}_n^*$

Let $n \in \mathbb{Z}^+$, $\alpha \in \mathbb{Z}_n^*$ and all $l, m \in \mathbb{Z}$. Then:

$$\gcd(l, m) = 1 \text{ and } \alpha^l \in (\mathbb{Z}_n^*)^m \implies \alpha \in (\mathbb{Z}_n^*)^m$$

Proof 6.2: Coprime Powers $\mathbb{Z}_n^*$

For $\alpha^l \in (\mathbb{Z}_n^*)^m$ to exists means, $\alpha^l = \beta^m \pmod n$ for some $\beta \in \mathbb{Z}_n^*$. Since $\gcd(l, m) = 1$, by Bezout's Identity, there exists $ls + mt = 1$ for some $s, t \in \mathbb{Z}$.

$$a^1 = a^{ls+mt} = a^{ls}a^{mt} = \left(a^l\right)^s a^{mt} = (\beta^m)^s \alpha^{mt} = \left(\beta^s \alpha^t\right)^m =: \gamma^m$$

Therefore, $\alpha = \gamma^m \pmod n$, thus $\alpha \in (\mathbb{Z}_n^*)^m$. ■

Definition 6.2: Quadratic Residue

Let $\alpha, n \in \mathbb{Z}$,$\beta \in \mathbb{Z}_n^*$, and $n > 1$. Then,

- "α **is a quadratic residue modulo n**" if $\gcd(\alpha, n) = 1$ and $\alpha \equiv \beta^2 \pmod n$.
- "α **is a quadratic non-residue modulo n**" if $\gcd(\alpha, n) = 1$ and $\alpha \not\equiv \beta^2 \pmod n$.
- "β **is a square root of** α **modulo n**" if $\beta^2 \equiv \alpha \pmod n$.

Quadratic Residues Modulo Primes

We shall consider odd primes p, i.e., primes greater than 2, as 2 creates special cases that can complicate some of our results on quadratic residues.

Theorem 6.4: Square Roots of 1 Modulo p

Let p be an odd prime, and $\beta \in \mathbb{Z}_p$. Then $\beta^2 = 1 \iff \beta = \pm 1$.

Proof 6.3: Square Roots of 1 Modulo p

For $\beta \in \mathbb{Z}_p$, if $\beta = \pm 1$ then $\pm 1^2 \equiv 1 \pmod p$. If $\beta^2 = 1$, then $\beta^2 - 1 \equiv 0 \pmod p$, and $p \mid (b^2 - 1)$. For difference of squares, $(b^2 - 1) = (b + 1)(b - 1)$, and since p is prime,
$p \mid (b + 1)$ or $p \mid (b - 1)$. Thus, $\beta \equiv \pm 1 \pmod p$. ■

To reduce repetition, we will use $(\mathbb{Z}_p^*)^2$, to denote Quadratic Residues modulo odd primes p.

Theorem 6.5: Square Roots $(\mathbb{Z}_p^*)^2$

Let p be an odd prime, for $\gamma, \beta \in \mathbb{Z}_p^*$. Then $\gamma^2 \equiv \beta^2 \pmod{p} \iff \gamma \equiv \pm\beta \pmod{p}$.
I.e., for some $\alpha \in \mathbb{Z}_p^*$, if $\alpha = \beta^2$, then α has two square roots modulo p: $\pm\beta$.

Proof 6.4: Square Roots $(\mathbb{Z}_p^*)^2$

Following from the theorem proof we have,

$$\gamma^2 = \beta^2 \iff \frac{\gamma^2}{\beta^2} = 1 \iff \frac{\gamma}{\beta} = \pm 1 \iff \gamma = \pm\beta$$

In terms of congruences, members of $\mathbb{Z}_p^*$, γ and β are invertible:

$$\begin{aligned} \gamma^2 \equiv \beta^2 \pmod{p} &\iff \gamma^2 \cdot \beta^{-2} \equiv 1 \pmod{p} \\ &\iff \gamma \cdot \beta^{-1} \equiv \pm 1 \pmod{p} \\ &\iff \gamma \equiv \pm\beta \pmod{p} \end{aligned}$$

■

Theorem 6.6: Cardinality of $(\mathbb{Z}_p^*)^2$

Let p be an odd prime. Then,

$$|(\mathbb{Z}_p^*)^2| = \frac{(p-1)}{2}$$

Allowing us to represent $(\mathbb{Z}_p^*)^2$ as the interval $[1, (p-1)/2]$.

Proof 6.5: Cardinality of $(\mathbb{Z}_p^*)^2$

Let $\beta^2 \in (\mathbb{Z}_p^*)^2$, then there are two square roots for β^2: $\pm\beta$. We define the map:

$$\begin{aligned} \sigma : \mathbb{Z}_p^* &\to \mathbb{Z}_p^* \\ \pm\beta &\mapsto \beta^2 \bmod p \end{aligned}$$

Since σ is two-to-one where two elements from $\mathbb{Z}_p^*$ map to one element $(\mathbb{Z}_p^*)^2$, we cut our output in half. Hence, $|(\mathbb{Z}_p^*)^2| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$. ■

Theorem 6.7: Euler's Criterion (Taking Square Root $(\mathbb{Z}_p^*)^2$)

Let p be an odd prime and $\alpha \in \mathbb{Z}_p^*$. Then,

(i) $\alpha^{(p-1)/2} \equiv \pm 1 \pmod p$

(ii) If $\alpha \in (\mathbb{Z}_p^*)^2$, then $\alpha^{(p-1)/2} \equiv 1 \pmod p$.

(iii) If $\alpha \notin (\mathbb{Z}_p^*)^2$, then $\alpha^{(p-1)/2} \equiv -1 \pmod p$.

Note: Remember for $a \in \mathbb{Z}$, that $a^{\frac{1}{2}}$ is cancelled by $(a^{\frac{1}{2}})^2 = a$.

Proof 6.6: Euler's Criterion

(i) Let $\gamma = \alpha^{(p-1)/2}$. Then $\gamma^2 = \alpha^{p-1} = 1$ (5.3). Then $\gamma = \pm 1$ (6.4).

(ii) If $\alpha \in (\mathbb{Z}_p^*)^2$, $\alpha = \beta^2 \in \mathbb{Z}_p^*$. Then $(\beta^2)^{(p-1)/2} = \alpha^{(p-1)/2}$. Then , $\beta^{p-1} \equiv 1 \pmod p$ (5.3).

(iii) Examine $|(\mathbb{Z}_p^*)^2| = (p-1)/2$. Then the other half of $\mathbb{Z}_p^*$ are quadratic non-residues, for which we define the set $\mathcal{P}$. We describe $\mathcal{P}$'s image by map μ:

$$\begin{aligned} \mu : \mathbb{Z}_p^* &\to \mathbb{Z}_p^* \\ \kappa\lambda &\mapsto \alpha \notin (\mathbb{Z}_p^*)^2 \end{aligned}$$

For $\kappa, \lambda \in \mathbb{Z}_p^* : \kappa \neq \lambda$. Then, $\lambda = \frac{\alpha}{\kappa}$, so λ is uniquely determined by κ. We define the set $C := \{\kappa\lambda \in \mathbb{Z}_p^* : \kappa\lambda = \alpha\}$, and $C \subseteq \mathcal{P}$. Then their product

$$\prod_{\{\kappa\lambda \in C\}} \kappa\lambda \quad = \prod_{\{\kappa\lambda \in C\}} \alpha = \alpha^{(p-1)/2}$$

as a result of $\mathcal{P}$ containing $(p-1)/2$ many $\kappa\lambda$ pairs. We define $\epsilon := \prod_{\{\kappa\lambda \in C\}} \kappa\lambda$, and partition $D := \{\{\kappa\lambda\} \in \mathcal{P} : \kappa\lambda = 1\}$. If $\kappa\lambda = 1$, then $\kappa := \lambda^{-1}$, and κ uniquely determines λ. then $\kappa = \lambda$ if and only if $\kappa^2 = 1$, which implies $\kappa = \pm 1$ (6.4). So we exclude $[\pm 1]$ from our set D. Still for other pairs, $\kappa\lambda = 1$, we proceed:

$$\epsilon = \ [1] \cdot [-1] \prod_{\{\kappa\lambda \in D\}} \kappa\lambda \ = \ [-1] \prod_{\{\kappa\lambda \in D\}} [1] = -1$$

As we bring back $[\pm 1]$ in the product, we see $\epsilon = -1$. Thus $\alpha^{(p-1)/2} \equiv -1 \pmod p$. ∎

To abstract our findings we define the Legendre Symbol.

Function 6.1: Legendre Symbol

Let p be an odd prime, and $\alpha \in \mathbb{Z}_p^*$. Then the Legendre Symbol is defined as:

$$\left(\frac{\alpha}{p}\right) = \begin{cases} 1 & \text{if } \alpha \in (\mathbb{Z}_p^*)^2 \ (\alpha \text{ is a quadratic residue}), \\ -1 & \text{if } \alpha \notin (\mathbb{Z}_p^*)^2 \ (\alpha \text{ is a quadratic non-residue}). \end{cases}$$

This next theorem is a direct result from part (iii) in our proof of Euler's Criterion (6.7).

Theorem 6.8: Wilson's Theorem

Let p be an odd prime, then

$$(p-1)! \equiv -1 \pmod{p}$$

Proof 6.7: Wilson's Theorem

Let p be an odd prime. We know each element $\kappa, \lambda \in \mathbb{Z}_p^* : \kappa \neq \lambda$, has an inverse $\kappa\lambda = 1$. Except for $[\pm 1]$, as 1 is its own inverse.

We take $(p-1)! = (p-1)(p-2)\cdots(2)(1)$, and pair each element with its inverse:

$$(p-1)! \equiv (2 \cdot 2^{-1})(3 \cdot 3^{-1})\cdots(1 \cdot (p-1)) \pmod{p}$$

Note, $(p-1) = -1$ as -1 congruently is equivalent to the last element, i.e., $p-1$, yielding:

$$(p-1)! \equiv (1)(1)\cdots(1 \cdot (p-1)) \pmod{p}$$

Thus, $(p-1)! \equiv (p-1) \pmod{p}$, which is $(p-1)! \equiv -1 \pmod{p}$.

$\blacksquare$