Abstract Algebra I

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

Subsection 1

Basics

Set Theory

- A **set** is a collection of objects.
- The symbols $\cap, \cup, \in$ denote, as usual, the **intersection** and **union** operations and the **membership** relation.
- Based on the Axiom of Comprehension, one can use the notation

$$B = \{a \in A : \ldots (\text{conditions on } a) \ldots\}$$

  for subsets of a given set A satisfying the listed conditions.
- The **order** or **cardinality** of a set A is denoted by $|A|$. If A is a finite set, the order of A is simply the number of elements of A.
- $B \subseteq A$ means that B is a **subset** of A and $B \subset A$ (or, for emphasis, $B \subsetneq A$) means that B is a **proper subset** of A.
  To show that $B \subseteq A$, it must be shown that every element of B is also an element of A.
- The **Cartesian product** of two sets A and B is the collection $A \times B = \{(a, b) : a \in A, b \in B\}$, of ordered pairs of elements from A and B.

Notation for Common Sets of Numbers

(1) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ denotes the **integers**.

(2) $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ denotes the **rational numbers** (or **rationals**).

(3) $\mathbb{R} = \{\text{all decimal expansions } \pm d_1 d_2 \ldots d_n . a_1 a_2 a_3 \ldots\}$ denotes the **real numbers** (or **reals**).

(4) $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$ denotes the **complex numbers**.

(5) $\mathbb{Z}^+, \mathbb{Q}^+$ and $\mathbb{R}^+$ will denote the positive (nonzero) elements in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.

Functions, Domains and Codomains

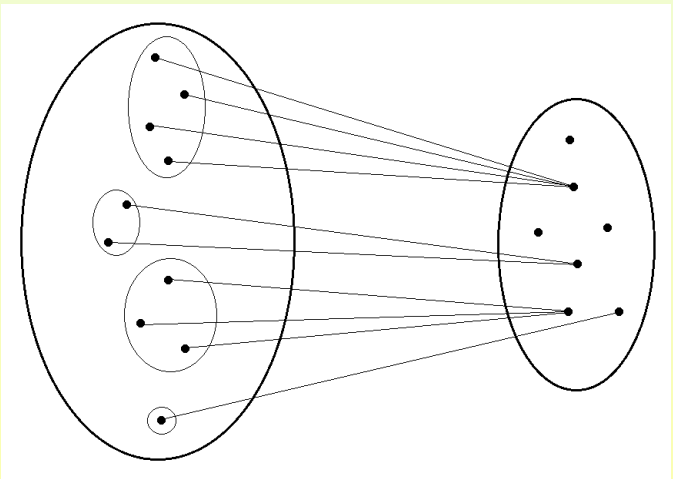
- We use the notation $f : A \to B$ or $A \xrightarrow{f} B$ to denote a **function**, or a **map**, f from A to B.
- The value of f at a is denoted $f(a)$.
- The set A is called the **domain** of f and B is called the **codomain** of f.
- The notation $f : a \mapsto b$, $a \xmapsto{f} b$, or $a \mapsto b$, if f is understood, indicates that $f(a) = b$, i.e., the function is being specified on elements.
- If the function f is not specified on elements, it is important in general to check that f is **well defined**, i.e., is unambiguously determined.

  Example: If the set A is the union of two subsets A_1 and A_2, then one can try to specify a function from A to the set $\{0, 1\}$ by declaring that f is to map everything in A_1 to 0 and is to map everything in A_2 to 1. This unambiguously defines f unless A_1 and A_2 have elements in common. Checking that this f is well defined, therefore, amounts to checking that A_1 and A_2 have empty intersection.

Image, Pre-Image and Fibers

- Let $f : A \to B$ be a function.
  - The set $f(A) = \{b \in B : b = f(a), \text{ for some } a \in A\}$ is a subset of B, called the **range** or **image** of f (or the **image of** A **under** f).
  - For each subset C of B the set $f^{-1}(C) = \{a \in A : f(a) \in C\}$, consisting of the elements of A mapping into C under f, is called the **preimage** or **inverse image** of C under f.

- For each $b \in B$, the preimage of $\{b\}$ under f is called the **fiber of** f **over** b.
  f^{-1} is not in general a function. The fibers of f generally contain many elements, since there may be many elements of A mapping to the element b.



Composition, Injectivity and Surjectivity

- If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by
$$(g \circ f)(a) = g(f(a)).$$
- Let $f : A \to B$.
  (1) f is **injective** or is an **injection** if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.
  (2) f is **surjective** or is a **surjection** if, for all $b \in B$, there is some $a \in A$, such that $f(a) = b$, i.e., the image of f is all of B.
  Since a function always maps onto its range (by definition) it is necessary to specify the codomain B in order for the question of surjectivity to be meaningful.
  (3) f is **bijective** or is a **bijection** if it is both injective and surjective.
  If such a bijection f exists from A to B, we say A and B are in **bijective correspondence**.
  (4) f has a **left inverse** if there is a function $g : B \to A$, such that $g \circ f : A \to A$ is the identity map on A, i.e., $(g \circ f)(a) = a$, for all $a \in A$.
  (5) f has a **right inverse** if there is a function $h : B \to A$, such that $f \circ h : B \to B$ is the identity map on B.

Injectivity/Surjectivity and Left/Right Inverses

Proposition

Let $f : A \to B$.

(1) The map f is injective if and only if f has a left inverse.

(2) The map f is surjective if and only if f has a right inverse.

(3) The map f is a bijection if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.

(1) ($\Rightarrow$): Suppose f is injective. Then, for every b in the range of f, there exists a unique $a_b \in A$, such that $f(a_b) = b$. Define $g : B \to A$ by $g(b) = a_b$, if b in the range of A, and $g(b)$ arbitrary, otherwise. Then, for all $a \in A$, $g(f(a)) = a$, i.e., g is a left inverse of f.

($\Leftarrow$): Suppose that f has a left inverse $g : B \to A$. Then, if $a_1 \neq a_2$ are in A, we have $g(f(a_1)) \neq g(f(a_2))$, whence, $f(a_1) \neq f(a_2)$. So f is injective.

Injectivity/Surjectivity and Left/Right Inverses (Cont'd)

(2) ($\Rightarrow$): Suppose f is surjective. Then, for every $b \in B$, there exists $a \in A$, such that $f(a) = b$. For each $b \in B$, pick such an $a_b \in A$ and define $h : B \to A$ by $h(b) = a_b$, for all $b \in B$. Then, for all $a \in A$, $(f \circ h)(b) = f(h(b)) = f(a_b) = b$, i.e., h is a right inverse of f.

($\Leftarrow$): Suppose that f has a right inverse $h : B \to A$. Then, if $b \in B$, we have $h(b) \in A$, and $f(h(b)) = (f \circ h)(b) = b$. So f is surjective.

(3) f is a bijection iff it is an injection and a surjection iff f has a left inverse g and a right inverse h. In the latter case, for all $b \in B$, $g(b) = g((f \circ h)(b)) = (g \circ f)(h(b)) = h(b)$, i.e., $g = h$.

Equipotency and Bijectivity

Proposition

Let $f : A \to B$. If A and B are finite sets with the same number of elements (i.e., $|A| = |B|$), then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.

- It suffices to show that, if A and B are finite sets, such that $|A| = |B|$, then $f : A \to B$ is injective if and only if it is surjective.
  - If f is injective, then $|A| = |f(A)|$. If f is not surjective, then $|f(A)| < |B|$. Therefore, $|A| = |f(A)| < |B|$, which contradicts the fact that $|A| = |B|$. Thus, f must be surjective.
  - If f is surjective, then $|f(A)| = |B|$. If f is not injective, then $|A| > |f(A)|$. Thus, $|A| > |f(A)| = |B|$, which contradicts $|A| = |B|$. Therefore, f must be injective.

Permutations, Restrictions and Extensions

- If $f : A \to B$ is a bijection, the map g, which is both a left and right inverse of f, is necessarily unique and is called the **2-sided inverse** (or simply the **inverse**) of f.

  A **permutation** of a set A is simply a bijection from A to itself.
- If $A \subseteq B$ and $f : B \to C$, we denote the **restriction of f to A** by $f|_A$

  When the domain we are considering is understood we may denote $f|_A$ again simply as f even though these are formally different functions (their domains are different).
- If $A \subseteq B$ and $g : A \to C$ and there is a function $f : B \to C$ such that $f|_A = g$, we shall say f is an **extension of g** to B (such a map f need not exist nor be unique).

Equivalence Relations and Partitions

- Let A be a nonempty set.
  (1) A **binary relation on** A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.
  (2) The relation $\sim$ on A is said to be:
    (a) **reflexive** if $a \sim a$, for all $a \in A$;
    (b) **symmetric** if $a \sim b$ implies $b \sim a$, for all $a, b \in A$;
    (c) **transitive** if $a \sim b$ and $b \sim c$ imply $a \sim c$, for all $a, b, c \in A$.

  A relation is an **equivalence relation** if it is reflexive, symmetric and transitive.
  (3) If $\sim$ defines an equivalence relation on A, then the **equivalence class** of $a \in A$ is defined to be $\{x \in A : x \sim a\}$. Elements of the equivalence class of a are said to be **equivalent** to a. If C is an equivalence class, any element of C is called a **representative** of the class C.
  (4) A **partition** of A is any collection $\{A_i : i \in I\}$ of nonempty subsets of A (I some indexing set) such that:
    (a) $A = \bigcup_{i \in I} A_i$;
    (b) $A_i \cap A_j = \emptyset$, for all $i, j \in I$, with $i \neq j$,

  i.e., A is the disjoint union of the sets in the partition.

Equivalence of Equivalence Relations and Partitions

Proposition

Let A be a nonempty set.

(1) If $\sim$ defines an equivalence relation on A then the set of equivalence classes of $\sim$ form a partition of A.

(2) If $\{A_i : i \in I\}$ is a partition of A, then there is an equivalence relation $\sim$ on A, defined, for all $a, b \in A$, by

$$a \sim b \quad \text{iff} \quad a, b \in A_i, \text{ for some } i \in I,$$

whose equivalence classes are precisely the sets $A_i, i \in I$.

(1) For each $a \in A$, $a \sim a$ by reflexivity. So $a \in [a] := \{x \in A : x \sim a\}$. Thus, $[a] \neq \emptyset$.
We show that, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$. Suppose, by contraposition, that $x \in [a] \cap [b]$. Then $x \sim a$ and $x \sim b$. By commutativity, $a \sim x$ and $x \sim b$. By transitivity, $a \sim b$.

Equivalence Relations and Partitions (Cont'd)

Now consider $y \in [a]$. Then $y \sim a$. By transitivity, $y \sim b$, i.e., $y \in [b]$. This proves $[a] \subseteq [b]$. By symmetry, $[b] \subseteq [a]$. Thus, $[a] = [b]$.
If $a \in A$, then $a \in [a]$. Hence, $A = \bigcup_{a \in A} [a]$.

(2) We show that $\sim$ as defined in Part (2) is an equivalence relation:
   (a) a is in the same part of the partition with itself. So $a \sim a$.
   (b) Suppose $a \sim b$. Then $a, b \in A_i$, for some i. Thus, $b, a \in A_i$. This shows that $b \sim a$.
   (c) Suppose that $a \sim b$ and $b \sim c$. Then, for some i, $a, b \in A_i$ and for some j, $b, c \in A_j$. But then $b \in A_i \cap A_j$ and we know that $A_i \cap A_j = \emptyset$ unless $i = j$. Thus, $i = j$ and $a, c \in A_i$. This yields $a \sim c$.

Proving an Equation by Induction

Proposition

Let n be a positive integer. Then $2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1$.

- We prove this by induction on n.
  - For $n = 1$, $2^0 = 2^1 - 1$ holds.
  - Suppose the result is true for $n = k$, i.e., assume $2^0 + 2^1 + \cdots + 2^{k-1} = 2^k - 1$.

    We must show that the equation is true for $n = k + 1$, i.e., that $2^0 + 2^1 + \cdots + 2^{k-1} + 2^k = 2^{k+1} - 1$.

$$\begin{aligned} 2^0 + 2^1 + \cdots + 2^{k-1} + 2^k &= 2^k - 1 + 2^k \\ &= 2 \cdot 2^k - 1 \\ &= 2^{k+1} - 1. \end{aligned}$$

Thus, the proposition is true for all positive integers.

Proving an Inequality by Induction

Proposition

Let n be a natural number. Then $10^0 + 10^1 + \cdots + 10^n < 10^{n+1}$.

- We prove this by induction on n.
  - For $n = 0$, $10^0 < 10^1$ holds.
  - Suppose the result is true for $n = k$, i.e., assume $10^0 + 10^1 + \cdots + 10^k < 10^{k+1}$.
    We must show that the equation is true for $n = k + 1$, i.e., that $10^0 + 10^1 + \cdots + 10^k + 10^{k+1} < 10^{k+2}$.

$$\begin{aligned} 10^0 + 10^1 + \cdots + 10^k + 10^{k+1} &< 10^{k+1} + 10^{k+1} \\ &= 2 \cdot 10^{k+1} \\ &< 10 \cdot 10^{k+1} \\ &= 10^{k+2}. \end{aligned}$$

Thus, the proposition is true for all positive integers.

Proving a Divisibility Relation by Induction

Proposition

Let n be a natural number. Then $4^n - 1$ is divisible by 3.

- We prove this by induction on n.
  - For $n = 0$, $4^0 - 1$ is divisible by 3.
  - Suppose the result is true for $n = k$, i.e., $3 \mid (4^k - 1)$. This means that $4^k - 1 = 3a$ for some integer a.
    We must show that the statement is true for $n = k + 1$, i.e., that $3 \mid (4^{k+1} - 1)$.

$$\begin{aligned} 4^{k+1} - 1 &= 4 \cdot 4^k - 1 \\ &= 4(4^k - 1) + 3 \\ &= 4 \cdot 3a + 3 \\ &= 3(4a + 1). \end{aligned}$$

Thus, the proposition is true for all natural numbers.

Subsection 2

Properties of the Integers

Well-Ordering and Divisibility

- We use the following properties of the integers $\mathbb{Z}$:
  (1) **Well Ordering of** $\mathbb{Z}^+$: If A is any non empty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$, called a **minimal element** of A.
  (2) If $a, b \in \mathbb{Z}$, with $a \neq 0$, we say a **divides** b if there is an element $c \in \mathbb{Z}$, such that $b = ac$. In this case we write $a \mid b$. If a does not divide b we write $a \nmid b$.
  (3) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer d, called the **greatest common divisor** of a and b or **g.c.d.** of a and b, satisfying:
    (a) $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b;
    (b) if $e \mid a$ and $e \mid b$, then $e \mid d$, i.e., d is the greatest such divisor.

  The g.c.d. of a and b will be denoted by (a, b).
  If $(a, b) = 1$, we say that a and b are **relatively prime**.
  (4) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer ℓ, called the **least common multiple** of a and b or **l.c.m.** of a and b, satisfying:
    (a) $a \mid \ell$ and $b \mid \ell$, i.e., ℓ is a common multiple of a and b;
    (b) if $a \mid m$ and $b \mid m$, then $\ell \mid m$, i.e., ℓ is the least such multiple.

  The connection between d and ℓ is given by $d\ell = ab$.

The Division and the Euclidean Algorithms

- We continue with properties of the integers:
  (5) **The Division Algorithm**: If $a, b \in \mathbb{Z} - \{0\}$, then there exist unique $q, r \in \mathbb{Z}$, such that
  $$a = qb + r \quad \text{and} \quad 0 \leq r < |b|,$$
  where q is the **quotient** and r the **remainder**. This is the usual "long division" familiar from elementary arithmetic.
  (6) **The Euclidean Algorithm** is an important procedure which produces a greatest common divisor of two integers a and b by iterating the Division Algorithm: If $a, b \in \mathbb{Z} - \{0\}$, then we obtain a sequence of quotients and remainders:
  $$\begin{aligned} a &= q_0 b + r_0 & &\vdots \\ b &= q_1 r_0 + r_1 & r_{n-2} &= q_n r_{n-1} + r_n \\ r_0 &= q_2 r_1 + r_2 & r_{n-1} &= q_{n+1} r_n, \end{aligned}$$
  where r_n is the last nonzero remainder. Such an r_n exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a decreasing sequence of strictly positive integers if the remainders are nonzero and such a sequence cannot continue indefinitely. Then r_n is the g.c.d. (a, b) of a and b.

Applying the Euclidean Algorithm

- Suppose $a = 57970$ and $b = 10353$. Applying the Euclidean Algorithm we obtain:

$$\begin{aligned} 57970 &= (5)10353 + 6205 \\ 10353 &= (1)6205 + 4148 \\ 6205 &= (1)4148 + 2057 \\ 4148 &= (2)2057 + 34 \\ 2057 &= (60)34 + 17 \\ 34 &= (2)17 + 0. \end{aligned}$$

which shows that

$$(57970, 10353) = 17.$$

The GCD as a $\mathbb{Z}$-Linear Combination

- We continue with properties of the integers:
  (7) One consequence of the Euclidean Algorithm is the following: If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$, such that $(a, b) = ax + by$, i.e., the g.c.d. of a and b is a $\mathbb{Z}$-linear combination of a and b. This follows by recursively writing the element r_n in the Euclidean Algorithm in terms of the previous remainders: Use the last equation to solve for $r_n = r_{n-2} - q_n r_{n-1}$ in terms of the remainders r_{n-1} and r_{n-2}. Then use the preceding equation to write r_n in terms of the remainders r_{n-2} and r_{n-3}, etc., eventually writing r_n in terms of a and b.

  Example: Suppose $a = 28$ and $b = 6$. The Euclidean algorithm gives:

$$28 = (4)6 + 4, \quad 6 = (1)4 + 2, \quad 4 = (2)2 + 0.$$

Thus, we find:

$$\begin{aligned} 2 &= 6 - (1)4 \\ &= 6 - (1)(28 - (4)6) \\ &= 6 - 28 + (4)6 \\ &= -28 + 5 \cdot 6. \end{aligned}$$

Primes and the Fundamental Theorem of Arithmetic

- We continue with properties of the integers:

(8) An element p of $\mathbb{Z}^+$ is called a **prime** if $p > 1$ and the only positive divisors of p are 1 and p.
An integer $n > 1$ which is not prime is called **composite**.
An important property of primes is that, if p is a prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

(9) **The Fundamental Theorem of Arithmetic**: If $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$, such that

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

This factorization is unique in the sense that, if $q_1, q_2, \ldots, q_t$ are any distinct primes and $\beta_1, \beta_2, \ldots, \beta_t$ positive integers such that $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$, then $s = t$ and, if we arrange the two sets of primes in increasing order, then $q_i = p_i$ and $\alpha_i = \beta_i$, for all $1 \leq i \leq s$.

Using the Fundamental Theorem to Find GCDs and LCMs

- Suppose the positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \quad \text{and} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s},$$

where $p_1, p_2, \ldots, p_s$ are distinct and the exponents are ≥ 0 (the exponents here are allowed to be 0 so that the products are taken over the same set of primes - the exponent will be 0 if that prime is not actually a divisor). Then the greatest common divisor of a and b is

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

The least common multiple is obtained by taking the maximum of the α_i and β_i instead of the minimum.

Example: If $a = 57970 = 2 \cdot 5 \cdot 11 \cdot 17 \cdot 31$ and $b = 10353 = 3 \cdot 7 \cdot 17 \cdot 29$, we get greatest common divisor 17.

The Euler φ-Function

- One more property of the integers:

  (10) The **Euler φ-function** is defined as follows: For $n \in \mathbb{Z}^+$, let $\varphi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n, i.e., $(a, n) = 1$.

  Example: $\varphi(12) = 4$, since 1, 5, 7 and 11 are the only positive integers less than or equal to 12 which have no factors in common with 12. Similarly, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

  - For primes p, $\varphi(p) = p - 1$.
  - For all $a \geq 1$, we have the formula $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.
  - The function φ is **multiplicative**, in the sense that $\varphi(ab) = \varphi(a)\varphi(b)$ if $(a, b) = 1$ (it is important that a and b be relatively prime).
  - Multiplicativity, together with the formula above, gives a general formula for the values of φ:
    If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) = p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)$.

  Example: $\varphi(12) = \varphi(2^2)\varphi(3) = 2^1(2-1)3^0(3-1) = 4$.

Subsection 3

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

Congruence Modulo n

- Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by $a \sim b$ if and only if $n \mid (b-a)$.
  - Clearly $a \sim a$. So $\sim$ is reflexive.
  - $a \sim b$ implies $b \sim a$ for any integers a and b, so $\sim$ is symmetric.
  - If $a \sim b$ and $b \sim c$, then n divides $a-b$ and n divides $b-c$, so n also divides their sum, i.e., n divides $(a-b)+(b-c)=a-c$, so $a \sim c$ and the relation is transitive.

  Hence, $\sim$ is an equivalence relation.
- Write $a \equiv b \pmod{n}$ and say a is **congruent to** b **mod** n if $a \sim b$.
- For $k \in \mathbb{Z}$, we shall denote the equivalence class of a by $\overline{a}$. It is called the **congruence class** or **residue class** of a mod n and consists of the integers which differ from a by an integral multiple of n, i.e., $a = \{a+kn : k \in \mathbb{Z}\} = \{a, a \pm n, a \pm 2n, a \pm 3n, \ldots\}$.
- There are n distinct equivalence classes mod n, namely $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ determined by the possible remainders after division by n.
- The set of equivalence classes under this equivalence relation will be denoted by $\mathbb{Z}/n\mathbb{Z}$ and called the **integers modulo** n.

Addition and Multiplication Modulo n

- For different n's the equivalence relation and equivalence classes are different. So before using the bar notation, care is needed to fix n.
- The process of finding the equivalence class mod n of some integer a is often referred to as **reducing** a mod n.
- In $\mathbb{Z}/n\mathbb{Z}$, one can define an **addition** and a **multiplication**: For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, define their **sum** and **product** by

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

  That is, to compute the sum or the product of $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$:
  - take representatives a in $\overline{a}$ and b in $\overline{b}$;
  - add or multiply the integers a and b as usual in $\mathbb{Z}$;
  - take the equivalence class containing the result.
- For this process to be valid we must show that the operations are well defined, i.e., do not depend on the choice of representatives taken for the elements $\overline{a}$ and $\overline{b}$ of $\mathbb{Z}/n\mathbb{Z}$.

Example of Modular Arithmetic

- Let us fix $n = 12$ and consider $\mathbb{Z}/12\mathbb{Z}$, which consists of the twelve residue classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{11}$, determined by the twelve possible remainders of an integer after division by 12.
- The elements in the residue class $\overline{5}$ are the integers which leave a remainder of 5 when divided by 12. Any such integer, such as $5, 17, 29, \ldots$ or $-7, -19, \ldots$, can serve as a representative for $\overline{5}$.
- $\mathbb{Z}/12\mathbb{Z}$ consists of the twelve elements above (each of which consists of an infinite number of usual integers).
- Suppose now that $\overline{a} = \overline{5}$ and $\overline{b} = \overline{8}$. The most obvious representatives for $\overline{a}$ and $\overline{b}$ are the integers 5 and 8, respectively. But 17 and -28 are also representatives of $\overline{a}$ and $\overline{b}$, respectively.
  - $\overline{5} + \overline{8} = \overline{13} = \overline{1}$, since 13 and 1 lie in the same class modulo $n = 12$.
  - $\overline{5} + \overline{8} = \overline{17 - 28} = \overline{-11} = \overline{1}$.

  The result does not depend on the choice of representatives.

Modular Addition and Multiplication are Well-Defined

Theorem

The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ are well defined, i.e., they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$, 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 $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., if $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ and $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

- Suppose $a_1 = b_1 \pmod{n}$, i.e., $a_1 - b_1$ is divisible by n. Then $a_1 = b_1 + sn$, for some integer s. Similarly, $a_2 \equiv b_2 \pmod{n}$ means $a_2 = b_2 + tn$, for some integer t. Then $a_1 + a_2 = (b_1 + b_2) + (s + t)n$, so that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, which shows that the sum of the residue classes is independent of the representatives chosen.
  Similarly, $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + stn)n$, showing that $a_1 a_2 \equiv b_1 b_2 \pmod{n}$. Thus, the product of the residue classes is also independent of the representatives chosen.

Suppressing the Class Notation

- The notion of adding equivalence classes is familiar in the context of adding rational numbers: Each rational number $\frac{a}{b}$ is really a class of expressions: $\frac{a}{b} = \frac{2a}{2b} = \frac{-3a}{-3b}$ etc. and we often change representatives (for instance, take common denominators) in order to add two fractions. E.g., $\frac{1}{2} + \frac{1}{3}$ is computed by taking instead the equivalent representatives $\frac{3}{6}$ for $\frac{1}{2}$ and $\frac{2}{6}$ for $\frac{1}{3}$ to obtain $\frac{1}{2} + \frac{1}{3} = \frac{3}{6} + \frac{2}{6} = \frac{5}{6}$.
- The notion of modular arithmetic is also familiar: to find the hour of day after adding or subtracting some number of hours we reduce mod 12 and find the least residue.
- It is convenient to think of the equivalence classes of some equivalence relation as elements which can be manipulated rather than as sets.
- Thus, we frequently denote the elements of $\mathbb{Z}/n\mathbb{Z}$ simply by $\{0, 1, \ldots, n-1\}$ where addition and multiplication are reduced mod n. Nevertheless, the elements of $\mathbb{Z}/n\mathbb{Z}$ are not integers, but rather collections of usual integers, and the arithmetic is quite different. For example, $5 + 8 \neq 1$ in $\mathbb{Z}$ as it is in $\mathbb{Z}/12\mathbb{Z}$.

Application of Modular Arithmetic

- We apply arithmetic in $\mathbb{Z}/n\mathbb{Z}$ to compute the last two digits in the number 2^{1000}.

  First observe that the last two digits give the remainder of 2^{1000} after we divide by 100, so we are interested in the residue class mod 100 containing 2^{1000}. We compute:

$$\begin{aligned} 2^{10} &= 1024 \equiv 24 \pmod{100}, \\ 2^{20} &= (2^{10})^2 = 24^2 = 576 \equiv 76 \pmod{100}, \\ 2^{40} &= (2^{20})^2 = 76^2 = 5776 \equiv 76 \pmod{100}, \\ 2^{80} &\equiv 2^{160} \equiv 2^{320} \equiv 2^{640} \equiv 76 \pmod{100}. \end{aligned}$$

  Finally, $2^{1000} = 2^{640}2^{320}2^{40} \equiv 76 \cdot 76 \cdot 76 \equiv 76 \pmod{100}$.

  So the final two digits of 2^{1000} are 76.

Multiplicative Inverses in $\mathbb{Z}/n\mathbb{Z}$

- An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \text{there exists } \overline{c} \in \mathbb{Z}/n\mathbb{Z}, \text{ with } \overline{a} \cdot \overline{c} = \overline{1}\}.$$

- $(\mathbb{Z}/n\mathbb{Z})^\times$ is also the collection of residue classes whose representatives are relatively prime to n, which proves the following proposition:

Proposition

$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}.$

- Note, if any representative of $\overline{a}$ is relatively prime to n, then all representatives are relatively prime to n, so that the set on the right in the proposition is well defined.

  Example: For $n = 9$ we obtain $(\mathbb{Z}/9\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$ from the proposition. The multiplicative inverses of these are $\{\overline{1}, \overline{5}, \overline{7}, \overline{2}, \overline{4}, \overline{8}\}$, respectively.

Computing Multiplicative Inverses in $\mathbb{Z}/n\mathbb{Z}$

- If a is an integer relatively prime to n, then the Euclidean Algorithm produces integers x and y, satisfying $ax + ny = 1$. Hence $ax \equiv 1 \pmod{n}$, so that $\overline{x}$ is the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$. This gives an efficient method for computing multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

  Example: Suppose $n = 60$ and $a = 17$. Applying the Euclidean Algorithm we obtain

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

  So a and n are relatively prime. Moreover,
$1 = 9-8 = 9-(17-9) = 2\cdot 9-17 = 2(60-3\cdot 17)-17 = 2\cdot 60-7\cdot 17.$
Hence $\overline{-7} = \overline{53}$ is the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$.