

Contents

0	Week 0	3
0.1	Notation	3
0.2	Maps	3
0.2.1	Composition	3
0.2.2	Identity	3
0.2.3	Properties	3
0.2.4	Surjective	4
0.2.5	Bijjective	4
0.2.6	Inverse Maps	4
0.3	Integers	4
0.3.1	Induction I	4
0.3.2	Induction II (Strong Induction)	5
0.3.3	Division of Integers	5
1	Week 1	9
1.1	Prime Numbers	9
1.1.1	Unique Factorization	10
1.1.2	Fundamental Theorem of Arithmetic	10
1.1.3	Euclid's Theorem	11
1.2	Congruences	11
1.2.1	Properties	11
1.2.2	Linear Congruence	12
1.3	Equivalence Relations	12
1.3.1	Equivalence Classes	12
2	Week 2	14
2.1	Congruence and Equivalent Classes	14
2.1.1	Equivalence Classes	14
2.1.2	Congruence Classes modulo m	15
2.1.3	Invertability	16
2.1.4	Set of Invertible Classes	16
2.2	Euler Totient Function	16
2.2.1	Properties	16
2.2.2	Chinese Remainder Theorem	17
2.3	Groups	18
2.3.1	Abelian Groups	18
2.3.2	Properties	19
3	Week 3	20
3.1	Homomorphisms of Groups	20
3.1.1	Properties	20
3.2	Isomorphisms of Groups	20
3.2.1	Properties	20
3.3	Cyclic Groups	21
3.3.1	Generator	21

3.3.2	Order of a Group	21
3.3.3	Cyclicity	21
4	Appendix	23

Chapter 0

Week 0

0.1 Notation

Let X, Y be sets. Then, we introduce some simple notation: inclusion

$$x \in X$$

union

$$X \cup Y$$

intersection

$$X \cap Y$$

and the cartesian product

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

We call the Natural Numbers \mathbb{N} , Integers \mathbb{Z} , Rationals \mathbb{Q} ($:= \{\frac{a}{b} : a, b \in \mathbb{Z}\}$), Reals \mathbb{R} , and Complex Numbers \mathbb{C} . Notice that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

0.2 Maps

Let X, Y be two sets. A **map** f between X and Y denoted as

$$f : X \rightarrow Y$$

is a rule that takes *every* element of $x \in X$ to *an* element $y = f(x) \in Y$.

0.2.1 Composition

Let X, Y, Z be sets. Suppose $X \xrightarrow{f} Y \xrightarrow{g} Z$. Then a function $h : X \rightarrow Z$, $h(x) = g(f(x)) \in Z$ is called the **composition** denoted as $h = g \circ f$.

0.2.2 Identity

The **identity map** is denoted as $\text{Id}_x : X \rightarrow X$, and is defined to be $\text{Id}(x) = x$

0.2.3 Properties

Let X, Y, Z be sets.

Injective

A map $f : X \rightarrow Y$ is **injective (into/one-to-one)** if for every $x_1, x_2 \in X$, we have $f(x_1) \neq f(x_2)$. Taking the contrapositive, we get the statement: If $f(x_1) = f(x_2)$, then $x_1 = x_2$. In shorthand, it is

$$\forall x_1, x_2 \in X, f(x_1) \neq f(x_2) \iff f(x_1) = f(x_2) \implies x_1 = x_2 \forall x_1, x_2 \in X$$

0.2.4 Surjective

A map $f : X \rightarrow Y$ is **surjective** (*onto*) if for every $y \in Y$, there exists some $x \in X$ such that $y = f(x)$. In shorthand, it is

$$\forall y \in Y, \exists x \in X : y = f(x)$$

0.2.5 Bijective

A map $f : X \rightarrow Y$ is **bijective** if it is both *injective* and *surjective*.

0.2.6 Inverse Maps

Let $f : X \rightarrow Y$ be a map. A map $g : Y \rightarrow X$ is called the **inverse of** f if the composition is the Identity map; that is, $g \circ f = \text{Id}_x$, $f \circ g = \text{Id}_y$ and is denoted as $g = f^{-1}$.

Proposition

A map $f : X \rightarrow Y$ has an inverse *if and only if* f is bijective.

Proof. (\implies) Let $g : Y \rightarrow X$ be an inverse of f . Then $g \circ f = \text{Id}_x$, $f \circ g = \text{Id}_y$. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Then,

$$\begin{aligned} x_1 &= \text{Id}_x(x_1) \\ &= (g \circ f)(x_1) \\ &= g(f(x_1)) \\ &= g(f(x_2)) && f(x_1) = f(x_2) \text{ by assumption} \\ &= (g \circ f)(x_2) \\ &= \text{Id}_x(x_2) \\ x_1 &= x_2 \end{aligned}$$

so f is injective.

Take any $y \in Y$. Then $x := g(y)$ for some $x \in X$. Then,

$$f(x) = f(g(y)) = (f \circ g)(y) = \text{Id}_y(y) = y$$

so f is surjective. Because f is both injective and surjective, it is bijective.

(\impliedby) Assume f be bijective. Then let $g : Y \rightarrow X$. Take any $y \in Y$. There exists a unique $x \in X$ such that $y = f(x)$ because f is bijective. Therefore, g is an inverse of f . \square

0.3 Integers

0.3.1 Induction I

Let $n_0 \in \mathbb{Z}$, and $P(n)$ be a statement for all $n \geq n_0$. Suppose

(i) $P(n_0)$ is true.

(ii) $P(n) \implies P(n+1)$ for every $n \geq n_0$.

Then $P(n)$ is true for all $n \geq n_0$.

Proposition

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Proof. Let $P(n) := 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. We will induct on n .

(i) $P(1)$ is true.

(ii) $P(n) \implies P(n+1)$

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

so $P(n+1)$ is true, completing the induction. □

0.3.2 Induction II (Strong Induction)

Let $n_0 \in \mathbb{Z}$, and $P(n)$ be a statement for all $n \geq n_0$. Suppose

(i) $P(n)$ is true.

(ii) For every $n > n_0$, if $P(k)$ is true for every $n_0 \leq k \leq n$, then $P(n)$ is true.

Then $P(n)$ is true for all $n \geq n_0$.

Proposition

Every positive integer can be written in the form

$$n = 2^{K_1} + 2^{K_2} + \cdots + 2^{K_m}$$

where $K_i \in \mathbb{Z}$ and $0 \leq K_1 < K_2 < \cdots < K_m$.

Proof. We will induct on n .

(i) $P(1)$ is true.

(ii) We know that $P(k)$ is true for $k = 1, 2, \dots, n-1$. Then for n , we find the largest s such that $2^s \leq n$. There are two cases:

(i) $n = 2^s$. Then $P(n)$ is true.

(ii) $2^s < n$, $p := n - 2^s > 0$.

Apply $P(p)$: $p = 2^{K_1} + \cdots + 2^{K_m}$, $0 \leq K_1 < K_2 < \cdots < K_m$.

$\implies n = 2^{K_1} + \cdots + 2^{K_m} + 2^s$ Then, $p > 2^{K_m}$, so $2^s > 2^{K_m}$

$\implies s > K_m$, completing the induction. □

0.3.3 Division of Integers

Let $n, m \in \mathbb{Z}, m \neq 0$. Then, n is divisible by m if there exists some $q \in \mathbb{Z}$ such that $n = mq$ ($\iff \frac{n}{m} \in \mathbb{Z}$) and we denote this as $m \mid n$, read as “ m divides n ”.

Properties

(i) $1 \mid n$ for every $n \in \mathbb{Z}$ and $m \mid 0$ for every $m \neq 0$.

(ii) If $m \mid n_1$ and $m \mid n_2$, then $m \mid (n_1 \pm n_2)$.

Proof. $n_1 = mq_1$ and $n_2 = mq_2$

$\implies n_1 \pm n_2 = mq_1 \pm mq_2 = m(q_1 \pm q_2) \implies m \mid (n_1 \pm n_2)$ since $q_1 \pm q_2 \in \mathbb{Z}$. □

(iii) If $m \mid n$, then $m \mid an$ for all $a \in \mathbb{Z}$.

Proof. $n = m \cdot q, q \in \mathbb{Z}, an = m \cdot (aq), aq \in \mathbb{Z} \implies m \mid an$. □

(iv) If $m \mid n_1$ and $m \mid n_2$, then $m \mid a_1n_1 + a_2n_2$ for every $a_1, a_2 \in \mathbb{Z}$.

Proof. By (iii), $m \mid a_1n_1$ and $m \mid a_2n_2$. By (ii), $m \mid a_1n_1 + a_2n_2$. □

(v) If $m \mid n, n \neq 0$, then $|m| \leq |n|$.

Proof. $n = m \cdot q, q \in \mathbb{Z}, q \neq 0, |n| = |m| \cdot |q| \geq |m|$. □

(vi) If $m \mid n$ and $n \mid m$, then $n = \pm m$.

Proof. By (v), $|m| \leq |n| \leq |m| \implies n = \pm m$. □

Division Algorithm

Theorem

Let $n, m \in \mathbb{Z}, m \neq 0$. Then, there are *unique* $q, r \in \mathbb{Z}$ such that

$$n = m \cdot q + r, 0 < r < m$$

where q is the partial quotient and r is the remainder on dividing n by m .

Proof. Existence

Define an infinite set $S = \{n - mx, x \in \mathbb{Z}\}$ containing nonnegative integers. Take $S \cap \mathbb{Z}^{\geq 0} \neq \emptyset$, so S is non-empty. Then by the well ordering principle, every non-empty set of $\mathbb{Z}^{\geq 0}$ has a least element,

$$n - mx \in S \cap \mathbb{Z}^{\geq 0}$$

Call $q = x, r := n - mx \geq 0$. Then

$$n = mx + r = mq + r$$

To show that $r < m$,

$$r - m = (n - mq) - m = n - m(q + 1) \in S$$

This shows that $r - m < r$, but since we chose r to be the *least* element in $S \cap \mathbb{Z}^{\geq 0}$, $r - m \notin S$. So $r - m < 0 \implies r < m$.

Uniqueness

Let $n = mq_1 + r_1 = mq_2 + r_2$ where $0 \leq r_1, r_2 < m$. Then,

$$0 = m(q_1 - q_2) + (r_1 - r_2)$$

so

$$r_1 - r_2 = m(q_2 - q_1)$$

but

$$q_1 - q_2 = 0$$

so

$$r_1 = r_2$$

□

Remark: $r = 0 \iff m \mid n$ and r contains $m - 1$ distinct integers.

Divisors

Let $n > 0$. A non-zero integer d is called a divider of n if $d \mid n$. Moreover,

$$|d| \leq |n| = n \iff -n \leq d \leq n$$

Proposition

Every $n > 0$ has finitely many unique divisors.

Proof. Let $X := \{1, 2, \dots, n\}$. Then, the set of divisors of n are a subset of X . Since X is finite, any subset of X is also finite. Therefore, n has a finite number of unique divisors. \square

Greatest Common Divisor

Take $n, m > 0$ and d the largest common divisor of m and n . Then,

$$d = \gcd(n, m) = (n, m) \geq 1$$

Euclidean Algorithm

Let $n, m > 0$. Then,

$$\begin{array}{ll} n = mq_1 + r_1 & 0 \leq r_1 < m \\ m = r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{k-2} = r_{k-1}q_k + r_k & 0 \leq r_k < r_{k-1} \\ r_{k-1} = r_kq_{k+1} & r_{k+1} = 0 \end{array}$$

Theorem

$$r_k = \gcd(n, m)$$

Proof. Let $d = \gcd(n, m)$. Then,

$$\begin{array}{ll} d \mid r_1 = n - mq_1 & \\ d \mid r_2 = m - r_1q_2 & r_k \mid r_{k-1} = r_kq_{k+1} \\ d \mid r_3 = r_1 - r_2q_3 & r_k \mid r_{k-2} = r_{k-1}q_k + r_k \\ \vdots & \vdots \\ d \mid r_k = r_{k-2} - r_{k-1}q_k & r_k \mid n = mq_1 + r_1 \end{array}$$

So $d \mid r_k \implies d \leq r_k$, a common divisor of n and m . So, $r_k \leq d$. Thus, $d = r_k$. \square

Bezout's Identity

Theorem

Let $n, m > 0$ and $d = \gcd(n, m)$. Then, there are $x, y \in \mathbb{Z}$ such that

$$d = nx + my$$

Another way of writing this is

$$nx + my = nx + (nm - nm) + my = n(x + m) + m(y - n)$$

Moreover, n and m are relatively prime (coprime) if $\gcd(n, m) = 1$.

Proof. Let $S := \{nx + my, x, y \in \mathbb{Z}\}$. We claim that $s = d$. Then,

$$s = nx + my, \quad n = sq + r, \quad 0 \leq r < s$$

Rearranging the second equation, we get

$$\begin{aligned} r &= n - sq \\ &= n - (nx + my)q && \text{Substitute equation 1} \\ &= n(1 - x) - myq \in S \end{aligned}$$

This implies that $r = 0 \implies (s \mid n \text{ and } s \mid m) \implies s \leq d$. But $d \mid n$ and $d \mid m$, so $d \mid s \implies d \leq s$. Therefore,

$$d = s = nx + my$$

□

Corollary

Let $n, m > 0$. Then, n and m are relatively prime *if and only if* there exists some $x, y \in \mathbb{Z}$ such that $nx + my = 1$

Proof. (\implies) Bezout's Identity

(\impliedby) $nx + my = 1, d = \gcd(n, m)$. Then $d \mid n$ and $d \mid m$ by definition. This implies that $d \mid (nx + my) \iff d \mid 1$. But $d \geq 1 \implies d = 1$. □

Chapter 1

Week 1

1.1 Prime Numbers

An integer $p > 1$ is called **prime** if the *only* divisors of p are ± 1 and $\pm p$. If $n > 0$ and p prime, then

$$\gcd(n, p) = \begin{cases} 1 & n \text{ and } p \text{ are coprime} \\ p & p \mid n \end{cases}$$

Proposition

Every integer $n > 1$ is a product of prime integers.

Proof. We will use strong induction on $n \geq 2$.

(i) ($n_0 = 2$)
2 is prime.

(ii) ($k \implies k + 1$)
Assume $P(k)$ is true for all k such that $2 \leq k < n$. There are two cases.

Case I: n is prime. Then we are done.

Case II: n is composite. Then, there are integers p and q such that $n = p \cdot q$. By definition, $1 < p, q < n$. Then, by the Inductive Hypothesis, $P(p)$ and $P(q)$ are true; i.e. p and q are products of primes. Therefore, $n = p \cdot q$ is a product of primes.

□

Lemma

Let p be a prime integer and $n, m > 0$ such that $p \mid nm$. Then, either

$$p \mid n \text{ or } p \mid m$$

Proof. There are two cases.

Case I: $p \mid n$. Then we are done.

Case II: p and n are coprime. Then, by Bezout's Identity we get

$$\begin{array}{ll} px + ny = 1 & \\ m(px + ny) = m & \text{multiply both sides by } m \\ mpx + mny = m & p \mid pmx, p \mid nm \cdot y \end{array}$$

so $p \mid m$.

□

Corollary

Let p be prime, $n_1, n_2, \dots, n_s > 0$ such that $p \mid n_1 n_2 \cdots n_s$. Then $p \mid n_i$ for some $i < s$.

Proof. We will induct on $s \in \mathbb{N}$.

(i) ($s = 1$)

This is true by the *Lemma* above.

(ii) ($s - 1 \implies s$)

Consider $p \mid (n_1 n_2 \cdots n_s - 1) \cdot n_s$. Then either $p \mid (n_1 n_2 \cdots n_s - 1)$ by the Inductive Hypothesis or $p \mid n_s$.

□

1.1.1 Unique Factorization

Let $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ and p_i, q_j be prime for all $i, j < s, t$. Then, their factorizations are the same if $s = t$ and $q_j = p_{\alpha(j)}$ for every $j = 1, 2, \dots, t$ where $\alpha : \{1, 2, \dots, s\} = \{1, 2, \dots, t\}$

1.1.2 Fundamental Theorem of Arithmetic

Theorem

Every integer $n > 1$ admits a unique factorization into a product of primes.

Proof. Let $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ and p_i, q_j be prime for all $i, j < s, t$. We will induct on $s \in \mathbb{N}$.

(i) ($s = 1$)

$n = p_1 = q_1$ is true.

(ii) ($s - 1 \implies s$)

$p_s \mid n = q_1 q_2 \cdots q_t \xRightarrow{\text{Corollary}} p_s \mid q_j$ for some integer $j \implies p_s = q_j$. Reorder the terms to get $j = t$. Then, $p_s = q_t$. We are left with $p_1 p_2 \cdots p_{s-1} = q_1 q_2 \cdots q_{t-1}$. Apply P($s - 1$) to get that $s - 1 = t - 1$. Then, $q_j = p_i$ up to the permutation. That is, $p_s = q_s$.

□

Proposition

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, $a_k, b_k \geq 0$. Then $m \mid n$ if and only if $b_1 \leq a_1, b_2 \leq a_2, \dots, b_k \leq a_k$.

Proof. (\implies)

$$n = m$$

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \right) \cdot q$$

Then, $b_1 \leq a_1 \iff a_1 = b_1 + c, q = p_1^{c_1} \cdots p_k^{c_k}, c_k \geq 0$.

(\impliedby) $n = mq$ where $q = p_1^{a_1 - b_1} \cdots p_k^{a_k - b_k}$. Since $a_i \geq b_i, a_i - b_i \geq 0 \forall i < k \implies m \mid n$

□

1.1.3 Euclid's Theorem

Theorem

There are infinitely many primes.

Proof. Suppose by contradiction that there are exactly n primes $\{p_1, p_2, \dots, p_n\}$. Define $N := p_1 p_2 \cdots p_n + 1 > 1$. Let p be a divisor of N and $p = p_i$ for some i . Then, $1 = N - p_1 p_2 \cdots p_n \implies p_i \mid 1$, a contradiction. \square

1.2 Congruences

Let $m > 0$ be an integer. We say that two integers are **congruent** modulo m if

$$m \mid (b - a)$$

and denote it as

$$a \equiv b \pmod{m}$$

Proposition

$a \equiv b \pmod{m}$ if and only if a and b have the same remainder on dividing by m .

Proof. (\implies) $a \equiv b \pmod{m}$ can be rewritten as $m \mid (b - a)$ or $b - a = mx$ where $a = mq + r$, $0 \leq r < m$. Then,

$$\begin{aligned} b &= a + mx \\ &= (mq + r) + mx && \text{substitute } a \\ &= m(q + x) + r \end{aligned}$$

(\impliedby) Suppose $a = mq + r$ and $b = ms + r$, where $0 \leq r < m$. Then

$$b - a = ms - mq = m(s - q) \implies m \mid (b - a) \iff a \equiv b \pmod{m}$$

\square

Corollary

Every integer is congruent modulo m to exactly one integer in the set

$$\{0, 1, \dots, m - 1\}$$

Proof. Let $a = mq + r$ where $0 \leq r < m$. Then, $r = m \cdot 0 + r \implies a \equiv r \pmod{m}$ where $r \in \{0, 1, \dots, m - 1\}$ \square

1.2.1 Properties

(i) $a \equiv b \pmod{m} \implies ax \equiv bx \pmod{m}$ for every $x \in \mathbb{Z}$.

$$\text{Proof. } m \mid (b - a) \implies m \mid (b - a)x = bx - ax$$

\square

(ii) $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

$$\text{Proof. } m \mid (b_1 - a_1) \text{ and } m \mid (b_2 - a_2) \implies m \mid (b_1 - a_1) + (b_2 - a_2) = (b_1 + b_2) - (a_1 + a_2).$$

\square

(iii) $a_1 \equiv b_1 \pmod{m}, a_1 \equiv b_1 \pmod{m} \implies a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Proof. $b_1 b_2 - a_1 a_2 = b_1 b_2 (-a_1 b_2 + a_1 b_2) + a_1 a_2 = (b_1 - a_1) b_2 + a_1 (b_2 - a_2)$. Here, $m \mid (b_1 - a_1)$ and $m \mid (b_2 - a_2)$ by assumption. Then, $m \mid (b_1 b_2 - a_1 a_2)$. \square

1.2.2 Linear Congruence

$ax \equiv b \pmod{m}$ for $m > 0, a, b \in \mathbb{Z}$.

Proposition

If $\gcd(a, m) = 1$, then there is an integer solution x .

Proof.

$$\begin{array}{ll} ay + mz = 1 & \text{Bezout's Identity} \\ b(ay + mz) = b & \text{multiply both sides by } b \\ aby + mbz = b & \\ \iff & \\ b - aby = mbz & \end{array}$$

Take $x := aby$. \square

1.3 Equivalence Relations

Let X be a set. A **relation** $a \sim b$ on X is a subset $\Omega \subset X \times X$. That is, for every $a, b \in X$, $a \sim b$ if $(a, b) \in \Omega$. A relation on X is called an **equivalence relation** if

- (i) Reflexive: $a \sim a$ for every $a \in X$
- (ii) Symmetric $a \sim b \implies b \sim a$ for every $a, b \in X$
- (iii) Transitive $a \sim b, b \sim c \implies a \sim c$ for every $a, b, c \in X$

1.3.1 Equivalence Classes

Let X be a set and \sim an equivalence relation. Then,

$$a \in X, X_a := \{b \in X : b \sim a\} \subset X$$

is an **equivalence class** of a .

Proposition

Let \sim be an equivalence relation on a set X . Then

- (i) If $a \sim b$, $X_a = X_b$. If $a \not\sim b$, then $X_a \cap X_b = \emptyset$.
- (ii) a and b belong to the same equivalence class *if and only if* $a \sim b$.
- (iii) X is the disjoint union of all equivalence classes.

Proof. (i) Suppose $a \sim b$. Take any $c \in X_a$. Then

$$\begin{aligned} c \sim a &\implies c \sim b \implies c \in X_b \implies X_a \subset X_b \\ c \sim b &\implies c \sim a \implies c \in X_a \implies X_b \subset X_a \end{aligned}$$

so $X_a = X_b$.

Assume $a \not\sim b$ by contradiction. Take $c \in X_a \cap X_b \implies c \sim a$ and $c \sim b \implies a \sim b$, a contradiction.

(ii) (\implies) Suppose $a, b \in X_c$. Then $a \sim c, b \sim c \implies c \sim b \implies a \sim b$.

(\impliedby) Suppose $a \sim b$. Then by (i), $a \in X_a = X_b \ni b$.

(iii) Suppose $a \in X_a$. Then, $\bigcup X_a = X$.

□

Note: The set of all equivalence relations on X is the same as the set of all partitions of X into disjoint union of subsets. That is, $X = \bigcup X_a$.

Chapter 2

Week 2

2.1 Congruence and Equivalent Classes

Proposition

$\equiv \pmod{m}$ is an equivalence relation for all $m \in \mathbb{N}$.

Proof. (i) Reflexive: Let $a, m \in \mathbb{Z}$. Then $m \mid a - a = 0$. So $a \equiv a \pmod{m}$.

(ii) Symmetric: Suppose $a \equiv b \pmod{m}$. Then $m \mid (b - a)$. Then $a - b = -(b - a) \implies b \equiv a \pmod{m}$.

(iii) Transitive: Suppose $a \equiv b$, $b \equiv c$. Then,

$$c - a = c(-b + b) - a = (c - b) + (b - a) \implies m \mid (c - a)$$

□

2.1.1 Equivalence Classes

The ***congruence class*** of m is denoted as

$$[a] := [a]_m := \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}$$

For example, $[2]_5 = \{\dots, -8, -3, 2, 7, \dots\}$.

Properties

(i) $[a] = [b] \iff a \equiv b \pmod{m}$.

(ii) $[a] \cap [b] = \emptyset \iff a \not\equiv b \pmod{m}$.

(iii) Integers a, b belong to the same congruence class if and only if $a \equiv b \pmod{m}$.

(iv) \mathbb{Z} is a disjoint union of congruence classes.

(v) There are exactly m congruence classes modulo m ($[0], [1], \dots, [m-1]$).

Proof. (At least)

Suppose $0 \leq j < k \leq m-1$. Then

$$0 < k - j \leq m - 1 < m \implies m \nmid (k - j) \implies j \not\equiv k \pmod{m}$$

(No more)

Let $[k]$ be a congruence class. Then $k = am + r$ where $0 \leq r < m$. We can rewrite this as

$$k - r = am \implies m \mid (k - r) \implies [k] = [r]$$

Therefore, there are exactly m congruence classes modulo m .

□

2.1.2 Congruence Classes modulo m

We denote congruence classes modulo m as

$$\mathbb{Z}/m\mathbb{Z} := \{\text{congruence classes mod } m\}$$

Addition

We will define addition as

$$[a]_m + [b]_m = [a + b]_m$$

Proof. We know

$$a' \equiv a \pmod{m}$$

$$b' \equiv b \pmod{m}$$

Then

$$m \mid a - a'$$

$$m \mid b - b'$$

or

$$(a + b) - (a' + b') = (a - a') + (b - b') \implies m \mid (a - a') + (b - b')$$

So $+$ is well-defined. □

Properties

(i) Commutativity: $[a]_m + [b]_m = [b]_m + [a]_m$.

$$\text{Proof. } [a]_m + [b]_m = [a + b]_m = [b + a]_m = [b]_m + [a]_m. \quad \square$$

(ii) Associativity: $([a]_m + [b]_m) + [c]_m = [a]_m + ([b]_m + [c]_m)$.

$$\text{Proof. Trivial.} \quad \square$$

(iii) Identity: $[a]_m + [0]_m = [a]_m$.

$$\text{Proof. } [a]_m = [a + 0]_m = [a]_m + [0]_m = [a]_m. \quad \square$$

(iv) Inverse: $[a]_m + [-a]_m = [0]_m$.

$$\text{Proof. } [a]_m + [-a]_m = [a + (-a)]_m = [0]_m. \quad \square$$

Multiplication

We will define multiplication as

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

Proof. We know

$$a' \equiv a \pmod{m}$$

$$b' \equiv b \pmod{m}$$

Then

$$m \mid a - a'$$

$$m \mid b - b'$$

or

$$(a \cdot b) - (a' \cdot b') = ab - ab' - a'b + a'b' = a(b - b') + a'(b - b') \implies m \mid (a'b' - ab)$$

So \cdot is well-defined. □

Properties

(i) Commutativity: $[a]_m \cdot [b]_m = [b]_m \cdot [a]_m$.

Proof. $[a]_m \cdot [b]_m = [a \cdot b]_m = [b \cdot a]_m = [b]_m \cdot [a]_m$. □

(ii) Associativity: $([a]_m \cdot [b]_m) \cdot [c]_m = [a]_m \cdot ([b]_m \cdot [c]_m)$.

Proof. *Trivial.* □

(iii) Identity: $[a]_m \cdot [1]_m = [a]_m$.

Proof. $[a]_m = [a \cdot 1]_m = [a]_m \cdot [1]_m = [a]_m$. □

(iv) Distributivity: $[a]_m \cdot ([b]_m + [c]_m) = [a]_m[b]_m + [a]_m[c]_m$.

Proof. $[a]_m \cdot ([b]_m + [c]_m) = [a \cdot (b + c)]_m = [ab + ac]_m = [ab]_m + [ac]_m = [a]_m[b]_m + [a]_m[c]_m$ □

2.1.3 Invertability

We say that $[a]_m$ is **invertible** if there exists some $[a]_m^{-1}$ such that

$$[a]_m[b]_m = [1]_m$$

Theorem

A class $[a]_m$ is invertible if and only if $\gcd(a, m) = 1$.

Proof. (\implies) Assume $[a]_m$ is invertible. Then by definition there is some $[b]_m$ such that $[a]_m[b]_m = [ab]_m = [1]_m \implies m \mid (ab - 1) \implies ab - 1 = km \iff ab - km = 1$. Suppose $d \mid a$ and $d \mid m$. Then

$$d \mid (ab - km) = 1$$

$$d \mid 1 \implies d = 1$$

(\impliedby) Assume $\gcd(a, m) = 1$. Then, there is an integer solution to $ax \equiv 1 \pmod{m}$. Then, $[ax]_m = [a]_m[x]_m = [1]_m \implies [a]_m$ is invertible. □

2.1.4 Set of Invertible Classes

We denote the set of invertible classes as

$$(\mathbb{Z}/m\mathbb{Z})^\times := \{[a]_m : [a]_m \text{ is invertible}\}$$

Note: $m = p$ a prime $\implies |(\mathbb{Z}/m\mathbb{Z})^\times| = p - 1$.

2.2 Euler Totient Function

We denote the number of integers $1, \dots, m - 1$ coprime to m as

$$\varphi(m)$$

2.2.1 Properties

(i) $m = p$ a prime $\implies \varphi(p) = p - 1$.

(ii) $m = p^k \implies \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

Proof. In the set $\{1, 2, \dots, p^k\}$, every p -th number is a multiple of p . There are p^{k-1} such elements in this set. Therefore, the elements that are coprime to p are $p^k - p^{k-1} = p^{k-1}(p - 1)$. □

2.2.2 Chinese Remainder Theorem

Lemma

Let $a \mid n$ and $b \mid n$. If $\gcd(a, b) = 1$, then $ab \mid n$.

Proof. Let $\gcd(a, b) = 1$. Then,

$$\begin{array}{ll} ax + by = 1 & \text{Bezout's Identity} \\ n(ax + by) = n & \text{multiply both sides by } n \\ nax + nby = n & \end{array}$$

By assumption, $a \mid n$ and $b \mid n$ so $ab \mid an$ and $ab \mid bn \implies ab \mid n$. \square

Corollary

Suppose $m_1 \mid n, m_2 \mid n, \dots, m_k \mid n$ for $m_i \neq m_j, i \neq j$ (pairwise relatively prime). Then $m_1 m_2 \cdots m_k \mid n$.

Proof. We will induct on $k \geq 2$.

(i) ($k = 2$) By the *Lemma*, this is true.

(ii) ($k = k + 1$) Consider $m_1(m_2 \cdots m_k)$. Then $\gcd(m_1, m_i) = 1$ for $i \leq k$. Then $(m_1, m_2 \cdots m_k) = 1$. By the Inductive Hypothesis, $m_2 \cdots m_k \mid n$. By the *Lemma*, $m_1 m_2 \cdots m_k \mid n$. \square

Proposition

If $m \mid n$, then $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$. That is,

$$[a]_n \mapsto [a]_m$$

Proof. Suppose $[a]_n = [a']_n$. Then $a \equiv a' \pmod{n}$. So

$$m \mid n \mid (a - a') \implies m \mid (a - a') \implies [a]_m = [a']_m$$

So \mapsto is well-defined.

We will now consider $n := m_1 m_2 \cdots m_k$ for some integer k . Then

$$f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

or

$$[a]_n \mapsto ([a]_{m_1} \mapsto [a]_{m_2} \mapsto \cdots \mapsto [a]_{m_k})$$

\square

Theorem

If m_i are pairwise relatively prime, then f (defined above) is a bijection.

Proof. Injective

Assume $f([a]_n) = f([b]_n)$. Then

$$([a]_{n_1}, \dots, [a]_{n_k}) = ([b]_{n_1}, \dots, [b]_{n_k})$$

$$[a]_i = [b]_i \forall i < n \implies m_i \mid (b - a) \implies \prod m_i \mid (b - a) \iff n \mid (b - a) \implies [a]_n = [b]_n$$

Surjective

Trivial. Since f is both injective and surjective, f is a bijection. \square

Note: the size of $\mathbb{Z}/n\mathbb{Z}$ is $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}|$

Theorem

Consider the following system of congruences:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

If m_1, \dots, m_k are pairwise relatively prime, then there is an integer solution to the above system of congruences.

Proof. Since $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ is a bijection, there is some $[x]_n$ such that $f([x]_n) = ([b]_{m_1}, \dots, [b]_{m_k})$ by surjectivity, so $[x]_{m_i} = [b_i]_{m_i} \implies x \equiv b_i \pmod{m_i} \forall i < k$. **(i)**

Suppose $[x]_{m_i} = [y]_{m_1}$. Then,

$$m_i \mid (x - y) \implies \prod m_i \mid (x - y)$$

so $[x]_n = [y]_n$. Let $[x]_n$ be a solution; i.e. $y \in [x]_n$. Then

$$m_i \mid n \mid (y - x) \implies m_i \mid (y - x) \implies [y]_m = [x]_m$$

□

2.3 Groups

Let G be a set. A binary operation, \cdot , on G is a map

$$G \times G \rightarrow G$$

such that

$$(a, b) \mapsto a \cdot b$$

A set G with a binary operation \cdot is a **group** if

- (i) Associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (ii) Unique Identity: There exists an $e \in G$ such that $a \cdot e = e \cdot a = a$.
- (iii) Unique Inverse: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

2.3.1 Abelian Groups

A group is said to be **abelian** if for every $a, b \in G$, \cdot is commutative; i.e.

$$a \cdot b = b \cdot a$$

Note: If G is abelian, we usually denote the binary operator as $+$, inverse as $-a$, and identity as 0 .

2.3.2 Properties

(i) Unique Identity e .

Proof. Let e_1, e_2 be two identities. Then, since e_1 is an identity, we get

$$e_1 \cdot e_2 = e_2$$

but since e_2 is an identity, we get

$$e_1 \cdot e_2 = e_1$$

so $e_1 = e_2$. □

(ii) Unique Inverse e .

Proof. Let a_1, a_2 be two inverses. Then

$$a_1 = a_1 \cdot e = a_1 \cdot (a \cdot a_2) = (a_1 \cdot a) \cdot a_2 = e \cdot a_2 = a_2$$

□

(iii) Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iv) $(a^{-1})^{-1} = a$

Proof. $a^{-1} \cdot a = a \cdot a^{-1} = e \implies a = (a^{-1})^{-1}$ □

(v) Powers.

$$a^0 = e$$

$$a^n = a \cdot a \cdots a$$

n times

$$a^{-n} = (a^n)^{-1} = (a^{-1})^n = a^{-1} \cdot a^{-1} \cdots a^{-1}$$

n times

(vi) Inverse: $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. $e = (ab) \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.

$e = (b^{-1}a^{-1}) \cdot (ab) = a^{-1}(b^{-1}b)a = a^{-1}ea = a^{-1}a = e$. □

(vii) Cancellation: $ax = bx \implies a = b$.

Proof. $a = ae = a(xx^{-1}) = (ax)x^{-1} = (bx)x^{-1} = b(xx^{-1}) = be = b$. □

Note: $xa = xb \implies a = b$ but $ax = xb \not\implies a = b$ since G need not be abelian!

Chapter 3

Week 3

3.1 Homomorphisms of Groups

Let G, H be two groups. A **homomorphism** between G and H is a map

$$f : G \rightarrow H$$

such that

$$H \ni f(x \cdot y) = f(x) \cdot f(y) \in H$$

for every $x, y \in G$.

3.1.1 Properties

Let $f : G \rightarrow H$ be a homomorphism.

(i) $f(e_G) = e_H$.

Proof. $f(e_G) \cdot f(e_G) = f(e_G \cdot e_G) = f(e_G) = e_H$ □

(ii) $f(x^{-1}) = f(x)^{-1}$ for every $x \in G$.

Proof.

$$e_H = f(x^{-1}) \cdot f(x) = f(x^{-1} \cdot x) = f(e_G) = e_H$$

$$e_H = f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_H$$
□

3.2 Isomorphisms of Groups

A homomorphism $f : G \rightarrow H$ is an **isomorphism** if f is a bijection. Two groups are called **isomorphic** if there is an isomorphism $f : G \rightarrow H$.

3.2.1 Properties

(i) $\text{Id}_G : G \rightarrow G$ is an isomorphism.

(ii) If f is an isomorphism, so is $f^{-1} : H \rightarrow G$.

Proof. Let f^{-1} be a bijection. Then,

$$\exists x \in G : f(x) = a \implies x = f^{-1}(a)$$

$$\exists y \in G : f(y) = b \implies y = f^{-1}(b)$$

Then,

$$\begin{aligned} f(x \cdot y) &= f(x) \cdot f(y) = ab \\ f^{-1}(ab) &= xy = f^{-1}(a) \cdot f^{-1}(b) \end{aligned}$$

□

(iii) If $f : G \rightarrow H$ and $f' : H \rightarrow K$ are isomorphisms, then so is $f' \circ f : G \rightarrow K$.

Theorem

The relation \simeq is an equivalence relation.

Proof. (i) $\text{Id}_G : G \rightarrow G$ is an isomorphism.

(ii) If f is an isomorphism, so is $f^{-1} : H \rightarrow G$.

Proof. Let f^{-1} be a bijection. Then,

$$\begin{aligned} x \in G : f(x) = a &\implies x = f^{-1}(a) \\ y \in G : f(y) = b &\implies y = f^{-1}(b) \end{aligned}$$

Then,

$$\begin{aligned} f(x \cdot y) &= f(x) \cdot f(y) = ab \\ f^{-1}(ab) &= xy = f^{-1}(a) \cdot f^{-1}(b) \end{aligned}$$

□

(iii) If $f : G \rightarrow H$ and $f' : H \rightarrow K$ are isomorphisms, then so is $f' \circ f : G \rightarrow K$.

□

3.3 Cyclic Groups

3.3.1 Generator

Let G be a group, and $a \in G$. The element **generates** G if every $x \in G$ can be written as

$$x = a^i$$

for some $i \in \mathbb{Z}$. We say that a is a **generator** of G .

3.3.2 Order of a Group

Let G be a group, and $a \in G$. The smallest $n > 0$ such that $a^n = e$ is called the **order** of a and is denoted as

$$\text{ord}(a) = n$$

Note that $\text{ord}(a) = \infty$ if such an n does not exist.

3.3.3 Cyclicity

A group G is called **cyclic** if G has a generator.

Theorem

Every cyclic group is isomorphic to either \mathbb{Z} or $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 0$.

Properties

Proposition

$[a]_n \in \mathbb{Z}/n\mathbb{Z}$ a generator if and only if $\gcd(a, n) = 1$. There are $\varphi(n)$ generators of $\mathbb{Z}/n\mathbb{Z}$.

Proof. (\implies) There exists some $i \in \mathbb{Z}$ such that $i \cdot [a]_n = [1]_n$. Then

$$[ia]_n = [1]_n \implies ia \equiv 1 \pmod{n} \iff n \mid ia - 1 \iff ia - 1 = nm \iff \gcd(a, n) = 1$$

(\impliedby) Let $\gcd(a, n) = 1$. Then for some $x, y \in \mathbb{Z}$,

$$1 = ax + ny$$

But $1 - ax$ is divisible by n , so we get

$$1 \equiv ax \pmod{n} \iff [1]_n = [ax]_n = x \cdot [a]_n$$

Now, take any $[b]_n \in \mathbb{Z}/n\mathbb{Z}$. We have that

$$[b]_n \equiv bx[a]_n$$

so $[a]_n$ is a generator of $\mathbb{Z}/n\mathbb{Z}$. □

Proposition

Let G be a cyclic group of order n . Then $\sigma \in G$ be a generator if and only if $\text{ord}(\sigma) = n$.

Proof. (\implies) Consider the powers of σ . $\sigma^0 = e$, $\sigma^1 = \sigma$, \dots , $\sigma^k = e$, $\sigma^{k+1} = \sigma$, \dots , $\sigma^{2k} = e$. Take k to be the smallest integer such that $\sigma^k = \sigma^i$ for $i \leq i \leq k$. We claim that $i = 0$.

If $i > 0$, we have $\sigma^{k-1} = \sigma^{i-1}$ for $0 \leq i < k$ a contradiction. Then $\sigma^k = \sigma^0 = e$. So $n = |G| = k \implies n$ is the smallest integer such that $\sigma^n = e$. So $n = \text{ord}(\sigma)$.

(\impliedby) By definition, n is the smallest integer such that $\sigma^n = e$. Then,

$$\{e, \sigma^1, \sigma^2, \dots, \sigma^{n-1}\}$$

are distinct elements. This shows that

$$G = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$$

That is, σ generates G . Thus, $|G| = n = \text{ord}(\sigma)$. □

Chapter 4

Appendix

Binomial Expansion

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Geometric Series

Finite:

$$S = \frac{a(1 - r^n)}{1 - r}$$

$$S = \frac{a}{1 - r}$$