

COMP0147 Discrete Mathematics for Computer Scientists Notes

Joe

April 17, 2019

Notes adapted from:

- Lecture notes by Max Kanovich and Robin Hirsch [1].
- *A First Course in Abstract Algebra* by Joseph J. Rotman [2].

Contents

1	Set Theory	7
1.1	Set Notations	7
1.2	Properties	7
1.3	Set Equality	7
1.4	Set Operations	7
1.5	Boolean Algebra	8
1.6	Set Algebra	9
2	Functions	11
2.1	Function Basics	11
2.2	Composition of Injections	12
2.3	Composition of Surjection	12
2.4	Composition of Bijection	12
2.5	Cardinality of Sets	13
3	Permutations	15
3.1	Permutation Basics	15
4	Binary Relations	17
4.1	Equivalence Relations	17
4.2	Equivalence Classes	17
4.3	Quotient Groups	18
5	Groups	21
5.1	Group Basics	21
5.2	Multiplicative Group	21
5.3	Additive Group	22
5.4	Associativity of Sequential Composition of Functions	23
5.5	Subgroups	23
5.6	Lagrange's Theorem	24
5.6.1	Equivalence Classes	26
5.6.2	Order of an Element in Lagrange's Theorem	28
6	Euclidean Algorithm	29
6.1	Euclidean Algorithm Basics	29
6.2	$\gcd(a, b)$ as a Linear Combination of a and b	29
6.3	Problems for Integers Modulo m	30

6.4	Multiplicative Group of Integers Modulo m	31
6.5	Rivest–Shamir–Adleman (RSA) Cryptography	33
7	Linear Algebra	35
7.1	Matrix Basics	35
7.1.1	Matrix Addition and Multiplication Properties	36
7.1.2	Determinant of a Square Matrix	37
7.2	Solving Linear System of Equations	38
7.3	Gaussian Elimination	39

1 Set Theory

1.1 Set Notations

- Set definition: $A = \{a, b, c\}$
- Set membership (element-of): $a \in A$
- Set builder notation: $\{x \mid x \in \mathbb{R} \wedge x^2 = x\}$
- Empty set: \emptyset

1.2 Properties

- No structure
- No order
- No copies

For example, a, b, c are references to actual objects in

$$\{a, b, c\} \Leftrightarrow \{c, a, b\} \Leftrightarrow \{a, b, c, b\}$$

1.3 Set Equality

Definition 1.3.1 (Set Equality). Set $A = B$ iff:

1. $A \subseteq B \implies \forall x(x \in A \rightarrow x \in B)$
2. $B \subseteq A \implies \forall y(y \in B \rightarrow y \in A)$

Remark. $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

1.4 Set Operations

- *Union:* $A \cup B := \{x \mid x \in A \vee x \in B\}$
- *Intersection:* $A \cap B := \{x \mid x \in A \wedge x \in B\}$
- *Relative Complement:* $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$
- *Absolute Complement:* $A^c := U \setminus A := \{x \mid x \in U \wedge x \notin A\}$
- *Symmetric Difference:* $A \Delta B := (A \setminus B) \cup (B \setminus A) := (A \cup B) \setminus (A \cap B)$
- *Cartesian Product:* $A \times B := \{(x, y) \mid x \in A \wedge y \in B\}$

1.5 Boolean Algebra

Definition 1.5.1 (De Morgan's Laws).

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad (1.1)$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad (1.2)$$

Definition 1.5.2 (Idempotent Laws).

$$p \vee p \equiv p \quad (1.3)$$

$$p \wedge p \equiv p \quad (1.4)$$

Definition 1.5.3 (Commutative Laws).

$$p \vee q \equiv q \vee p \quad (1.5)$$

$$p \wedge q \equiv q \wedge p \quad (1.6)$$

Definition 1.5.4 (Associative Laws).

$$p \vee (q \vee r) \equiv (p \vee q) \vee r \quad (1.7)$$

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r \quad (1.8)$$

Definition 1.5.5 (Distributive Laws).

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad (1.9)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \quad (1.10)$$

Definition 1.5.6 (Identity Laws).

$$p \vee F \equiv p \quad (1.11)$$

$$p \vee T \equiv T \quad (1.12)$$

$$p \wedge T \equiv p \quad (1.13)$$

$$p \wedge F \equiv F \quad (1.14)$$

Definition 1.5.7 (Absorption Laws).

$$p \vee (p \wedge q) \equiv p \quad (1.15)$$

$$p \wedge (p \vee q) \equiv p \quad (1.16)$$

Definition 1.5.8 (Implication and Negation Laws).

- *Identity:* $p \rightarrow q \equiv \neg p \vee q$
- *Counter-example:* $\neg(p \rightarrow q) \equiv p \wedge \neg q$
- *Equivalences:* $p \rightarrow q \rightarrow r \equiv (p \wedge q) \rightarrow r \equiv q \rightarrow (p \rightarrow r)$

- *Absorption:*
 $p \rightarrow T \equiv T$
 $p \rightarrow F \equiv \neg p$
 $T \rightarrow p \equiv p$
 $F \rightarrow p \equiv T$
- *Contrapositive:* $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- *Law of Excluded Middle:*
 $p \vee \neg p \equiv T$
 $p \wedge \neg p \equiv F$
- *Double Negation:* $\neg\neg p \equiv p$
- *Reduction to Absurdity:* $\neg p \rightarrow F \equiv p$

1.6 Set Algebra

Definition 1.6.1 (De Morgan's Laws).

$$(A \cup B)^c \equiv A^c \cap B^c \quad (1.17)$$

$$(A \cap B)^c \equiv A^c \cup B^c \quad (1.18)$$

Definition 1.6.2 (Idempotent Laws).

$$A \cup A \equiv A \quad (1.19)$$

$$A \cap A \equiv A \quad (1.20)$$

Definition 1.6.3 (Commutative Laws).

$$A \cup B \equiv B \cup A \quad (1.21)$$

$$A \cap B \equiv B \cap A \quad (1.22)$$

Definition 1.6.4 (Associativity Laws).

$$A \cup (B \cup C) \equiv (A \cup B) \cup C \quad (1.23)$$

$$A \cap (B \cap C) \equiv (A \cap B) \cap C \quad (1.24)$$

Definition 1.6.5 (Distributive Laws).

$$A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C) \quad (1.25)$$

$$A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C) \quad (1.26)$$

Definition 1.6.6 (Identity Laws).

$$A \cup \emptyset \equiv A \quad (1.27)$$

$$A \cap \emptyset \equiv \emptyset \quad (1.28)$$

$$A \cap U \equiv A \quad (1.29)$$

$$A \cup U \equiv U \quad (1.30)$$

Definition 1.6.7 (Absorption Laws).

$$A \cup (A \cap B) \equiv A \quad (1.31)$$

$$A \cap (A \cup B) \equiv A \quad (1.32)$$

Definition 1.6.8 (Difference Identity Laws).

$$C \setminus (A \cup B) \equiv (C \setminus A) \cap (C \setminus B) \quad (1.33)$$

$$C \setminus (A \cap B) \equiv (C \setminus A) \cup (C \setminus B) \quad (1.34)$$

Definition 1.6.9 (Complement-Difference Identity Law).

$$C \setminus D \equiv C \cap D^c \quad (1.35)$$

Definition 1.6.10 (Double Complement Law).

$$(D^c)^c \equiv D \quad (1.36)$$

Definition 1.6.11 (Contraposition).

$$C \subseteq D \Leftrightarrow D^c \subseteq C^c \quad (1.37)$$

$$C = D \Leftrightarrow C^c = D^c \quad (1.38)$$

Definition 1.6.12 (Arbitrary Union).

Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cup A_2 \cup \dots \cup A_n := \bigcup_{i \in I} A_i \quad (1.39)$$

Then

$$x \in \bigcup_{i \in I} A_i \Leftrightarrow \exists i \in I: x \in A_i \quad (1.40)$$

Definition 1.6.13 (Arbitrary Intersection).

Given sets A_1, A_2, \dots, A_n where $I = \{1, 2, \dots, n\}$

$$A_1 \cap A_2 \cap \dots \cap A_n := \bigcap_{i \in I} A_i \quad (1.41)$$

Then

$$x \in \bigcap_{i \in I} A_i \Leftrightarrow \forall i \in I: x \in A_i \quad (1.42)$$

2 Functions

2.1 Function Basics

Definition 2.1.1 (Function). A function f is a mapping from X to Y

$$f: X \mapsto Y \quad (2.1)$$

- $\text{domain}(f) = X$
- $\text{image}(f) = f(X)$

Definition 2.1.2 (Total Function). A function is *total* if

$$\text{domain}(f) = X \quad (2.2)$$

Definition 2.1.3 (Partial Function). A function is *partial* if

$$\text{domain}(f) \subseteq X \quad (2.3)$$

Definition 2.1.4 (Surjection). A function $f: X \mapsto Y$ is *surjective* iff

$$f(X) = Y \Leftrightarrow \forall y \in Y: \exists x \in X: f(x) = y \quad (2.4)$$

Namely each $y \in Y$ has a corresponding $x \in X$.

Definition 2.1.5 (Injection (Encodings, One-to-one)). A function $f: X \mapsto Y$ is *injective* iff

$$\forall x_1, x_2 \in X: x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2) \quad (2.5)$$

$$\Leftrightarrow \forall x_1, x_2 \in X: f(x_1) = f(x_2) \rightarrow x_1 = x_2 \quad (2.6)$$

Namely each distinct element $x \in X$ maps to a different element in Y .

Definition 2.1.6 (Bijection). A function $f: X \mapsto Y$ is *bijective* iff f is both *injective* and *surjective*.

$$\text{Bijective}(f) := \text{Injective}(f) \wedge \text{Surjective}(f) \quad (2.7)$$

The *inverse bijection* $f^{-1}: Y \mapsto X$ does exist.

2.2 Composition of Injections

Proposition 2.2.1 (Composition of Injection). Given *injections* $f: X \mapsto Y$ and $g: Y \mapsto Z$, then their *composition* $h: X \mapsto Z$ is given by

$$h(x) := g(f(x)) \quad (2.8)$$

Then h is also an *injective* function. Namely $h = g \circ f$ where h is composed from g and f with f applied first.

Proof. Given any $x_1, x_2 \in X$ where $x_1 \neq x_2$, then

$$f(x_1) \neq f(x_2) \quad (2.9)$$

as f is *injective*, and thus

$$h(x_1) = g(f(x_1)) \neq g(f(x_2)) = h(x_2) \quad (2.10)$$

h is *injective* consequently. ■

2.3 Composition of Surjection

Proposition 2.3.1 (Composition of Surjection). Given *surjections* $f: X \mapsto Y$ and $g: Y \mapsto Z$, then their *composition* $h: X \mapsto Z$ is given by

$$h(x) := g(f(x)) \quad (2.11)$$

Then h is also a *surjective* function.

Proof. To prove $h: X \mapsto Z$ is *surjective*, it is required to prove that

$$\forall z \in Z: \exists x \in X: h(x) = z \quad (2.12)$$

Where $h(x) \Leftrightarrow (g \circ f)(x) \Leftrightarrow g(f(x))$.

Given any element $z \in Z$ ($\forall z \in Z$):

1. That $g: Y \mapsto Z$ is *surjective* by definition, then $\exists y \in Y: g(y) = z$.
2. That $f: X \mapsto Y$ is *surjective* by definition, then $\exists x \in X: f(x) = y$.

Then $\forall z \in Z: \exists x \in X: h(x) = (g \circ f)(x) = g(f(x)) = g(y) = z$ holds true. ■

2.4 Composition of Bijection

Proposition 2.4.1 (Composition of Bijection). Given *bijections* $f: X \mapsto Y$ and $g: Y \mapsto Z$, then their composition $h: X \mapsto Z$ is given by

$$h(x) := g(f(x)) \quad (2.13)$$

Then h is also a *bijective* function; an *inverse bijection* $h^{-1}: Z \mapsto X$ also exists.

2.5 Cardinality of Sets

Definition 2.5.1 (Cardinality). The number of elements in a set X is denoted $|X|$.

Definition 2.5.2 (Equal Cardinality and Bijection).

$$|X| = |Y| \quad (2.14)$$

Holds true if there exists a *bijection* $h: X \mapsto Y$ (one-to-one correspondence between X and Y).

Namely, X and Y have the same number of distinct elements, and each distinct element $x \in X$ corresponds to exactly one distinct element $y \in Y$.

Theorem 2.5.1 (Cantor-Bernstein). Given

1. *injective* function $f: X \mapsto Y$
2. *injective* function $g: Y \mapsto X$

Then there exists a *bijection* function $h: X \mapsto Y$.

Equivalently,

$$(|X| \leq |Y|) \wedge (|Y| \leq |X|) \rightarrow (|X| = |Y|) \quad (2.15)$$

Remark. Examples include countable sets, enumerable sets

$$|\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{N}| = \aleph_0 \quad (2.16)$$

Where the cardinality of countable sets such as the *rational numbers*, *integers* and the *natural numbers* is denoted as "aleph-zero" (\aleph_0).

On the other hand, continuum such as the *real numbers* are not countable and as such

$$|\mathbb{R}| > \aleph_0 \quad (2.17)$$

3 Permutations

3.1 Permutation Basics

Definition 3.1.1 (Permutation). The bijection – *permutation* – of

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{array} \quad (3.1)$$

Is denoted as

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \quad (3.2)$$

Where $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is the *permutation* bijection.

Definition 3.1.2 (Counting Permutations).

$$|S_n| := n! \quad (3.3)$$

Which is the number of different ways to permute n elements $\{1, 2, \dots, n\} \subset \mathbb{Z}$. Together, the different permutations for n distinct elements is the *symmetric group* S_n .

Remark. For example, with $S_3 = \{1, 2, 3\}$, there are $3! = 6$ different ways to arrange the three distinct elements

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad (3.4)$$

Definition 3.1.3 (Order of Permutation). The *order* of a permutation σ is the smallest $k \in \mathbb{Z}^+$ such that

$$\sigma^k = \epsilon \quad (3.5)$$

Where ϵ is the *identity permutation*

$$\epsilon(x) = x \quad (3.6)$$

Definition 3.1.4 (Sign of Permutation). The *sign* of a permutation $\text{sgn } \sigma: \sigma \rightarrow \{-1, +1\}$ where $\sigma \in S_n$ is defined as

$$\text{sgn}(\sigma) = (-1)^k \quad (3.7)$$

Where k is the number of *disorders* within σ , the number of pairs (x, y) such that $x > y \rightarrow \sigma(x) < \sigma(y)$ or the converse $x < y \rightarrow \sigma(x) > \sigma(y)$. Additionally,

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } k \text{ is even} \\ -1 & \text{if } k \text{ is odd} \end{cases} \quad (3.8)$$

Remark. For example, in

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$1 < 2$ but $\sigma(1) = 2 > \sigma(2) = 1$, hence a disorder.

For each $i \in \{1, \dots, n\}$, starting from $i = 1$, compare $\sigma(i)$ with $\sigma(i+1), \dots, \sigma(n)$ and add the number of disordered pairs, then move on to $i+1$ and compare $\sigma(i+1)$ with $\sigma(i+2), \dots, \sigma(n)$ and so on.

Theorem 3.1.1 (Composition of Permutation).

$$\text{sgn}(\sigma_1 \sigma_2) := \text{sgn}(\sigma_1) \cdot \text{sgn}(\sigma_2) \quad (3.9)$$

Where

\circ	even	odd
even	even	odd
odd	odd	even

Table 3.1: Sign Changes on Composition

4 Binary Relations

Definition 4.0.1 (Binary Relation). A binary relation $R(x, y)$ describes some relationship between x and y where $R: X \rightarrow Y$, $R \subseteq X \times Y$, $x \in X$ and $y \in Y$. This relation can be expressed in infix notation as xRy .

4.1 Equivalence Relations

Definition 4.1.1 (Equivalence Relation). A binary relation $E(x, y)$ is an *equivalence relation* on X iff it satisfies all three conditions:

1. **Reflexivity**

$$\forall x \in X: E(x, x)$$

2. **Symmetry**

$$\forall x, y \in X: E(x, y) \rightarrow E(y, x)$$

3. **Transitivity**

$$\forall x, y, z \in X: E(x, y) \wedge E(y, z) \rightarrow E(x, z)$$

4.2 Equivalence Classes

Definition 4.2.1 (Equivalence Class). If $a \in X$, the *equivalence class* $[a]$ is

$$[a] := \{x \in X: E(x, a)\} \subseteq X \quad (4.1)$$

Definition 4.2.2 (Congruence and Equivalence Class of mod m on \mathbb{Z}). For *congruence mod m* on \mathbb{Z} , if $a \in \mathbb{Z}$ then the *congruence class* of a is

$$[a]_m := \{x \in \mathbb{Z}: x = a + km\} \quad (4.2)$$

Where $k \in \mathbb{Z}$. Since $x = a + km \Leftrightarrow x \equiv a \pmod{m}$, then the *equivalence class* of a is also the *congruence class*.

$$\Leftrightarrow [a]_m := \{x \in \mathbb{Z}: x \equiv a \pmod{m}\} \quad (4.3)$$

Definition 4.2.3 (Set of Remainders). Over \mathbb{Z} , the *remainder* r from the integer division $k \div m$ is

$$r \bmod m \equiv k \bmod m \quad (4.4)$$

Then the set of remainders G_m from the integer division $k \div m$ is defined by

$$G_m := \{0, 1, 2, \dots, m-2, m-1\} \quad (4.5)$$

4.3 Quotient Groups

Definition 4.3.1 (Quotient Group). A *quotient group* is a group constructed via congruence mod m .

Definition 4.3.2 (Congruence Class). If $m \leq 2$ and $a \in \mathbb{Z}$ then the *congruence class* of $a \bmod m$ is $[a] \subseteq \mathbb{Z}$

$$[a] := \{b \in \mathbb{Z} : b \equiv a \bmod m\} \quad (4.6)$$

$$\Leftrightarrow \{a + km : k \in \mathbb{Z}\} \quad (4.7)$$

$$\Leftrightarrow \{\dots, a - 2m, a - m, a, a + m, a + 2m, \dots\} \quad (4.8)$$

Remark. Let $E(x, y) := "x - y \equiv 0 \bmod 2"$, that is, $x - y$ is divisible by 2. Then,

$$[k]_2 := \{y : E(k, y)\} \quad (4.9)$$

Where $[k]_2$ is the congruence class of integers modulo 2.

Computing $[0]_2$ and $[1]_2$ yields

- $[0]_2 = \{0, 2, -2, 4, -4, \dots, 2n, -2n, \dots\}$
- $[1]_2 = \{1, -1, 3, -3, \dots, 2n + 1, \dots\}$

Observe that

$$[1]_2 \oplus [1]_2 \Leftrightarrow [2]_2 \Leftrightarrow [0]_2 \quad (4.10)$$

It can be deduced that $[0]_2$ and $[1]_2$ are two congruence (and equivalence) classes which partition the integers \mathbb{Z} into two disjoint subsets – integers which are odd, and integers which are even. This may be denoted as

$$\mathbb{Z}/E \equiv \{\text{EVEN}, \text{ODD}\} \quad (4.11)$$

Definition 4.3.3 (Congruence Modular Arithmetic (mod m) on \mathbb{Z}).

$$[a]_m \oplus [b]_m \equiv [a + b]_m \quad (4.12)$$

$$[a]_m \otimes [b]_m \equiv [a \cdot b]_m \quad (4.13)$$

If $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$ then

$$a_1 + b_1 \equiv a_2 + b_2 \bmod m \quad (4.14)$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \bmod m \quad (4.15)$$

$$(4.16)$$

Remark. We may introduce addition (+) and multiplication (*) over the remainders G_m previously defined as

$$G_m := \{0, 1, 2, \dots, m - 2, m - 1\} \quad (4.17)$$

For example, given $m = 3$, then the multiplication and addition table of $+$ (mod 3) and $*$ (mod 3) over G_3 can be computed:

$+$ (mod 3) 0 1 2	$*$ (mod 3) 0 1 2
0 0 1 2	0 0 0 0
1 1 2 0	1 0 1 2
2 2 0 1	2 0 2 1

Table 4.1: Multiplication and Addition Table of G_3

5 Groups

5.1 Group Basics

A *group* is an abstract collection consisting of:

- A *nonempty set* G .
- A *binary operation* $\star: G \times G \rightarrow G$.

It has the following properties:

1. **Closure**

$$\forall x, y: x \in G \wedge y \in G \rightarrow x \star y \in G \quad (5.1)$$

2. **Associativity**

$$\forall x, y, z \in G: (x \star y) \star z \equiv x \star (y \star z) \quad (5.2)$$

3. **Neutral Element**

$$\exists \epsilon \in G: \forall x \in G: x \star \epsilon \equiv \epsilon \star x \equiv x \quad (5.3)$$

That there exists an unique *neutral* element $\epsilon \in G$.

4. **Invertibility**

$$\forall x \in G: \exists y \in G: x \star y \equiv y \star x \equiv \epsilon \quad (5.4)$$

That there exists an unique *inverse* element $y := x^{-1} \in G$ where x^{-1} denotes the *inverse* element of x .

Definition 5.1.1 (Commutative Group). An *commutative group* (or *abelian group*) is a *group* for which its operation $\star: G \times G \rightarrow G$ satisfies the additional *commutative* property:

- **Commutativity**

$$\forall x, y \in G: x \star y \equiv y \star x \quad (5.5)$$

5.2 Multiplicative Group

Proposition 5.2.1 (Multiplicative Group). A *multiplicative group* is a *group* $(G, *)$ which has the binary operation $*: G \times G \rightarrow G$:

- **Closure, Associativity.** The multiplication operation $*: G \times G \rightarrow G$ is closed and is left associative.
- **Neutral Element.** The neutral element ϵ is unique.
- **Invertibility.** The inverse element x^{-1} is unique.

- For all $a, b \in G$ the equation

$$a * x = b \quad (5.6)$$

Has the unique solution

$$x = a^{-1} * b \quad (5.7)$$

Since

$$a * x = b \Leftrightarrow a^{-1} * (a * x) = a^{-1} * b \quad (\text{Multiply by inverse element}) \quad (5.8)$$

$$\Leftrightarrow (a^{-1} * a) * x = a^{-1} * b \quad (\text{Associativity}) \quad (5.9)$$

$$\Leftrightarrow \epsilon * x = a^{-1} * b \quad (\text{Invertibility}) \quad (5.10)$$

$$\Leftrightarrow x = a^{-1} * b \quad (\text{Neutral Element}) \quad (5.11)$$

Remark. An example of a multiplicative group is permutations under composition, namely S_n is a group (G, \circ) where $\circ: G \times G \rightarrow G$.

For example, let G be the set of permutations

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (5.12)$$

To verify that G does form a group with composition \circ , one may draw the multiplication table for the group. Note that

$$\sigma_2 \sigma_2 = \sigma_1^4 = \sigma_1^3 \sigma_1 = \epsilon \sigma_1 = \sigma_1 \quad (5.13)$$

\circ	ϵ	σ_1	σ_2
ϵ	ϵ	σ_1	σ_2
σ_1	σ_1	σ_2	ϵ
σ_2	σ_2	ϵ	σ_1

Table 5.1: Multiplication Table of Composition \circ over G

5.3 Additive Group

Definition 5.3.1 (Additive Group). An *additive group* is a *group* $(G, +)$ with the binary operation $+: G \times G \rightarrow G$. It has the same properties of a general *group*.

1. **Closure**

$$\forall x, y: x \in G \wedge y \in G \rightarrow x + y \in G \quad (5.14)$$

2. **Associativity**

$$\forall x, y, z \in G: (x + y) + z \equiv x + (y + z) \quad (5.15)$$

3. **Neutral Element**

$$\exists \epsilon \in G: \forall x \in G: x + \epsilon \equiv \epsilon + x \equiv x \quad (5.16)$$

That there exists an unique *neutral* element $0_G \in G$ (usually denoted simply as 0).

4. Invertibility

$$\forall x \in G: \exists y \in G: x + y \equiv y + x \equiv 0 \quad (5.17)$$

That there exists an unique *inverse* element $y := -x \in G$ where $-x$ denotes the *inverse* element of x .

Remark. An example of an additive group is $(\mathbb{Z}, +)$ (i.e. addition over the integers). Then for any of such *commutative group* $(G, +)$

- *Neutral element* 0 is unique.
- *Inverse element* $-x$ is unique.
- For any $a, b \in G$ the equation

$$a + x = b \quad (5.18)$$

Has a unique solution

$$x = b + (-a) = b - a \quad (5.19)$$

5.4 Associativity of Sequential Composition of Functions

Definition 5.4.1 (Sequential Composition of Functions). Let $f * g$ denote the sequential composition of functions $f * X \rightarrow Y$ and $g: Y \rightarrow Z$ such that $f * g: X \rightarrow Z$ where f is applied first then g , i.e. $\forall x \in X: (f * g)(x) := g(f(x))$.

Proposition 5.4.1 (Associativity of Sequential Composition of Functions). Given sets X, Y and Z and

- *Injection* $f: A \rightarrow B$
- *Injection* $g: B \rightarrow C$
- *Injection* $h: C \rightarrow D$

Then their composition is associative:

$$(f * g) * h \equiv f * (g * h) \quad (5.20)$$

Proof.

Let $s = (f * g)$ and $t = (s * h)$, then $t(x) = h(s(x)) = h(g(f(x)))$.

Let $u = (g * h)$ and $v = (f * u)$, then $v(x) = u(f(x)) = h(g(f(x)))$.

Together they yield the desired equality $t(x) = v(x)$. ■

5.5 Subgroups

Definition 5.5.1 (Subgroup). Given a *group* $(G, *)$, then the subset $H \subseteq G$ is a *subgroup* of G if it fulfills the properties:

1. Closure

$$\forall x, y: x \in H \wedge y \in H \rightarrow x * y \in H \quad (5.21)$$

2. Neutral Element

$$\epsilon \in H \quad (5.22)$$

That is, the *neutral* element ϵ from G is contained within the subset $H \subseteq G$.

3. Invertibility

$$\forall x \in H: x^{-1} \in H \quad (5.23)$$

5.6 Lagrange's Theorem

Theorem 5.6.1 (Lagrange's Theorem). Given a finite *group* of order n $(G, *)$ where

$$G := \{g_1, g_2, \dots, g_n\} \quad (5.24)$$

And its *subgroup* $(H, *)$ of order $k \leq n$

$$H := \{h_1, h_2, \dots, h_k\} \quad (5.25)$$

Then $k|n$ (k divides n).

G can be *partitioned* into ℓ disjoint subsets of the same size k such that

$$n = k\ell \quad (5.26)$$

Definition 5.6.1 (Left Coset). Given $(G, *)$ is a *group*, $(H, *)$ is a *subgroup* of $(G, *)$ and $g \in G$ then the *left coset* gH of H in G with respect to g is defined as

$$gH := \{g * h : h \in H\} \quad (5.27)$$

Remark. Visually,

$$G \equiv \left. \begin{array}{c} \boxed{g_1 H} \\ \boxed{g_2 H} \\ \vdots \\ \boxed{g_\ell H} \end{array} \right\} \ell \text{ disjoint subsets} \quad (5.28)$$

To verify that the *left cosets* together do in fact reconstruct G , check the multiplication table

$*$	h_1	h_2	\dots	h_k
$g_1 H$	$g_1 * h_1$	$g_1 * h_2$	\dots	$g_1 * h_k$
$g_2 H$	$g_2 * h_1$	$g_2 * h_2$	\dots	$g_2 * h_k$
\vdots	\vdots	\vdots	\ddots	\vdots
$g_\ell H$	$g_\ell * h_1$	$g_\ell * h_2$	\dots	$g_\ell * h_k$

Table 5.2: Multiplication Table from ℓ Left Cosets, Each of Size $|H| = k$

Proposition 5.6.1. For any $a, b \in G$ from $(G, *)$

$$(a * b)^{-1} \equiv b^{-1} * a^{-1} \quad (5.29)$$

Proof.

$$(a * b)^{-1} \Leftrightarrow (a * b)^{-1} * \epsilon \quad (\text{Neutral element}) \quad (5.30)$$

$$\Leftrightarrow (a * b)^{-1} * (a * a^{-1}) \quad (\text{Invertibility}) \quad (5.31)$$

$$\Leftrightarrow (a * b)^{-1} * ((a * \epsilon) * a^{-1}) \quad (\text{Neutral element}) \quad (5.32)$$

$$\Leftrightarrow (a * b)^{-1} * [(a * (b * b^{-1})) * a^{-1}] \quad (\text{Invertibility}) \quad (5.33)$$

$$\Leftrightarrow (a * b)^{-1} * [(a * b) * (b^{-1} * a^{-1})] \quad (\text{Associativity}) \quad (5.34)$$

$$\Leftrightarrow [(a * b)^{-1} * (a * b)] * (b^{-1} * a^{-1}) \quad (\text{Associativity}) \quad (5.35)$$

$$\Leftrightarrow \epsilon * (b^{-1} * a^{-1}) \quad (\text{Invertibility}) \quad (5.36)$$

$$\Leftrightarrow b^{-1} * a^{-1} \quad (\text{Neutral Element}) \quad (5.37)$$

■

Proof. For a constructive proof of Lagrange's Theorem:

Let the binary relation $E(x, y)$ be defined on the *group* $(G, *)$, with its *subgroup* $(H, *)$

$$E(x, y) := x^{-1} * y \in H \quad (5.38)$$

For the equivalence

$$x = y \Leftrightarrow x^{-1} * y = 1 \quad (5.39)$$

Then for each of the required properties:

- **Neutral Element** from *Reflexivity* of $E(x, y)$

$$\forall x \in G: E(x, x) \quad (5.40)$$

Since

$$E(x, x) \equiv x^{-1} * x \in H \equiv \epsilon \in H \quad (5.41)$$

Then this satisfies the *reflexivity* requirement for *equivalence relations*, and proves the *neutral element* requirement for *subgroups*.

- **Invertibility** from *Symmetry* of $E(x, y)$

$$\forall x, y \in G: E(x, y) \rightarrow E(y, x) \quad (5.42)$$

Let for some $h \in H$, $x^{-1} * y = h$, then by proposition 5.6.1

$$y^{-1} * x \equiv (x^{-1} * y)^{-1} \equiv h^{-1} \in H \quad (5.43)$$

Which satisfies the *symmetry* requirement for *equivalence relations*, and proves the *invertibility* requirement for *subgroups*.

- **Closure** from *Transitivity* of $E(x, y)$

$$\forall x, y, z \in G: E(x, y) \wedge E(y, z) \rightarrow E(x, z) \quad (5.44)$$

Let for some $h_1, h_2 \in H$, $(x^{-1} * y = h_1) \wedge (y^{-1} * z = h_2)$, then

$$x^{-1} * z \Leftrightarrow x^{-1} * \epsilon * z \quad (5.45)$$

$$\Leftrightarrow (x^{-1} * y) * (y^{-1} * z) \quad (5.46)$$

$$\Leftrightarrow h_1 * h_2 \in H \quad (5.47)$$

Which satisfies the *transitivity* requirement for *equivalence relations*, and proves the *closure* requirement for *subgroups*. ■

Remark. To demonstrate Lagrange's Theorem, let the *group* be constructed from $x * y \pmod{10}$.

Let $(G, *)$ be a finite *group* of order $n = 4$ where

$$G = \{1, 3, 7, 9\} \quad (5.48)$$

And $(H, *)$ be its *subgroup* of order $k = 2$.

Constructing the multiplication table yields

$* \pmod{10}$	1	9
$1 * H$	1	9
$3 * H$	3	7
$7 * H$	7	3
$9 * H$	9	1

Table 5.3: Multiplication Table for $(G, *)$

There are only $\ell = 2$ disjoint subsets (unique cosets) gH ; G can be partitioned into ℓ disjoint subsets, each of size $|H| = 2$ such that $4 = n = k\ell = 2 \cdot 2$.

Visually,

$$G = \left. \begin{array}{l} 1 * H = 9 * H = \{1, 9\} \\ 3 * H = 7 * H = \{3, 7\} \end{array} \right\} \ell = 2 \quad (5.49)$$

5.6.1 Equivalence Classes

Definition 5.6.2 (Equivalence Class). Given *group* $(G, *)$ and its *subgroup* $(H, *)$, then the *equivalence class* $[g]$ is defined as

$$[g] := \{y \in G \mid g^{-1} * y \in H\} \quad (5.50)$$

Then

$$\forall h \in H: g^{-1} * y = h \Leftrightarrow y = g * h \quad (5.51)$$

Which yields the equivalence

$$\{y \in G \mid g^{-1} * y \in H\} \equiv \{y \in G \mid y \in gH\} \quad (5.52)$$

Hence

$$[g] \equiv gH \quad (5.53)$$

That the *equivalence class* $[g]$ is exactly the *left coset* gH .

Let ℓ be the number of disjoint equivalence class $[g]$, then G can be partitioned into ℓ disjoint subsets where visually,

$$G = \left. \begin{array}{c} [g_1] \equiv g_1 H \\ [g_2] \equiv g_2 H \\ \vdots \\ [g_\ell] \equiv g_\ell H \end{array} \right\} \ell \text{ disjoint subsets} \quad (5.54)$$

Proposition 5.6.2.

$$\forall g \in G: |gH| \equiv |H| \equiv k \quad (5.55)$$

Proof. Let I be the set of indices $I := \{1, \dots, k\}$

$$\forall i, j \in I: (h_i = h_j) \leftrightarrow (g * h_i = g * h_j) \quad (5.56)$$

$$\Leftrightarrow \forall i, j \in I: (h_i \neq h_j) \leftrightarrow (g * h_i \neq g * h_j) \quad (5.57)$$

■

Remark. Let A_n be the set of all *even permutations* and B_n be the set of all *odd permutations*.

Given the *group* $(S_n, *)$, then $(A_n, *)$ is a *subgroup* of S_n .

With the multiplication table

*	A_n
$\epsilon * A_n$	A_n
$\epsilon * A_n$	B_n

Table 5.4: Multiplication Table for Group S_n

Since

$$\sigma * A_n \equiv \begin{cases} A_n & \text{if } \sigma \text{ is even} \\ B_n & \text{if } \sigma \text{ is even} \end{cases} \quad (5.58)$$

Hence,

$$|A_n| \equiv \frac{1}{2} \cdot |S_n| \equiv \frac{1}{2} \cdot n! \quad (5.59)$$

5.6.2 Order of an Element in Lagrange's Theorem

Definition 5.6.3 (Order of an Element). Given a *group* $(G, *)$ and element $a \in G$ then the *order* of the element a is the smallest $k \in \mathbb{Z}^+$ such that

$$a^k = \epsilon \quad (5.60)$$

Proposition 5.6.3. Given a *group* $(G, *)$ with *order* n , then for any $a \in G$, should its *order* k exist, then $k|n$ (k divides n).

Proposition 5.6.4. Given *group* $(G, *)$,

$$\forall a \in G: a^{|G|} \equiv 1 \quad (5.61)$$

Proof. With the *cyclic subgroup* generated by $a \in G$

$$\{a^m \mid m \in \mathbb{Z}\} = \{\epsilon, a, a^2, \dots\} \quad (5.62)$$

■

Remark. This may be used to calculate the modulo of integers raised to large exponents. For example, for $2^{20} \pmod{15}$. To compute this, let the *multiplicative group* $(G, *)$ be defined over G of *order* 8 where

$$G = \{1, 2, 4, 7, 8, 11, 13, 14\} \quad (5.63)$$

And the *binary operation* $x * y := x * y \pmod{15}$.

Note that $2^{-1} = 8 \pmod{15}$ and $4^{-1} = 4 \pmod{15}$.

Since $|G| = 8$,

$$2^8 = 1 \pmod{15} \quad (5.64)$$

Then $2^{20} \pmod{15}$ can be calculated by decomposing its exponent:

$$2^{20} = 2^{2 \cdot 8 + 4} = (2^8)^2 * 2^4 = 1 * 16 = 1 \pmod{15} \quad (5.65)$$

6 Euclidean Algorithm

6.1 Euclidean Algorithm Basics

Definition 6.1.1 (Euclidean Algorithm). The *Euclidean Algorithm* can be used to compute the *greatest common divisor* of two integers $a, b \in \mathbb{Z}$, denoted $\gcd(a, b)$.

Its process, given $a \geq b$ is

$$a = q_0 \cdot b + r_1 \quad (6.1)$$

$$b = q_1 \cdot r_1 + r_2 \quad (6.2)$$

$$r_1 = q_2 \cdot r_2 + r_3 \quad (6.3)$$

\vdots

$$r_{k-1} = q_k \cdot r_k + r_{k+1} \quad (6.4)$$

$$r_k = q_{k+1} \cdot r_{k+1} + r_{k+2} \quad (6.5)$$

\vdots

$$r_{n-1} = q_n \cdot r_n + r_{n+1} \quad (6.6)$$

$$r_n = q_{n+1} \cdot r_{n+1} + 0 \quad (6.7)$$

Such that $\gcd(a, b) := r_{n+1}$.

6.2 $\gcd(a, b)$ as a Linear Combination of a and b

Proposition 6.2.1. Given $a, b \in \mathbb{Z}$, then for some $k_1, k_2 \in \mathbb{Z}$, and some $d \in \mathbb{Z}$,

$$d = \gcd(a, b) = k_1 a + k_2 b \quad (6.8)$$

Remark. To solve the congruence $4 * x = 1 \pmod{17}$ for x , find x in the form of $x = 4^{-1} \pmod{17}$.

For instance, to find $\gcd(34, 13)$ as a linear combination $k_1 a + k_2 b$, then first use the Euclidean algorithm to find $\gcd(34, 13)$:

$$\begin{array}{l|l} 34 = 2 \cdot 13 + 8 & a = 2 \cdot b + r_1 \\ 13 = 8 + 5 & b = r_1 + r_2 \\ 8 = 5 + 3 & r_1 = r_2 + r_3 \\ 5 = 3 + 2 & r_2 = r_3 + r_4 \\ 3 = 2 + \boxed{1} & r_3 = r_4 + \boxed{r_5} \\ 2 = 2 \cdot 1 + 0 & r_4 = 2 \cdot r_5 + 0 \end{array} \quad (6.9)$$

Note that

$$\begin{array}{ll}
 a = 2 \cdot b + r_1 & r_1 = a - 2b \\
 b = r_1 + r_2 & r_2 = b - r_1 \\
 r_1 = r_2 + r_3 & r_3 = r_1 - r_2 \\
 r_2 = r_3 + r_4 & r_4 = r_2 - r_3 \\
 r_3 = r_4 + \boxed{r_5} & \boxed{r_5} = r_3 - r_4 \\
 r_4 = 2 \cdot r_5 + 0 &
 \end{array} \quad (6.10)$$

It is now possible to *collect* k_1 and k_2 in a bottom-up manner:

$$\boxed{r_5} = r_3 - r_4 \quad (6.11)$$

$$= r_3 - (r_2 - r_3) \quad (6.12)$$

$$= -r_2 + 2r_3 \quad (6.13)$$

$$= -r_2 - 2(r_1 - r_2) \quad (6.14)$$

$$= 2r_1 - 3r_2 \quad (6.15)$$

$$= 2r_1 - 3(b - r_1) \quad (6.16)$$

$$= -3b + 5r_1 \quad (6.17)$$

$$= -3b + 5(a - 2b) \quad (6.18)$$

$$= 5a - 13b \quad (6.19)$$

Hence $\gcd(34, 13) = \gcd(a, b) = 5a - 13b$ for some $a, b \in \mathbb{Z}$. One may verify this by checking that

$$5 \cdot 34 - 13 \cdot 13 = 170 - 169 = 1 \quad (6.20)$$

6.3 Problems for Integers Modulo m

- $\boxed{a * x = b \pmod{m} \Leftrightarrow x = a^{-1} * b \pmod{m}}$
For \mathbb{R}^+ , given some $a, b, m \in \mathbb{Z}$

$$a * x = b \pmod{m} \quad (6.21)$$

$$\Leftrightarrow a^{-1} * a * x = a^{-1} * b \pmod{m} \quad (6.22)$$

$$\Leftrightarrow x = a^{-1} * b \pmod{m} \quad (6.23)$$

- $\boxed{a^n \pmod{m} \Leftrightarrow (a \cdot a^2 \cdot a^4 \cdot a^8 \cdot \dots) \pmod{m}}$

That is, to decompose the exponent into smaller equivalences.

- $\boxed{x^a = b \pmod{m} \Leftrightarrow x = b^{a^{-1}} \pmod{m}}$

For \mathbb{R}^+ , given some $a, b, m \in \mathbb{Z}$

$$x^a = b \pmod{m} \quad (6.24)$$

$$x = \sqrt[a]{b} \pmod{m} \quad (6.25)$$

$$x = b^{\frac{1}{a}} \pmod{m} \quad (6.26)$$

$$x = b^{a^{-1}} \pmod{m} \quad (6.27)$$

- For the discrete logarithm: $a^x = b \pmod{m} \Leftrightarrow x = \log_a b \pmod{m}$

6.4 Multiplicative Group of Integers Modulo m

Definition 6.4.1 (Relatively Prime, Coprime). Two integers $a, b \in \mathbb{Z}$ are *relatively prime* (or *coprime*) if

$$\gcd(a, b) = 1 \quad (6.28)$$

Definition 6.4.2 (Multiplicative Group of mod m). Given $m \in \mathbb{Z}$, then

$$G_m^\times := \{a \in \mathbb{Z} \mid (1 \leq a < m) \wedge (\gcd(a, m) = 1)\} \quad (6.29)$$

Forms a group $(G_m^\times, * \pmod{m})$ under *multiplicative modulo m* .

1. Closure

$$\forall a, b, m \in G_m^\times : (\gcd(a, m) = 1) \wedge (\gcd(b, m) = 1) \rightarrow (\gcd(a * b, m) = 1) \quad (6.30)$$

2. Associativity

Given by multiplication on integers modulo m .

3. Neutral Element

$$\forall m \in G_m^\times : \gcd(1, m) = 1 \quad (6.31)$$

4. Invertibility

$$\forall a \in G_m^\times : \exists y \in G_m^\times : a * y = 1 \pmod{m} \quad (6.32)$$

For which the inverse element y is denoted a^{-1} , giving

$$\forall a \in G_m^\times : a * a^{-1} = 1 \pmod{m} \quad (6.33)$$

Theorem 6.4.1 (Euler Totient Function). Given the *multiplicative modulo group G_m^\times* , then

$$\phi(m) := |G_m^\times| \quad (6.34)$$

Theorem 6.4.2. If p is prime then

$$\phi(p) \equiv p - 1 \quad (6.35)$$

Theorem 6.4.3. If p is prime and $k \geq 1$ then

$$\phi(p^k) \equiv p^{k-1}(p - 1) \quad (6.36)$$

Theorem 6.4.4. If $a, b \in \mathbb{Z}$ and a, b are *relatively prime* (i.e. $\gcd(a, b) = 1$) then

$$\phi(ab) \equiv \phi(a)\phi(b) \quad (6.37)$$

Theorem 6.4.5. If $a, m \in \mathbb{Z}$ are *relatively prime* (i.e. $\gcd(a, m) = 1$) then

$$a^{\phi(m)} \equiv 1 \pmod{m} \quad (6.38)$$

Theorem 6.4.6 (Fermat's Little Theorem). Given p is a prime number, then for any $a \in \mathbb{Z}$

$$a^p \equiv a \pmod{p} \quad (6.39)$$

Additionally, if $a, p \in \mathbb{Z}$ are *relatively prime*, $\gcd(a, p) = 1$,

$$a^{p-1} \equiv 1 \pmod{p} \quad (6.40)$$

Remark. Given $a \in G_m^\times$, to find x such that

$$a * x = b \pmod{m} \quad (6.41)$$

Find $a^{-1} \pmod{m}$.

For example, for

$$13 * x = 6 \pmod{34} \quad (6.42)$$

Since

$$x = 13^{-1} * 6 \pmod{34} \quad (6.43)$$

Find $13^{-1} \pmod{34}$ via the *Euclidean algorithm* which gives

$$13^{-1} = 21 \pmod{34} \quad (6.44)$$

Then

$$x = 21 * 6 \pmod{34} \quad (6.45)$$

$$= 126 - 3 * 34 \pmod{34} \quad (6.46)$$

$$= 24 \pmod{34} \quad (6.47)$$

Remark. To compute expressions of the form

$$a^n \pmod{m} \quad (6.48)$$

One should decompose a^n to $a^n = a \cdot a^2 \cdot a^4 \cdot \dots$, and use Fermat's Little Theorem and Euler Totient Function Identities whenever possible.

Remark. For equations of the form

$$x^a = b \pmod{m} \quad (6.49)$$

Then

$$x = b^{a^{-1}} \pmod{m} \quad (6.50)$$

If $\gcd(a, \phi(m)) = 1$ then

$$a * y = 1 \pmod{\phi(m)} \quad (6.51)$$

$$x = b^y \pmod{m} \quad (6.52)$$

if $\gcd(b, m) = 1$, that is if b, m are *relatively prime*

$$x^a = (b^y)^a \pmod{m} \quad (6.53)$$

$$= b^{a*y} \pmod{m} \quad (6.54)$$

$$= b^{1+k\phi(m)} \pmod{m} \quad (6.55)$$

$$= b * (b^{\phi(m)})^k \pmod{m} \quad (6.56)$$

$$= b * 1^k \pmod{m} \quad (6.57)$$

$$= b \pmod{m} \quad (6.58)$$

6.5 Rivest–Shamir–Adleman (RSA) Cryptography

Definition 6.5.1 (RSA, Public Keys and Private Keys). Given actors Alice and Bob, the process of RSA is

1. Alice provides *secrete* primes p and q .

$$n = p * q \quad (6.59)$$

2. Alice provides two integers d and e such that

$$d * e = 1 \pmod{\phi(p * q)} \quad (6.60)$$

3. Alice distributes the pair (n, e) to everyone.
4. Encryption and Decryption is then

$$\text{encrypt}_{n,e}(m) := m^e \pmod{n} \quad (6.61)$$

$$\text{decrypt}_{n,d}(m) := c^d \pmod{n} \quad (6.62)$$

5. Bob *encrypts* message m as the encrypted message c where

$$c := \text{encrypt}_{n,e}(m) \quad (6.63)$$

And sends c to Alice.

6. Alice *decrypts* c as

$$m' = \text{decrypt}_{n,d}(c) \quad (6.64)$$

Check that $\gcd(m, n) = 1$, that is if m, n are *relatively prime*, then

$$m' \pmod{n} = c^d \pmod{n} \quad (6.65)$$

$$= (m^e)^d \pmod{n} \quad (6.66)$$

$$= m^{d*e} \pmod{n} \quad (6.67)$$

$$= m^{1+k\phi(p*q)} \pmod{n} \quad (6.68)$$

$$= m \pmod{n} \quad (6.69)$$

Then *only* Alice can decrypt the encrypted message c in polynomial time.

Remark. An example of the RSA process:

1. Alice provides secret primes $p = 3, q = 41$

$$n = 3 * 41 = 123 \quad (6.70)$$

2. Alice provides two integers $d = 27, e = 3$

$$d * e \pmod{\phi(3 * 41)} = 27 * 3 \pmod{\phi(3 * 41)} \quad (6.71)$$

$$= 81 \pmod{[\phi(3) * \phi(41)]} \quad (6.72)$$

$$= 81 \pmod{[2 * 40]} \quad (6.73)$$

$$= 81 \pmod{80} \quad (6.74)$$

$$= 1 \pmod{80} \quad (6.75)$$

3. Alice distributes $(n, e) = (123, 3)$ to everyone.

4. The encryption and decryption functions are

$$\text{encrypt}_{n,e}(m) = m^3 \pmod{n} \quad (6.76)$$

$$\text{decrypt}_{n,d}(c) = c^{27} \pmod{n} \quad (6.77)$$

5. Given a message $m = 5$ then Bob sends

$$c = 5^3 \pmod{123} \quad (6.78)$$

$$= 125 \pmod{123} \quad (6.79)$$

$$= 2 \pmod{123} \quad (6.80)$$

6. Alice receives the encrypted message $c = 2$ and decrypts with the fact that $\gcd(123, 5) = 1$

$$m' \pmod{123} = 2^{27} \pmod{123} \quad (6.81)$$

$$= 5 \pmod{123} \quad (6.82)$$

7 Linear Algebra

7.1 Matrix Basics

Definition 7.1.1 (Matrix). A $(n \times m)$ -dimension matrix A has n rows and m columns, and each of its entries $a_{j,k}$, for $1 \leq j \leq n$ and $1 \leq k \leq m$ are denoted as

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{bmatrix} \quad (7.1)$$

Definition 7.1.2 (Set of Matrices of Dimension $n \times m$). Let $\mathcal{M}(n, m)$ denote the set of all matrices with dimension $n \times m$, that is, having n rows and m columns.

Definition 7.1.3 (Square Matrix). A *square matrix* is a matrix with dimension $n \times n$.

Definition 7.1.4 (Matrix Addition). Let $A, B \in \mathcal{M}(n, m)$ be two matrices of the same dimension $n \times m$. Then the sum matrix $C = A + B$ is defined to have entries

$$c_{j,k} = a_{j,k} + b_{j,k} \quad (7.2)$$

That is,

$$\begin{aligned} & \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{bmatrix} + \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,m} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,m} \end{bmatrix} \\ & := \begin{bmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & \cdots & a_{1,m} + b_{1,m} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} & \cdots & a_{2,m} + b_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} + b_{n,1} & a_{n,2} + b_{n,2} & \cdots & a_{n,m} + b_{n,m} \end{bmatrix} \end{aligned} \quad (7.3)$$

Definition 7.1.5 (Matrix Multiplication). Let A be an $(l \times m)$ matrix and B be an $(m \times n)$ matrix. Then their product $C = A \cdot B$ is the $(l \times n)$ matrix where each entry $c_{j,k}$ is

$$c_{j,k} := \sum_{s=1}^m a_{j,s} b_{s,k} \quad (7.4)$$

Note that matrix multiplication is *not commutative*, that is, for most cases $A \cdot B \neq B \cdot A$

Definition 7.1.6 (Identity Matrix). Let I_n denote the *identity* matrix with dimension $n \times n$

$$I_n := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \quad (7.5)$$

Notice that all diagonal entries $i_{j,k}$ with indices $j = k$ is 1, while all other entries are 0.

Alternatively, the *identity* matrix can be defined with entries $\delta_{j,k}$ where δ is the *Kronecker symbol* such that

$$\delta_{j,k} := \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases} \quad (7.6)$$

Definition 7.1.7 (Matrix Multiplication by Scalar λ). Let $\lambda \in \mathbb{R}$ be a constant, then the multiplication of an $(n \times m)$ -dimension matrix A by λ is defined as

$$\lambda A := \begin{bmatrix} \lambda a_{1,1} & \lambda a_{1,2} & \cdots & \lambda a_{1,m} \\ \lambda a_{2,1} & \lambda a_{2,2} & \cdots & \lambda a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{n,1} & \lambda a_{n,2} & \cdots & \lambda a_{n,m} \end{bmatrix} \quad (7.7)$$

If the dimension of A is $n \times n$, i.e. A is a *square matrix*, then λA is equivalently

$$\lambda A := \begin{bmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{bmatrix} \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix} \quad (7.8)$$

Lemma 7.1.1. If A is a matrix with dimension $n \times n$, A is a *square matrix*, then

$$AI \equiv IA \equiv A \quad (7.9)$$

Where I is the *identity* matrix with dimension $n \times n$.

Proof. Let $B = AI$, then

$$b_{j,k} = \sum_{s=1}^n a_{j,s} \delta_{s,k} \quad (7.10)$$

Only $\delta_{k,k}$ is non-zero, thus $b_{j,k} = a_{j,k}$. The same is true for IA . ■

7.1.1 Matrix Addition and Multiplication Properties

Proposition 7.1.1 (Associative Matrix Multiplication). Given matrices $A \in \mathcal{M}(n, m)$, $B \in \mathcal{M}(m, p)$ and $C \in \mathcal{M}(p, q)$ then

$$(AB)C \equiv A(BC) \quad (7.11)$$

Proof. The entry $t_{j,l}$ of $T = (AB)C$ is

$$t_{j,l} = \sum_{k=1}^p \left(\sum_{s=1}^m a_{j,s} b_{s,k} \right) c_{k,l} \equiv \sum_{k=1}^p a_{j,s} \left(\sum_{s=1}^m b_{s,k} c_{k,l} \right) = u_{j,l} \quad (7.12)$$

Where $u_{j,l}$ are entries of the matrix $U = A(BC)$ ■

Proposition 7.1.2 (Distributive Matrix Multiplication). Given matrices $A \in \mathcal{M}(n, m)$, $B \in \mathcal{M}(m, p)$ and $C \in \mathcal{M}(p, q)$ then

$$A(B + C) = AB + AC \quad (7.13)$$

$$(A + B)C = AC + BC \quad (7.14)$$

Proof. Let $S = A(B + C)$ and $E = AB + AC$, then each entry $s_{j,l}$ from S is

$$s_{j,l} = \sum_{s=1}^m a_{j,s} (b_{s,l} + c_{s,l}) \equiv \sum_{s=1}^m a_{j,s} b_{s,l} + \sum_{s=1}^m a_{j,s} c_{s,l} = e_{j,l} \quad (7.15)$$

Where $e_{j,l}$ are entries from E .

Let $T = (A + B)C$ and $F = AC + BC$, then each entry $t_{j,l}$ from T is

$$t_{j,l} = \sum_{s=1}^m (a_{j,s} + b_{j,s}) c_{s,l} \equiv \sum_{s=1}^m a_{j,s} c_{s,l} + \sum_{s=1}^m b_{j,s} c_{s,l} = f_{j,l} \quad (7.16)$$

Where $f_{j,l}$ are entries from F . ■

7.1.2 Determinant of a Square Matrix

Definition 7.1.8 (Determinant of a 2×2 Matrix). Given a 2×2 square matrix $A \in \mathcal{M}(2, 2)$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (7.17)$$

Then the determinant of A , denoted $\det(A)$ or $|A|$ is calculated with

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \quad (7.18)$$

Definition 7.1.9 (Determinant of a 3×3 Matrix). Given a 3×3 square matrix $A \in \mathcal{M}(3, 3)$

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \quad (7.19)$$

Then the determinant of A , denoted $\det(A)$ or $|A|$ is calculated with

$$\det(A) = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a \begin{vmatrix} \square & \square & \square \\ \square & e & f \\ \square & h & i \end{vmatrix} - b \begin{vmatrix} \square & \square & \square \\ d & \square & f \\ g & \square & i \end{vmatrix} + c \begin{vmatrix} \square & \square & \square \\ d & e & \square \\ g & h & \square \end{vmatrix} \quad (7.20)$$

$$= a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix} \quad (7.21)$$

$$= aei - afh + bfg - bdi + cdh - ceg \quad (7.22)$$

Definition 7.1.10 (Upper Triangular Matrix). An $n \times n$ matrix $A \in \mathcal{M}(n, n)$ is called a *upper triangular* (or *right triangular*) matrix if it has the form

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ & a_{2,2} & \cdots & a_{2,n} \\ & & \ddots & \vdots \\ 0 & & & a_{n,n} \end{bmatrix} \quad (7.23)$$

Where all the lower triangular part are 0s.

Lemma 7.1.2 (Determinant of an Upper Triangular Matrix). Given an $n \times n$ *upper triangular* matrix A , then its *determinant* $\det(A)$ can be calculated as

$$\det(A) = \begin{vmatrix} \gamma_1 & * & * & \cdots & * \\ \vdots & \gamma_2 & * & \ddots & \vdots \\ \vdots & \cdots & \gamma_3 & * & * \\ \vdots & \ddots & \vdots & \ddots & * \\ 0 & \cdots & \cdots & \cdots & \gamma_n \end{vmatrix} = \gamma_1 \gamma_2 \cdots \gamma_n \quad (7.24)$$

Where $*$ represents arbitrary entries.

Corollary 7.1.2.1. A specialization of this lemma is the case for 3×3 *upper triangular* matrix A :

$$\det(A) = \begin{vmatrix} \gamma_1 & * & * \\ 0 & a & b \\ 0 & c & d \end{vmatrix} = \begin{vmatrix} \gamma_1 & * & * \\ 0 & a & b \\ 0 & 0 & d - b \cdot \frac{c}{a} \end{vmatrix} = \gamma_1(ad - bc) \quad (7.25)$$

7.2 Solving Linear System of Equations

Definition 7.2.1. Matrices are useful for solving a *linear system of equations* of the form

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2 \\ \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n = b_n \end{cases} \quad (7.26)$$

Then, the matrix of the *coefficients* is denoted as A with dimension $n \times n$ where

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix} \quad (7.27)$$

The *unknowns* are denoted as X with dimension $n \times 1$ where

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad (7.28)$$

The *constants* are denoted as B with dimension $n \times 1$ where

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \quad (7.29)$$

Together, they yield the matrix equation

$$A \cdot X = B \quad (7.30)$$

To solve for X , one needs to find the *inverse* matrix A^{-1} of A such that

$$A \cdot X = B \quad (7.31)$$

$$A^{-1} \cdot A \cdot X = A^{-1} \cdot B \quad (7.32)$$

$$I \cdot X = A^{-1} \cdot B \quad (7.33)$$

$$X = A^{-1} \cdot B \quad (7.34)$$

Where I is the *identity* matrix.

7.3 Gaussian Elimination

Definition 7.3.1 (Augmented Matrix). Given a system of linear equations

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2 \\ \vdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n}x_n = b_n \end{cases} \quad (7.35)$$

Then its *augmented* matrix $A|B$ is

$$\left[\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} & b_{n,n} \end{array} \right] \quad (7.36)$$

Definition 7.3.2 (Row Operations).

1. **Multiply and Add Row**

Multiply row by scalar γ then add the result to another row.

$$\det(A') = \det(A) \quad (7.37)$$

2. **Swap Rows**

$$\det(A') = -\det(A) \quad (7.38)$$

3. **Multiply Row**

Multiply a row by scalar γ .

$$\det(A') = \gamma \det(A) \quad (7.39)$$

Definition 7.3.3 (Gaussian Elimination). Using the *row operations* applied to $A|B$ then one transforms $AX = B$ into an equivalent system

$$A'X = B' \quad (7.40)$$

If it is the case that

$$A' = I \quad (7.41)$$

Then there exists a *solution* $X = B'$ to the system

$$B' = A'X = IX = X \quad (7.42)$$

Definition 7.3.4 (Inverse Matrix). The *inverse* matrix A^{-1} of A is the matrix for which under multiplication yields the *identity* matrix I

$$AA^{-1} \equiv A^{-1}A \equiv I \quad (7.43)$$

With *Gaussian Elimination* applied to $A|I$ then one transforms

$$AA^{-1} = I \Rightarrow A'A^{-1} = B' \quad (7.44)$$

If

$$A' = I \quad (7.45)$$

Then there exists a solution to $A^{-1} = B'$

$$B' = A'A^{-1} = IA^{-1} = A^{-1} \quad (7.46)$$

Bibliography

- [1] Max Kanovich and Robin Hirsch.
“Lecture Notes on Discrete Mathematics for Computer Scientists”.
URL: http://www.cs.ucl.ac.uk/1819/a4u/t2/comp0147_discrete_mathematics_for_computer_scientists/.
- [2] Joseph J. Rotman. *A First Course in Abstract Algebra*. 3rd ed.
University of Illinois at Urbana-Champaign: Pearson. ISBN: 978-0131862678.