

Preliminaries

Contents

| | | |
|----------|--|----------|
| 1 | Basics | 2 |
| 2 | Properties of Integers | 3 |
| 3 | $\mathbb{Z}/n\mathbb{Z}$: The integers modulo n | 5 |

1 Basics

Definition. (Functions) Let $f : A \rightarrow B$

1. **(injection)** $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
2. **(surjection)** image of f is all of B , i.e. $\forall b \in B \exists a \in A f(a) = b$
3. **(left inverse)** a function $g : B \rightarrow A$ such that $g \circ f : A \rightarrow A$ is the identity map on A
4. **(right inverse)** a function $h : B \rightarrow A$ such that $f \circ h : B \rightarrow B$ is the identity map on B

Proposition. Let $f : A \rightarrow B$

1. f is injective if and only if f has a left inverse
2. f is surjective if and only if f has a right inverse
3. f is bijective if exists $g : B \rightarrow A$ such that $f \circ g$ is identity map on B and $g \circ f$ is identity map on A (g is the two-sided inverse)
4. If A, B are finite sets and $|A| = |B|$, then f is bijective iff f is injective iff it is surjective

Definition. (Permutation, Restriction, Extension)

1. **(permutation)** of set A is a bijection from A to itself
2. **(restriction)** If $A \subset B$ and $f : B \rightarrow C$, $f|_A$ is restriction of f to A .
3. **(extension)** If $A \subset B$ and $g : A \rightarrow C$ and there is a function $f : B \rightarrow C$ such that $f|_A = g$, then f is an extension of g to B

Definition. (Equivalence Relation & Partition)

1. **(binary relation)** on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$
2. **(relation)** \sim on A is an equivalence relation if it is
 - (reflexive) $a \sim a$ for all $a \in A$
 - (symmetric) $a \sim b$ implies $b \sim a$, for all $a, b \in A$
 - (transitive) $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$
3. **(equivalence class)** Given \sim on A , the equivalence class of $a \in A$ is $\{x \in A \mid x \sim a\}$. If C is any equivalence class, any element of C is a representative to class C
4. **(partition)** of A is any collection $\{A_i \mid i \in I\}$ of nonempty subsets of A , for some indexing set I such that
 - $A = \cup_{i \in I} A_i$
 - $A_i \cap A_j = \emptyset$ for all $i, j \in I$ with $i \neq j$

Proposition. (Equivalence relation and partition are the same) Let A be nonempty set

1. If \sim is an equivalence relation on A then the set of equivalence classes of \sim forms a partition of A
2. If $\{A_i \mid i \in I\}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i , $i \in I$

2 Properties of Integers

Definition. (Properties of \mathbb{Z})

1. **(well ordering of \mathbb{Z})** If $A \subset \mathbb{Z}^+$, exists $m \in A$ such that $m \leq a$ for all $a \in A$ (m is minimal element of A)
2. **(divides)** If $a, b \in \mathbb{Z}$ and $a \neq 0$, $a \mid b$ if there is an element $c \in \mathbb{Z}$, such that $b = ac$. Otherwise, $a \nmid b$
3. **(g.c.d.)** If $a, b \in \mathbb{Z} - \{0\}$, there is unique $d \in \mathbb{Z}^+$, the greatest common divisor (a, b) of a, b satisfying
 - (a) d is a common divisor of a, b ($d \mid a$ and $d \mid b$)
 - (b) d is greatest such divisor (If $e \mid a$ and $e \mid b$, then $e \mid d$)

Intuitively, an a -by- b rectangle can be covered with square tiles of side-length c only if c is a common divisor of a and b . gcd of a and b is the largest of such c

4. **(relative prime)** If $(a, b) = 1$, then a, b are relative prime
5. **(l.c.m)** If $a, b \in \mathbb{Z} - \{0\}$. there is unique $l \in \mathbb{Z}^+$, the least common multiple of a, b satisfying
 - (a) l is a common multiple of a and n ($a \mid l$ and $b \mid l$)
 - (b) l is least of such multiple (If $a \mid m$ and $b \mid m$, then $l \mid m$)
6. **(Relation between g.c.d. and l.c.m)** Let $a, b \in \mathbb{Z} - \{0\}$, let $d = (a, b)$ and $l = \text{l.c.m.}(a, b)$, then $dl = ab$
7. **(The Division Algorithm)** If $a, b \in \mathbb{Z} - \{0\}$ there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$, where q is the quotient and r is the remainder.
8. **(Euclidean Algorithm)** is a procedure that generates g.c.d. of two integers by iterating the division algorithm. Idea is g.c.d. of a, b where $a > b$ is same as g.c.d. of $b, a - b$. Or equivalently.

$$\begin{aligned}
 a &= q_0 b + r_0 \\
 b &= q_1 r_0 + r_1 \\
 r_0 &= q_2 r_1 + r_2 \\
 &\vdots \\
 r_{n-2} &= q_n r_{n-1} + r_n \\
 r_{n-1} &= q_{n+1} r_n
 \end{aligned}$$

where $r_n = (a, b)$ is the last nonzero remainder

9. **(Consequence of Euclidean Algorithm)** If $a, b \in \mathbb{Z} - \{0\}$, then exists $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

by reversing steps of Euclidean algorithm

10. **(prime)** $p \in \mathbb{Z}^+$ is called a prime if $p > 1$ and the only positive divisors of p are 1 and p . An integer greater than 1 which is not prime is composite. For any prime number p where $p \mid ab$ for some $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$
11. **(fundamental theorem of arithmetic)** If $n \in \mathbb{Z}$ and $n > 1$, then n can be factored uniquely into products of primes, i.e. exists distinct p_1, \dots, p_s and $\alpha_1, \dots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

Additionally suppose $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$ where α_i, β_i can be 0. then

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$$

and l.c.m. is obtained by taking maximum of α_i, β_i instead of minimum

- $57970 = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 31$ and $10353 = 3 \cdot 7 \cdot 17 \cdot 19$, then $(57970, 10353) = 17$

12. (**Euler φ -function**) for $n \in \mathbb{Z}^+$, let $\varphi(n)$ be number of positive integers $a \leq n$ with a relative prime to n , i.e. $(a, n) = 1$.

- $\varphi(12) = 4$ (1, 5, 6, 7)

3 $\mathbb{Z}/n\mathbb{Z}$: The integers modulo n

Definition. (Integer Modulo n)

1. **(modulo relation)** Define $a \sim b$ iff $n \mid (b - a)$. \sim satisfies axioms for a relation
2. **(congruence)** a is congruent to $b \pmod n$ iff $a \equiv b \pmod n$ iff $a \sim b$
3. **(congruence/residue class of $a \pmod n$)** is the equivalence class by congruent modulo n , consisting of integers which differ from a by an integral multiple of n , i.e.

$$\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$$

There are n distinct equivalence classes $\pmod n$, i.e. $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Specifically, \bar{i} are integers which leave a remainder of i when divided by n

4. **(integer modulo n group)** $\mathbb{Z}/n\mathbb{Z} = (\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}, \sim)$
5. **(reducing $a \pmod n$)** is the process of finding the equivalence class $\pmod n$ of some integer a . Specifically, this is referring to finding the smallest nonnegative integer congruent to $a \pmod n$
6. **(modular arithmetic)** Let $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, define sum and product by $\bar{a} + \bar{b} = \overline{a + b}$ and $\bar{a} \cdot \bar{b} = \overline{ab}$.
7. **(theorem)** Modular Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ is well defined; the sum/product of the residue classes does not depend on the choice of representatives chosen. Specifically, if $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ with $\bar{a}_1 = \bar{b}_1$ and $\bar{a}_2 = \bar{b}_2$ then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$.
- $(\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z}$ are residue classes which have a multiplicative inverse

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \bar{c} \in \mathbb{Z}/n\mathbb{Z} \ \bar{a} \cdot \bar{c} = \bar{1}\} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

- (example) $(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ ($(3, 9) \neq 1$ and $(6, 9) \neq 1$), with inverses $\{\bar{1}, \bar{5}, \bar{7}, \bar{2}, \bar{4}, \bar{8}\}$
- (method) for computing inverse of $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. The condition for inverse is $\overline{aa^{-1}} = \bar{1}$ or $aa^{-1} \equiv 1 \pmod n$. Since \bar{a} is in $(\mathbb{Z}/n\mathbb{Z})^\times$, $(a, n) = 1$ holds, then exists $x, y \in \mathbb{Z}^+$ such that $ax + ny = 1$, i.e. $ax \equiv 1 \pmod n$ the desired condition for inverses. Therefore, \bar{x} is the multiplicative inverse of \bar{a} . So to find inverse for \bar{a} , we simply use Euclidean algorithm to compute the coefficient x
- (example) For $(\mathbb{Z}/60\mathbb{Z})^\times$ and $a = 17$. Apply Euclidean algorithm,

$$60 = (3)17 + 9$$

$$17 = (1)9 + 8$$

$$9 = (1)8 + 1$$

$(a, n) = 1$ so $\bar{a} \in (\mathbb{Z}/60\mathbb{Z})^\times$ and $(-7)17 + (1)60 = 1$. So $\overline{-7} = \overline{53}$ is multiplicative inverse of $\overline{17}$