Preliminaries

Contents

1 Basics

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

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 $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A*
4. ***(right inverse)*** *a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B*

Proposition. *Let $f : A \to B$*

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 $g : B \to A$ 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 $f : B \to C$, $f|_A$ is restriction of f to A.*
3. ***(extension)*** *If $A \subset B$ and $g : A \to C$ and there is a function $f : B \to C$ 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* $m \le a$ *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* $l = l.c.m.(a, b)$, *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* $0 \le r < |b|$, *where* q *is the quotient and* r *is the reminder.*

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 reminder*

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 positie 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. ***(foundamental theorem of arithemtic)*** *If* $n \in \mathbb{Z}$ *and* $n > 1$, *then* n *can be factored uniquely into products of primes, i.e. exists distinct* $p_1, \cdots, p_s$ *and* $\alpha_1, \cdots, \alpha_s$ *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. $(a, n) = 1$. Then for any prime powers p^a for some $a \geq 1$,*

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

and for any $n \in \mathbb{Z}^+$,

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

where $p \mid n$ are the distinct prime numbers dividing n.

Proof. **(1)** Since p is prime, $(m, p^a) \in \{1, p, p^2, \cdots, p^a\}$. The only time $(m, p^a) \neq 1$ is when m is some multiple of p, i.e. $m \in \{p, 2p, 3p, \cdots, p^k\}$ which has order p^{k-1}. Therefore $\varphi(p^a) = p^a - p^{a-1}$, exactly when $(m, p^a) = 1$ **(2)** Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ by foundamental theorem of arithmetic, therefore

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) \\
&= p_1^{\alpha_1}(1 - \frac{1}{p_1}) p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_s^{\alpha_s}(1 - \frac{1}{p_s}) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}(1 - \frac{1}{p_1})(1 - \frac{2}{p_2}) \cdots (1 - \frac{1}{p_s}) \\
&= n \prod_{p|n} (1 - \frac{1}{p})
\end{aligned}$$

□

- *(fact) φ is multiplicative*

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad (a, b) = 1$$

- *(example)* $\varphi(12) = \varphi(2^2)\varphi(3) = (12)(1 - 1/2)(1 - 1/3) = 4$ *(1,5,6,7 are coprime to 12)*
- ***(theorem)*** $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$

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* $\mod n$ *iff* $a \equiv b \,(mod\;\; n)$ *iff* $a \sim b$
3. ***(congruence/residue class of*** $a \mod n$***)*** *is the equivalence class by congruent modulo n, consisting of integers which differ from a by an integral multiple of n, i.e.*

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

There are n distanct equivalence classes $\mod n$, *i.e.* $\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$. *Specifically.* $\overline{i}$ *are integers which leave a reminder of i when divided by n*

4. ***(integer modulo*** n ***group)*** $\mathbb{Z}/n\mathbb{Z} = \left(\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}, \sim\right)$
5. ***(reducing*** $a \mod n$***)*** *is the process of finding the equivalence class mod n of some integer a. Specifically, this is refering to finding the smallest nonnegative integer congruent to* $a \mod n$
6. ***(modular arithmetic)*** *Let* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, *define sum and product by* $\overline{a} + \overline{b} = \overline{a+b}$ *and* $\overline{a} \cdot \overline{b} = \overline{ab}$.
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* $\overline{a_1} = \overline{b_1}$ *and* $\overline{a_2} = \overline{b_2}$ *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*

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

- *(example)* $(\mathbb{Z}/9\mathbb{Z})^{\times} = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}$ $((3,9) \neq 1$ *and* $(6,9) \neq 1)$, *with inverses* $\left\{\overline{1}, \overline{5}, \overline{7}, \overline{2}, \overline{4}, \overline{8}\right\}$
- *(method) for computing inverse of* $\overline{a} \subset (\mathbb{Z}/n\mathbb{Z})^{\times}$. *The condition for inverse is* $\overline{aa^{-1}} = \overline{1}$ *or* $aa^{-1} \equiv 1 \,(mod\;\; n)$. *Since* $\overline{a}$ *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.* $ax \equiv 1 \,(mod\;\; n)$ *the desired condition for inverses. Therefore,* $\overline{x}$ *is the multiplicative inverse of* $\overline{a}$. *So to find inverse for* $\overline{a}$, *we simply use Euclidean algorithm to compute the coefficient x*
- *(example) For* $(\mathbb{Z}/60\mathbb{Z})^{\times}$ *and* $a = 17$. *Apply Euclidean algorithm,*

$$\begin{aligned} 60 &= (3)17 + 9 \\ 17 &= (1)9 + 8 \\ 9 &= (1)8 + 1 \end{aligned}$$

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