Chapter 0 – Preliminaries

Harley Caham Combest

Su2025 MATH5353 Lecture Notes – Mk1

0.1 Basics

Historical Context. The concepts in this section — sets, functions, and relations — are so common now that they can feel "obvious." But each idea has a history:

- **Sets**: Ancient mathematicians grouped things (all even numbers, all triangles of a certain kind) without naming the concept. In the late 19th century, **Georg Cantor** defined sets formally and introduced the symbols $\in$, $\subseteq$, and $|A|$ for membership, subsets, and size.
- **Functions**: In the 18th century, a "function" meant a formula. **Dirichlet** (1837) redefined it as a general rule pairing each input with exactly one output.
- **Relations**: People long used ideas like "has the same remainder" or "is the same shape" without abstraction. By the early 20th century, the notion of a *relation* was formalized within set theory, leading to the powerful concepts of *equivalence relations* and *partitions*.

This section establishes the exact definitions and notation for these ideas so that later topics can be expressed with full precision.

Sets and Notation. A **set** is a collection of distinct objects, called *elements* or *members*.

- $\mathbf{x} \in \mathbf{A}$: x is an element of A.
- $\mathbf{x} \notin \mathbf{A}$: x is not an element of A.
- $\mathbf{B} \subseteq \mathbf{A}$: every element of B is in A ("B is a subset of A").
- $\mathbf{B} \subset \mathbf{A}$: B is a *proper* subset of A (and $B \neq A$).
- $\varnothing$: the empty set.
- $|\mathbf{A}|$: the *cardinality* (number of elements) of A if A is finite.

Subset by a Rule. We can describe a subset of A by giving a condition:

$$B = \{a \in A \mid \text{condition on } a\}.$$

Example: If $A = \{0, 1, 2, 3\}$, then

$$B = \{n \in A \mid n \text{ is even}\} = \{0, 2\}.$$

Cartesian Product. Given sets A and B, the *Cartesian product* $A \times B$ is:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Example: If $A = \{1, 2\}$ and $B = \{x, y\}$, then

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}.$$

Functions (Maps). A **function** $f : A \to B$ assigns *exactly one* output in B to *each* input in A.

- **Domain**: A, the set of allowed inputs.
- **Codomain**: B, the set where outputs live.
- **Value at** a: $f(a)$.

Example. Let $A = \{0, 1, 2\}$, $B = \{1, 3, 5, 7\}$, and

$$f(0) = 1, \quad f(1) = 3, \quad f(2) = 5.$$

Image / Range. The *image* (or *range*) of f is:

$$f(A) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}.$$

In the example: $f(A) = \{1, 3, 5\}$.

Preimage / Inverse Image. For $C \subseteq B$, the *preimage* of C is:

$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}.$$

If $C = \{3, 5\}$, then $f^{-1}(C) = \{1, 2\}$.

Fiber over b. The *fiber* over a single $b \in B$ is $f^{-1}(\{b\})$, the set of all inputs mapping to b.

Special Types of Functions.

- **Injective** (one-to-one): $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$.
- **Surjective** (onto): every $b \in B$ has some $a \in A$ with $f(a) = b$.
- **Bijective**: both injective and surjective; has a unique two-sided inverse.

Relations. A **binary relation** R on a set A is a subset of $A \times A$. We write $a\,R\,b$ if $(a, b) \in R$.

An **equivalence relation** has three properties:

- Reflexive: $a\,R\,a$ for all $a \in A$.
- Symmetric: $a\,R\,b \implies b\,R\,a$.
- Transitive: $a\,R\,b$ and $b\,R\,c \implies a\,R\,c$.

Equivalence Classes. For $a \in A$, the *equivalence class* $[a]$ is:

$$[a] = \{x \in A \mid x\,R\,a\}.$$

Any element of an equivalence class is called a *representative* of said equivalence class.

Partitions. A *partition* of A is a collection of nonempty, disjoint subsets whose union is A. Equivalence relations and partitions are two views of the same structure: the equivalence classes of an equivalence relation form a partition, and any partition defines an equivalence relation.

Proposition 1 (Characterizing injections, surjections, bijections via inverses). Let $f : A \to B$ be a function.

1. f is injective $\iff$ f has a *left inverse*: there exists $g : B \to A$ with $g \circ f = \mathrm{id}_A$.
2. f is surjective $\iff$ f has a *right inverse*: there exists $h : B \to A$ with $f \circ h = \mathrm{id}_B$.
3. f is bijective $\iff$ there exists $g : B \to A$ with $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. In this case g is unique and equals f^{-1}.
4. If A and B are finite with $|A| = |B|$, then f is injective $\iff$ surjective $\iff$ bijective.

Proof. (1) "$\Rightarrow$" Assume f is injective.

For each $b \in B$, if there exists $a \in A$ with $f(a) = b$, define $g(b) := a$ (this a is unique by injectivity).

If no such a exists, define $g(b)$ arbitrarily in A (choose a fixed $a_0 \in A$).

Then for every $a \in A$, we have $f(a)$ in the first case, so $g(f(a)) = a$. Hence $g \circ f = \mathrm{id}_A$.

"$\Leftarrow$" Suppose there is $g : B \to A$ with $g \circ f = \mathrm{id}_A$.

If $f(a_1) = f(a_2)$, then applying g gives

$$a_1 = (g \circ f)(a_1) = (g \circ f)(a_2) = a_2,$$

so f is injective.

(2) "$\Rightarrow$" Assume f is surjective.

For each $b \in B$, choose some $a_b \in A$ with $f(a_b) = b$ (choice is possible by surjectivity).

Define $h(b) := a_b$. Then $(f \circ h)(b) = f(a_b) = b$ for all b, so $f \circ h = \mathrm{id}_B$.

"$\Leftarrow$" If there is h with $f \circ h = \mathrm{id}_B$, then for each $b \in B$ we have $b = (f \circ h)(b) = f(h(b))$, so b lies in the image of f. Thus f is surjective.

(3) If f is bijective, then it has a two-sided inverse $f^{-1} : B \to A$ with $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$ (standard inverse of a bijection).

Conversely, if there exists g with both identities, then by (1) f is injective (since it has a left inverse g) and by (2) f is surjective (since it has a right inverse g), hence bijective.

Uniqueness of the inverse: If $g_1, g_2 : B \to A$ both satisfy $f \circ g_i = \mathrm{id}_B$ and $g_i \circ f = \mathrm{id}_A$ for $i = 1, 2$, then

$$g_1 = (g_1 \circ \mathrm{id}_B) = (g_1 \circ (f \circ g_2)) = ((g_1 \circ f) \circ g_2) = (\mathrm{id}_A \circ g_2) = g_2.$$

(4) Assume $|A| = |B| < \infty$.

If f is injective, then no two elements of A map to the same element of B; with $|A| = |B|$, this forces f to hit all of B (pigeonhole principle), hence f is surjective.

Conversely, if f is surjective, then mapping $|A|$ elements onto $|B| = |A|$ elements forces no collisions, hence f is injective.

Therefore injective $\Leftrightarrow$ surjective, and either implies bijective. $\square$

Quick Lemmas and Corollaries (Right after Proposition 1).

Lemma A (Left inverse $\Rightarrow$ injective). If $g \circ f = \mathrm{id}_A$ for some $g : B \to A$, then $f : A \to B$ is injective.

Proof. If $f(a_1) = f(a_2)$, apply g to both sides: $a_1 = (g \circ f)(a_1) = (g \circ f)(a_2) = a_2$.

So distinct inputs cannot collide; f is injective. □

. . . .

Lemma B (Right inverse $\Rightarrow$ surjective). If $f \circ h = \mathrm{id}_B$ for some $h : B \to A$, then $f : A \to B$ is surjective.

Proof. For any $b \in B$, we have $b = (f \circ h)(b) = f(h(b))$, so b is hit by f. □

. . . .

Lemma C (Two-sided inverse is unique). If $g_1, g_2 : B \to A$ both satisfy $f \circ g_i = \mathrm{id}_B$ and $g_i \circ f = \mathrm{id}_A$ for $i = 1, 2$, then $g_1 = g_2$.

Proof. $g_1 = g_1 \circ \mathrm{id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_A \circ g_2 = g_2$. □

. . . .

Lemma D (Fiber tests for injectivity/surjectivity). Let $f : A \to B$. For $b \in B$, the *fiber* over b is $f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$.

1. f is injective $\iff$ every fiber has size at most 1.
2. f is surjective $\iff$ every fiber is nonempty.

Proof. (1) Injective means no two distinct inputs share an output, i.e. each fiber has ≤ 1 point.

(2) Surjective means every $b \in B$ is hit by some $a \in A$, i.e. each fiber is nonempty. □

. . . .

Lemma E (Composition preserves injective/surjective). Let $A \xrightarrow{f} B \xrightarrow{g} C$.

1. If f and g are injective, then $g \circ f$ is injective.
2. If f and g are surjective, then $g \circ f$ is surjective.

Proof. (1) If $(g \circ f)(a_1) = (g \circ f)(a_2)$, injectivity of g gives $f(a_1) = f(a_2)$, then injectivity of f gives $a_1 = a_2$.

(2) Given $c \in C$, surjectivity of g gives $b \in B$ with $g(b) = c$; surjectivity of f gives $a \in A$ with $f(a) = b$; then $(g \circ f)(a) = c$. □

. . . .

Corollary F (Finite pigeonhole consequences). If A, B are finite with $|A| = |B|$ and $f : A \to B$, then:

1. If f is injective, it is automatically surjective.
2. If f is surjective, it is automatically injective.

Proof. (1) Injective map $A \to B$ between equal-size finite sets cannot miss any element of B.

(2) Dually, a surjection from $|A|$ points onto $|B| = |A|$ cannot identify two distinct inputs. □

. . . .

Corollary G (Bijectivity and the inverse map). $f : A \to B$ is bijective $\iff$ there exists a unique $f^{-1} : B \to A$ with $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

Proof. "⇒" A bijection has both a left and right inverse; Lemma C gives uniqueness.

"⇐" If such f^{-1} exists, Lemma A gives injective and Lemma B gives surjective. □

Proposition 2 (Equivalence relations $\Longleftrightarrow$ partitions). Let A be a nonempty set.

1. If $\sim$ is an equivalence relation on A, then the set of equivalence classes $\{[a] : a \in A\}$ forms a partition of A.

2. Conversely, if $\{A_i\}_{i \in I}$ is a partition of A (each $A_i \neq \varnothing$, $A_i \cap A_j = \varnothing$ for $i \neq j$, and $\bigcup_{i \in I} A_i = A$), then there is an equivalence relation $\sim$ on A whose equivalence classes are exactly the A_i.

Proof. (1) For an equivalence relation $\sim$, define $[a] = \{x \in A : x \sim a\}$.

Reflexivity gives $a \in [a]$, so each class is nonempty. If $[a] \cap [b] \neq \varnothing$, pick x in the intersection.

Then $x \sim a$ and $x \sim b$.

By symmetry, $a \sim x$; by transitivity with $x \sim b$, we get $a \sim b$.

Now if $y \in [a]$, then $y \sim a \sim b$, hence $y \in [b]$; similarly any $z \in [b]$ lies in $[a]$.

Thus $[a] = [b]$, proving the classes are pairwise disjoint unless equal.

Finally, for any $x \in A$, reflexivity gives $x \in [x]$, so $\bigcup_{a \in A} [a] = A$.

Hence the classes form a partition.

. . . .

(2) Given a partition $\{A_i\}_{i \in I}$, define $x \sim y$ iff x and y lie in the *same* block A_i.

This is well-defined because the blocks are disjoint and cover A.

Reflexive: each x lies in some A_i, so $x \sim x$.

Symmetric: if $x \sim y$, they share the same A_i, so $y \sim x$.

Transitive: if $x \sim y$ and $y \sim z$, then all three lie in the same A_i, hence $x \sim z$.

Thus $\sim$ is an equivalence relation; its classes are precisely the blocks A_i. □

0.2 Properties of the Integers

Historical Context. The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are among the oldest mathematical objects.

Their properties have been studied since antiquity:

- **Ancient Number Theory**: The Greeks, especially Euclid (c. 300 BCE), formalized results on divisibility, greatest common divisors, and primes in *Elements*, Book VII.
- **The Euclidean Algorithm**: Known to Euclid and perhaps earlier in Mesopotamia, this algorithm for finding the gcd of two integers remains fundamental today.
- **Primes and Unique Factorization**: Euclid proved there are infinitely many primes. The idea that every integer factors uniquely into primes is implicit in ancient work and formalized in the Fundamental Theorem of Arithmetic.
- **Euler's φ-function**: Introduced by Leonhard Euler (18th century) to generalize Fermat's Little Theorem and study multiplicative structure modulo n.

These basic properties underpin much of algebra and number theory. We state them precisely and prove them in the modern set-theoretic language.

1. Well Ordering of $\mathbb{Z}^+$.

Proposition 1 (Well Ordering Principle)**.** *Every nonempty subset $A \subseteq \mathbb{Z}^+$ has a smallest element m such that $m \leq a$ for all $a \in A$.*

Proof. Suppose A is nonempty.

Let $S = \{1, 2, 3, \dots\} \cap A$.

If $1 \in A$ we are done.

Otherwise, check $2, 3, \dots$ in order.

Because A is a subset of the positive integers, and these are well ordered by the usual $\leq$, we eventually find the first element of A.

This minimal element m is the one desired. □

. . . .

Calculative 2 (Well Ordering in practice)**.** *Let $A = \{\, n \in \mathbb{Z}^+ \mid n$ is a multiple of 5 and $n > 12 \,\} = \{15, 20, 25, \dots\}$.*

Then $\min A = 15$. This concretely illustrates that a nonempty subset of $\mathbb{Z}^+$ has a least element.

2. Divisibility. For $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a *divides* b (write $a \mid b$) if there exists $c \in \mathbb{Z}$ with $b = ac$.

. . . .

Lemma 3. *If $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for all $s, t \in \mathbb{Z}$.*

Proof. Write $b = ak$ and $c = al$.

Then $sb + tc = s(ak) + t(al) = a(sk + tl)$, so a divides $sb + tc$. □

. . . .

Calculative 4 (Divisibility is stable under $\mathbb{Z}$-linear combintions)**.** *Since $4 \mid 20$ and $4 \mid 28$, for any $s, t \in \mathbb{Z}$ we have $4 \mid s \cdot 20 + t \cdot 28$.*

Take $s = 3$, $t = -2$: $3 \cdot 20 + (-2) \cdot 28 = 60 - 56 = 4$, and indeed $4 \mid 4$.

3. Greatest Common Divisor and Least Common Multiple.

Definition 1. The *greatest common divisor* of $a, b \in \mathbb{Z} \setminus \{0\}$ is the unique positive integer d such that:

1. $d \mid a$ and $d \mid b$ (common divisor),
2. if $e \mid a$ and $e \mid b$, then $e \mid d$ (greatest).

Write $d = (a, b)$. If $(a, b) = 1$ we say a and b are *relatively prime.*

. . . .

Proposition 5 (Bezout's Identity)**.** *For $a, b \in \mathbb{Z} \setminus \{0\}$ there exist $x, y \in \mathbb{Z}$ such that $(a, b) = ax + by$.*

Proof. Apply the Euclidean Algorithm to a and b.

This produces remainders r_k satisfying

$$r_{k-2} = q_k r_{k-1} + r_k, \quad 0 \leq r_k < |r_{k-1}|.$$

When $r_n \neq 0$ and $r_{n+1} = 0$, we have $r_n = (a, b)$.

Back-substitute each r_k in terms of a and b to express r_n as a $\mathbb{Z}$-linear combination of a and b. □

. . . .

Definition 2. The *least common multiple* ℓ of a and b is the unique positive integer such that:

1. $a \mid \ell$ and $b \mid \ell$,
2. if $a \mid m$ and $b \mid m$ then $\ell \mid m$.

We write $\ell = \operatorname{lcm}(a, b)$.

Relation: $(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$.

4. Division Algorithm and Euclidean Algorithm.

Proposition 6 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = qb + r, \quad 0 \leq r < |b|.$$

Proof. Existence: Divide a by b in the usual sense to get a quotient q and remainder r satisfying the bounds.

Uniqueness: If $a = qb + r = q'b + r'$ with $0 \leq r, r' < |b|$, subtracting gives $(q - q')b = r' - r$.

The right side has absolute value less than $|b|$, so it must be 0, hence $q = q'$ and $r = r'$. □

. . . .

Calculative 7 (Example: Division Algorithm in action)**.** *Let $a = 101$ and $b = 7$. We seek q, r with*

$$101 = q \cdot 7 + r, \quad 0 \leq r < 7.$$

Dividing: $7 \times 14 = 98$, so $q = 14$ and $r = 3$. Thus

$$101 = (14) \cdot 7 + 3,$$

matching the abstract definition: $q, r \in \mathbb{Z}$ and $0 \leq r < |7|$.

. . . .

Proposition 8 (Euclidean Algorithm)**.** *Repeated application of the Division Algorithm to (a, b) terminates with remainder 0 and last nonzero remainder equal to (a, b).*

Proof. Apply Division Algorithm: $a = q_0 b + r_0$, then $b = q_1 r_0 + r_1$, etc.

Remainders strictly decrease in absolute value and are nonnegative, so the process stops.

The last nonzero remainder divides the previous two terms in the sequence and thus divides any common divisor; hence it equals (a, b). □

Calculative 9 (Example: Euclidean Algorithm in action)**.** *Let* $a = 252$ *and* $b = 165$.

$$\begin{aligned} 252 &= 1 \cdot 165 + 87, \\ 165 &= 1 \cdot 87 + 78, \\ 87 &= 1 \cdot 78 + 9, \\ 78 &= 8 \cdot 9 + 6, \\ 9 &= 1 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

The last nonzero remainder is 3*, so* $(252, 165) = 3$*.*

Back-substitution (Bezout coefficients):
$3 = 9 - 1 \cdot 6$*,*
$6 = 78 - 8 \cdot 9 \ \Rightarrow\ 3 = 9 - 1 \cdot (78 - 8 \cdot 9) = 9 \cdot 9 - 1 \cdot 78$*,*
$9 = 87 - 1 \cdot 78 \ \Rightarrow\ 3 = (87 - 78) \cdot 9 - 1 \cdot 78 \ldots$ *etc.,*
until we express $3 = 252 \cdot x + 165 \cdot y$*.*

Calculative 10 (gcd, lcm, and Bézout on a friendlier pair)**.** *For* $a = 84$*,* $b = 60$*:*

$$84 = 1 \cdot 60 + 24, \quad 60 = 2 \cdot 24 + 12, \quad 24 = 2 \cdot 12 + 0,$$

so $(84, 60) = 12$ *and* $\mathrm{lcm}(84, 60) = \dfrac{84 \cdot 60}{12} = 420$*.*

Back-substitution:

$$12 = 60 - 2 \cdot 24 = 60 - 2(84 - 60) = 3 \cdot 60 - 2 \cdot 84,$$

hence $12 = -2 \cdot 84 + 3 \cdot 60$*.*

5. Primes and Fundamental Theorem of Arithmetic.

Definition 3. A prime is a positive integer $p > 1$ whose only positive divisors are 1 and p.

Non-primes > 1 are composite.

. . . .

Lemma 11 (Prime Divides a Product)**.** *If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \nmid a$, then $(p, a) = 1$. Bezout's Identity gives $px + ay = 1$ for some x, y. Multiply by b:

$$pbx + aby = b.$$

Since $p \mid pbx$ and $p \mid aby$, we have $p \mid b$. □

. . . .

Calculative 12 ("Prime divides a product" at work)**.** *Let $p = 5$, $a = 14$, $b = 15$. Then $ab = 210$ and $5 \mid 210$.*

Since $5 \nmid 14$ (remainders $14 \equiv -1 \pmod 5$), it must be that $5 \mid 15$, which holds.

. . . .

Theorem 13 (Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be written uniquely (up to order) as*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

with distinct primes p_i and positive integers α_i.

Proof. Existence: Induct on n. If n is prime, done. If composite, write $n = ab$ with $a, b < n$, factor each by induction, and combine.

Uniqueness: Suppose $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_m^{\beta_m}$ with primes in ascending order. $p_1 \mid q_1^{\beta_1} \dots q_m^{\beta_m}$, so $p_1 = q_j$ for some j.

Cancel and repeat inductively to match all primes and exponents.

□

Calculative 14 (Fundamental Theorem of Arithmetic: sample factorizations)**.**

$$360 = 2^3 \cdot 3^2 \cdot 5, \qquad 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

Each factorization is unique up to the order of prime factors.

6. Euler's Totient Function.

Definition 4. For $n \in \mathbb{Z}^+$, $\varphi(n)$ is the number of integers $1 \le a \le n$ with $(a, n) = 1$.

. . . .

Theorem 15 (Chinese Remainder Theorem for Two Moduli)**.** *Let $m, n \in \mathbb{Z}^+$ with* $\gcd(m, n) = 1$*.*

Then for any integers a, b there exists an integer x such that

$$x \equiv a \pmod{m} \quad \textit{and} \quad x \equiv b \pmod{n}.$$

Moreover, this x is unique modulo mn.

Proof. Since $\gcd(m, n) = 1$, Bezout's Identity gives integers u, v with

$$um + vn = 1.$$

Define

$$x := a \cdot (vn) + b \cdot (um).$$

Then modulo m:

$$x \equiv a \cdot (vn) + b \cdot (um) \equiv a \cdot (0) + b \cdot (um) \pmod{m}.$$

But $um \equiv 0 \pmod{m}$ and $vn \equiv 1 \pmod{m}$ (since $vn = 1 - um$), so actually:

$$x \equiv a \cdot 1 + b \cdot 0 \equiv a \pmod{m}.$$

Similarly, modulo n:

$$x \equiv a \cdot (vn) + b \cdot (um) \equiv a \cdot 0 + b \cdot 1 \equiv b \pmod{n}.$$

Thus x satisfies both congruences.

If x' is another such integer, then $m \mid (x - x')$ and $n \mid (x - x')$.
As $\gcd(m, n) = 1$, it follows that $mn \mid (x - x')$, so $x \equiv x' \pmod{mn}$. □

. . . .

Calculative 16 (Chinese Remainder Theorem: solving a pair of congruences)**.** *Solve*

$$x \equiv 3 \pmod 4, \qquad x \equiv 2 \pmod 5.$$

Since $4(-1) + 5(1) = 1$*, take* $u = -1$*,* $v = 1$*,* $m = 4$*,* $n = 5$*,* $a = 3$*,* $b = 2$ *and set*

$$x = a \cdot (vn) + b \cdot (um) = 3 \cdot 5 + 2 \cdot (-4) = 15 - 8 = 7.$$

Check: $7 \equiv 3 \pmod 4$ *and* $7 \equiv 2 \pmod 5$*.*
General solution: $x \equiv 7 \pmod{20}$*.*

. . . .

Corollary 17 (Multiplicativity of φ)**.** *If* $\gcd(a, b) = 1$*, then* $\varphi(ab) = \varphi(a)\varphi(b)$*.*

Proof. By the theorem, the reduction map

$$\mathbb{Z}/(ab)\mathbb{Z} \;\longrightarrow\; \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, \quad [x]_{ab} \mapsto ([x]_a, [x]_b)$$

is a bijection of rings when $\gcd(a, b) = 1$. This bijection restricts to a bijection of unit groups:

$$(\mathbb{Z}/(ab)\mathbb{Z})^\times \;\cong\; (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Taking cardinalities yields $\varphi(ab) = \varphi(a)\varphi(b)$. □

. . . .

Proposition 18 (Values of φ)**.** *If* p *is prime and* $\alpha \geq 1$*, then*

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

If $(a, b) = 1$*, then* $\varphi(ab) = \varphi(a)\varphi(b)$*.*

Proof. For p^α: The integers $1, \ldots, p^\alpha$ divisible by p are $p, 2p, \ldots, p^{\alpha-1}p$ — exactly $p^{\alpha-1}$ of them.

Subtract from total p^α to get $\varphi(p^\alpha)$.

For multiplicativity: By the Chinese Remainder Theorem, reduction modulo a and b is a bijection

$$(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \text{ when } (a, b) = 1\text{, hence } \varphi(ab) = \varphi(a)\varphi(b).$$

□

. . . .

Calculative 19 (Counting $\varphi(n)$ by hand)**.** *For* $n = 12$*, list* $1 \leq a \leq 12$ *coprime to* 12*:* $\{1, 5, 7, 11\}$*.*

Thus $\varphi(12) = 4$*.*

For $n = 18$*, the coprimes in* $1, \ldots, 18$ *are* $\{1, 5, 7, 11, 13, 17\}$*, so* $\varphi(18) = 6$*.*

Formula check: $18 = 2 \cdot 3^2$*, so* $\varphi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6$*.*

. . . .

Calculative 20 (Multiplicativity of φ with coprime inputs)**.** *Let* $a = 8$*,* $b = 15$*;* $\gcd(8, 15) = 1$*.*

$\varphi(8) = 4$ *(numbers* $\{1, 3, 5, 7\}$ *mod* 8*),* $\varphi(15) = 8$ *(exclude multiples of* 3 *or* 5*).*

Then $\varphi(120) = \varphi(8)\varphi(15) = 32$*.*

Direct check via formula: $120 = 2^3 \cdot 3 \cdot 5$*, so*

$$\varphi(120) = 120\Big(1 - \tfrac{1}{2}\Big)\Big(1 - \tfrac{1}{3}\Big)\Big(1 - \tfrac{1}{5}\Big) = 120 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 32.$$

. . . .

Calculative 21 (Euler's totient on prime powers)**.** *For* $p = 3$*,* $\alpha = 2$*:* $\varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$*.*

Indeed, among $1, \ldots, 9$*, the six coprime to* 9 *are* $\{1, 2, 4, 5, 7, 8\}$*.*

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Historical Context. The study of integers *modulo n* began in earnest with Carl Friedrich Gauss's *Disquisitiones Arithmeticae* (1801).

Gauss introduced the notation $a \equiv b \pmod{n}$ and built a systematic theory of congruences.

The idea itself is older: the Chinese Remainder Theorem dates back to Sun Zi (3rd–5th century CE), and modular methods appear implicitly in work by Euler and Fermat.

Today, $\mathbb{Z}/n\mathbb{Z}$ — the set of *residue classes modulo n* — is fundamental in algebra, number theory, cryptography, and coding theory. It allows us to treat numbers that differ by multiples of n as *the same* for arithmetic purposes, forming a finite ring.

Congruence Modulo n.

Definition 5. Let $n \in \mathbb{Z}^+$. For $a, b \in \mathbb{Z}$ we say a is *congruent to b modulo n*, written

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

if $n \mid (a - b)$. Equivalently, a and b have the same remainder upon division by n.

. . . .

Proposition 22. *Congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

Proof. Reflexive: $a - a = 0$ is divisible by n.

Symmetric: If $n \mid (a - b)$, then $n \mid (b - a)$.

Transitive: If $n \mid (a - b)$ and $n \mid (b - c)$, then $n \mid [(a - b) + (b - c)] = a - c$.

□

. . . .

Calculative 23 (Checking congruence in two ways)**.** *Let $n = 7$, $a = 51$, and $b = 16$.*

Method 1: Divisibility of the difference. *Compute $a - b = 51 - 16 = 35$. Since $35 = 7 \cdot 5$, we have $7 \mid (a - b)$, hence*

$$51 \equiv 16 \pmod{7}.$$

Method 2: Same remainder upon division by n. *By the Division Algorithm:*

$$51 = 7 \cdot 7 + 2, \quad 16 = 7 \cdot 2 + 2.$$

Both have remainder 2 when divided by 7, so $51 \equiv 16 \pmod{7}$.

Conclusion: *The two methods agree — congruence modulo n can be verified either by checking $n \mid (a - b)$ or by comparing remainders.*

Residue Classes and $\mathbb{Z}/n\mathbb{Z}$.

Definition 6. The *residue class* of $a \in \mathbb{Z}$ modulo n is

$$[a]_n = \{\, b \in \mathbb{Z} \mid b \equiv a \pmod{n} \,\}.$$

The set of all residue classes is denoted $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

. . . .

Calculative 24 (Residue classes mod 5)**.** *$\mathbb{Z}/5\mathbb{Z}$ has the five classes* $[0], [1], [2], [3], [4]$. *For instance,* $[7]_5 = [2]_5$ *since* $7 - 2 = 5$ *is divisible by* 5.

. . . .

Proposition 25 (Well-defined operations (Theorem 3))**.** *For* $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ *define*

$$[a]_n + [b]_n := [a+b]_n, \quad [a]_n \cdot [b]_n := [ab]_n.$$

These are well-defined*, i.e. the result does not depend on the choice of representatives.*

Proof. Suppose $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then $n \mid (a-a')$ and $n \mid (b-b')$.

For addition: $(a+b)-(a'+b') = (a-a')+(b-b')$ is divisible by n, so $[a+b]_n = [a'+b']_n$.

For multiplication: $(ab) - (a'b') = b(a-a') + a'(b-b')$ is a sum of multiples of n, hence divisible by n. □

. . . .

Calculative 26 (Addition and multiplication mod 7)**.** $[3]_7 + [5]_7 = [8]_7 = [1]_7$, $[4]_7 \cdot [6]_7 = [24]_7 = [3]_7$.

Units (Invertible Classes).

Definition 7. A class $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ is a *unit* (i.e. is *invertible*) if there exists $[b]_n$ with $[a]_n \cdot [b]_n = [1]_n$. The set of units (i.e. invertible classes) is $(\mathbb{Z}/n\mathbb{Z})^\times$.

. . . .

Proposition 27 (Proposition 4)**.**

$$(\mathbb{Z}/n\mathbb{Z})^\times \;=\; \{\, [a]_n \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1 \,\}.$$

Proof. ($\subseteq$) Let $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Then there exists $[b]_n$ such that

$$[a]_n \cdot [b]_n = [1]_n.$$

By definition of multiplication in $\mathbb{Z}/n\mathbb{Z}$, this means $ab \equiv 1 \pmod{n}$, i.e. $ab - 1 = kn$ for some $k \in \mathbb{Z}$.

Any common divisor of a and n must divide 1, hence $\gcd(a,n) = 1$.

($\supseteq$) Conversely, suppose $\gcd(a,n) = 1$.

By Bézout's Identity, there exist integers x, y such that

$$ax + ny = 1.$$

Reducing modulo n, we have $ax \equiv 1 \pmod{n}$, so $[a]_n \cdot [x]_n = [1]_n$.

Thus $[a]_n$ has a multiplicative inverse and is in $(\mathbb{Z}/n\mathbb{Z})^\times$. □

. . . .

Calculative 28 (Example: Units mod 12)**.** *The positive integers less than* 12 *and coprime to* 12 *are* $1, 5, 7, 11$. *Thus:*

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{[1], [5], [7], [11]\}.$$

Check: $[5]_{12}^2 = [25]_{12} = [1]_{12}$, *so* $[5]$ *is its own inverse.*

. . . .

Calculative 29 (Example: Inverse via Euclidean Algorithm)**.** *Find the inverse of* $[17]_{60}$.

Apply the Euclidean Algorithm:

$$60 = 3 \cdot 17 + 9, \quad 17 = 1 \cdot 9 + 8, \quad 9 = 1 \cdot 8 + 1.$$

Back-substitute:

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 = 2(60 - 3 \cdot 17) - 17 = 2 \cdot 60 - 7 \cdot 17.$$

Thus -7 *is an inverse of* 17 *modulo* 60*, i.e.* $[53]_{60}$ *is the multiplicative inverse.*