[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 6, 2017.

I216e (Computational Complexity and Discrete Math): Discrete Math

- URL: `http://www.jaist.ac.jp/~fujisaki/index-e.html`
- Date: 11/6, 11/8, 11/13, 11/15, 11/20 (twice), 11/22, 11/27 (test)
- Room: Room I-2
- Office Hour: Monday 13:30 – 15:10
- Reference (参考図書)
  - 「代数概論」森田康夫著，裳華房.
  - "Abstract Algebra," David Dummit and Richard Foote, Prentice Hall.
  - 「代数学入門」松本眞,
    Free eBook URL:
    `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/`
  - "A Computational Introduction to Number Theory and Algebra,"
    Victor Shoup, Cambridge University Press.
    Free eBook URL: `http://www.shoup.net/ntb/`

What will you study in the part of Discrete Math.?

From Algebra (抽象代数)

- Axioms of Groups (群), Rings (環), Fields (体)
- Equvalent class (同値類)
  - Equivalent relation (同値関係), Congruence (合同)
- Lagrange's Theorem (ラグランジェの定理)
  - Lagrange's Theorem $\rightarrow$ Fermat's little Theorem, and Euler's Theorem
- Fundamental Homomorphism Theorem(s) (準同型定理)
  - Normal subgroup (正規部分群), Residue class group (剰余類群) (= Quotient group (商群))
  - Fundamental Homomorphism Theorem $\rightarrow$ Chinese Reminder Theorem (CRT).
- Ring Fundamental Homomorphism Theorem (環準同型定理)
  - Ideal; Ideal (for ring) $\Longleftrightarrow$ Normal subgroup (for group).
  - Residue class ring (剰余類環) (= Quotient ring (商環))

What will you study (cont.)

Number Theory (初等整数論)

- Generalization of Integers (Informal)
  - Integral Domain (整域): Euclidean domain (ユークリッド整域), Principal ideal domain (PID) (単項イデアル整域), Unique factorization domain (UFD) (一意分解整域).
  - Euclidean domain $\subset$ PID $\subset$ UFD.
- Extended Euclidean Algorithm (拡張ユークリッドの互除法)
  - Solution for:
    - linear Diophantine equation (一次ディオファントス方程式), and
    - computing the inverse of an (invertible) element in (residue class) ring $\mathbb{Z}/n\mathbb{Z}$.

Application: RSA public-key cryptosystem. Related to:

- Euler's totient function $\phi(n)$, Euler's Theorem
- Structure of $\mathbb{Z}/n\mathbb{Z}$
- Chinese Remainder Theorem

Today's Lecture

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

- A main actor in this course.
- Called "zed over en zed" (or "zi over en zi").
- For convenience, regard $\mathbb{Z}/n\mathbb{Z}$ as the set $\{0, 1, \dots, n-1\}$, where n is a positive integer.
- Define two binary operations, addition "$+$" and multiplication "$\cdot$", for $a, b \in \mathbb{Z}/n\mathbb{Z}$ as:

$$a + b := a + b \bmod n$$
$$a \cdot b := a \cdot b \bmod n$$

  Then, $\mathbb{Z}/n\mathbb{Z}$ is close under addition "$+$" and multiplication "$\cdot$".
- $(\mathbb{Z}/n\mathbb{Z}, +)$: Group.
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$: Ring.
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$: Field (if n is prime).

The Extended Euclidean Algorithm

- The Euclidean Algorithm: is an algorithm to output the greatest common divisor (GCD) of $a, b \in \mathbb{Z}$ (i.e., $d := (a, b)$)
- The Extended Euclidean Algorithm (Ext EA): is an algorithm to output (X, Y, d), where $X, Y \in \mathbb{Z}$ and the GCD d, such that

  $$aX + bY = d$$

  for $a, b \in \mathbb{Z}$.
- Note: The Ext EA computes a^{-1} for $a \in \mathbb{Z}/n\mathbb{Z}$ if a^{-1} exists.
- Note: a^{-1} exists for $a \in \mathbb{Z}/n\mathbb{Z}$ if and only if there are integers (X, Y) such that $aX + nY = 1$.
- Note: There exist integers (X, Y) such that $aX + nY = 1$ if and only if $(a, n) = 1$.

Fermat's little Theorem (フェルマーの小定理)

- For $a \in \mathbb{Z}$ and prime p, it holds that

$$a^{p-1} = 1 \pmod{p}.$$

Easily led by Lagrange's Theorem.

Chinese Remainder Theorem (中国人の剰余定理)

- In Sunzi Suanjing (「孫子算経」): What is that integer when divided by 3 is remainder 2; divided by 5 is remainder 3; and divided by 7 is remainder 2.

$$x = 2 \bmod 3$$
$$x = 3 \bmod 5$$
$$x = 2 \bmod 7$$

- For $n = p_1 p_2 \cdots p_k$ (such that for every p_i, p_j $(i \neq j)$, $(p_i, p_j) = 1$), it holds

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z}. \quad \text{(isomorphism)}$$

The CRT gives the concrete map ψ.

$$\psi : \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}.$$

Finite Field $\mathbb{F}_{p^n}$ (有限体)

- Also known as $GF(p^n)$ (in coding theory).
- p is a prime number, and $n \in \mathbb{N}$.
- The order (位数) of $\mathbb{F}_{p^n}$ is p^n, where the order means the number of the elements in $\mathbb{F}_{p^n}$.
- $\mathbb{F}_p$ is called a prime field, and $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ (isomorphism).
- Can represent an element in $\mathbb{F}_{p^n}$ as that in $\mathbb{Z}/p\mathbb{Z}[X]$, such that for some $f(x)$, addition $+$ and multiplication $\cdot$ are defined as:

$$a(X) + b(X) = a(X) + b(X) \bmod f(X)$$
$$a(X) \cdot b(X) = a(X) \cdot b(X) \bmod f(X)$$

where $a(X), b(X) \in \mathbb{Z}/p\mathbb{Z}[X]$.

Today's Lecture

Binary Operation (二項演算) and Magma

Definition 1

A *binary operation* $\circ$ on set S is a function $\circ : S \times S \to S$. For any $a, b \in S$, we shall write $a \circ b$.

- The usual addition and multiplication, $+, \times$, on the set of natural numbers $\mathbb{N}$ are binary operations.
- Are the addition $+$, subtraction $-$, and $\times$ on $\mathbb{Z}$ and $\mathbb{R}$ binary operation ?
- How about addition, subtraction, product on the $n \times n$ square matrices ?

Definition 2

A set S associated with binary operation $\circ$, denoted $(S, \circ)$, is called a *magma*.

Semi-group (半群) and Monoid (単位的半群)

Definition 3

Magma $(G, \circ)$ is called a semi-group if

- G_1 (結合法則): $\forall a, b, c \in G\,[(a \circ b) \circ c = a \circ (b \circ c)]$
  i.e., $\circ$ is *associative*.

Definition 4

An element $e \in G$ for semi-group $(G, \circ)$ is called an *identity* (単位元) if

- $\forall a \in G\,[a \circ e = e \circ a = a]$.

Definition 5

A seme-group $(G, \circ)$ is called a *monoid* if it has an identity e.

Uniquness of Identity

Proposition 1

An idenity e is *unique* if semi-group$(G, \circ)$ has e,
i.e., If there are two identies, e, e', then $e = e'$.

Proof.

Homework or at this lecture. □

Inverse (逆元) and Invertible Element (可逆元)

Definition 6

Let $(G, \circ)$ be a monoid with identy e. $a' \in G$ is called an *inverse* of $a \in G$ if $a \circ a' = a' \circ a = e$. Then, $a \in G$ is called an *invertible element* or an *unit* (単元).

By a^{-1}, denote *the* inverse of a.
Note that the inverse of a is unique if $(G, \circ)$ is a monoid.

Group (群)

Definition 7

Let $(G, \circ)$ be a monoid. Then, $(G, \circ)$ is called a group (群) if all elements in G are invertible.

Equivalently,

Definition 8

Let G be a set and $\circ$ be a binary operation on G. $(G, \circ)$ is called a *group* (群) if the it satisfies the following axioms:

- G_1 (結合法則) $\forall a, b, c \in G \quad [(a \circ b) \circ c = a \circ (b \circ c)]$.
- G_2 (単位元の存在) $\exists e \in G, \forall a \in G \quad [a \circ e = e \circ a = a]$.
- G_3 (逆元の存在) $\forall a \in G, \exists a^{-1} \in G \quad [a \circ a^{-1} = a^{-1} \circ a = e]$.

Abelian Group (Abel 群) or Commutative Group (可換群)

Definition 9

A group $(G, \circ)$ is called *commutative* or *abelian* if

- G_4 （可換律） $\forall a, b \in G \quad [a \circ b = b \circ a]$.

- For an Abelian group, often represent $\circ$ as $+$, and call $(G, +)$ an *additive group* (加法群).
- $(G, \circ)$ is called a *finite group* if G is a finite set.
- The number of elements in a group (resp. ring, or field) is called the *order* (位数) of the group (resp. the ring, or the field).

Ring (環)

Definition 10

A *ring* R is a set together with two binary operations, $+$ and $\cdot$, denoted by $(R, +, \cdot)$, satisfying the following axioms:

- R_1: $(R, +)$ is an Abelian group (or an additive group). That is:
  - G_1: For all $a, b, c \in R$, $(a+b)+c = a+(b+c)$.
  - G_2: For all $a \in R$, there is the identity 0 such that $a+0 = 0+a$.
  - G_3: For all $a \in R$, there is the inverse $(-a)$ such that $a+(-a) = (-a)+a = 0$.
  - G_4: For all $a, b \in R$, $a+b = b+a$.
- R_2: $(R, \cdot)$ is a sem-group, i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- R_3 [distributed law (分配法則)]: For all $a, b, c \in R$,

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

Field (体)

Definition 11

A ring $(K, +, \cdot)$ is called a *field* if

- $(K - \{0\}, \cdot)$ is a commutative group (可换群).

- We write $K^\times$ to denote the set of invertible elements in monoid $(K, \cdot)$.
- $(K, +, \cdot)$ is a field if and only if $K^\times = K - \{0\}$ and $(K^\times, +)$ is commutative.
- Let 1 be the identiy of group $(K^\times, \cdot)$. Then, $1 \neq 0$ by definition.
- $(K^\times, \cdot)$ is called the multicative group (乘法群) of field $(K, +, \cdot)$.

Consider examples:

- Magma (マグマ)
- Semi-group (半群)
- Monoid (単位的半群)
- Group (群)
  - Commutative (可換)
  - Non-commutative (非可換)
- Ring (環)
- Field (体)