[I216e] Computational Complexity and Discrete Mathematics

Ryuhei Uehara, and Eiichiro Fujisaki

Japan Advanced Institute of Science and Technology

November 13th, 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 Contents

Equivalence Relation (同値関係)

Definition 1 (Binary Relation (関係))

A binary relation on set S is a subset R of $S \times S$ ($R \subset S \times S$) and we write $a \sim b$ if $(a, b) \in R$.

Definition 2 (Equivalence Relation)

We say that relation (on set S), $\sim$, is an *equivalence relation* (on S) if for all $a, b, c \in S$, the following conditions hold.

- (Reflexive) $a \sim a$.
- (Symmetric) If $a \sim b$, then $b \sim a$.
- (Transitive) If $a \sim b$ and $b \sim c$, then $a \sim c$.

Equivalence Class (同値類)

Definition 3 (Equivalence Class)

Let $\sim$ be an equivalence relation on S. We define by $C(a) \triangleq \{x \in S \mid x \sim a\}$ *the equivalence class* of a (with respects to $(S, \sim)$).

Proposition 1

- $a \in C(a)$.
- If $b \in C(a)$, then $C(b) = C(a)$.
- If $C(a) \neq C(b)$, then $C(a) \bigcap C(b) = \emptyset$.

Partition (分割)

Definition 4 (Partition)

Let I be some index set. A collection $\{S_i | i \in I\}_{i \in I}$ of subsets of S is called *a partition* of S if

- $S = \bigcup_{i \in I} S_i$, and
- For all $i, j \in I$ $(i \neq j)$, $S_i \bigcap S_j = \emptyset$.

The notions of an equivalence relation on S and a partition of S are the same:

Proposition 2

- Let $\sim$ be an equivalence relation on S. Then, $\{C(a)\}_{a \in S}$, where $C(a) = \{x \mid x \sim a\}$, is a partition of S.
- If $\{S_i | i \in I\}_{i \in I}$ is a partition of S, then there is an equivalence relation $\sim$ on S, such that the equivalence classes are precisely $\{S_i | i \in I\}$'s $(i \in I)$.

More,

Proposition 3

Let $\sim$ be an equivalence relation on S and let $C(a) = \{x \in S \mid x \sim a\}$ be the equivalence class of a. Then, there is a subset A of S ($A \subset S$) such that

- $\{C(a)\}_{a \in A}$ is a partition of S, and
- For all $a, b \in A$ ($a \neq b$), $C(a) \bigcap C(b) = \emptyset$.

- The partition of S defined by $\sim$, i.e., $\{C(a)\}_{a \in S}$, is unique.
- In other word, $\{C(a)\}_{a \in A}$ and $\{C(a)\}_{a \in S}$ are the same partition, regardless of the choice of A (where A is not unique).

Quotient Set (商集合)

Definition 5 (Quotient Set)

We write $S/\!\sim$ to denote the partition of S defined by $\sim$, and call it *the quotient set* of S by $\sim$.

Today's Contents

1. Equivalence Class (同値類), Partition (分割), and Quotient Set (商集合)
2. Congruence (合同) and Residue Class (剰余類)
3. Lagrange's Theorem
4. Fermat's Little Theorem and Euler's Theorem
5. Appendix (Reminder)

Congruence (合同)

Definition 6 (Congruence)

For $n \in \mathbb{N}$, we say that a is *congruent* to b mod n (a は n を法として b と合同である) if n divides $(a - b)$, i.e., $n|(a - b)$. Also write

$$a \equiv b \pmod{n} \quad \text{if and only if} \quad n|(a - b)$$

- Note that the congruence mod n defines an equivalence relation $\sim_n$ on $\mathbb{Z}$:

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad a \sim_n b$$

- The equivalence classes of $\mathbb{Z}$ by $\sim_n$ are

$$n\mathbb{Z},\ 1 + n\mathbb{Z},\ \ldots,\ (n-1) + n\mathbb{Z}.$$

We write $\mathbb{Z}/n\mathbb{Z}$ to denote the quotient set (of $\mathbb{Z}$ by $\sim_n$), i.e., $\mathbb{Z}/\sim_n$.

Residue class (剰余類) or Coset (傍系)

Definition 7 (Reminder)

Let H be a subgroup of G. For $a \in G$, define

$$aH \triangleq \{a \circ h | h \in H\}$$
$$Ha \triangleq \{h \circ a | h \in H\}.$$

We call aH a left coset (左剰余類) of H and Ha a right coset (右剰余類) of H.

If G is commutative (可換), then $aH = Ha$.

Equivalence Relation from Residue Class

Let H be a subset of G and aH be a left coset (左剰余類).

Proposition 4

For $a, b \in G$, define

$$a \sim b \quad \text{by} \quad aH = bH.$$

Then, $\sim$ turns out an equivalence relation on G.

Proof.

- $aH = aH$.
- If $aH = bH$, then $bH = aH$.
- If $aH = bH$ and $bH = cH$, then $aH = cH$.

$\square$

Similarly, the right coset of H defines an equivalence relation. Note that $aH \neq Ha$ in general.

Proposition 5

For $a, b \in G$, it holds that

$$aH = bH \iff a^{-1}b \in H.$$

So, we can also define $a \sim b$ by $a^{-1}b \in H$, instead of $aH = bH$. We say that *a is left congruent to b mod H*.

$$a \equiv b \pmod{H} \iff a^{-1}b \in H$$

We can similarly define *the right congruence mod H*.

This is a generalization of the congruence mod integer n.

Congruence and Residue Class, Cont.

- The congruence mod integer n: For $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod{n} \iff a - b \in n\mathbb{Z}$$

- The (left) congruence mod subgroup H: For $a, b \in G$,

$$a \equiv b \pmod{H} \iff a^{-1} \circ b \in H$$

- The (right) congruence mod subgroup H: For $a, b \in G$,

$$a \equiv b \pmod{H} \iff a \circ b^{-1} \in H$$

Note $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. *The congruence mod a subgroup* forms an equivalence class.

Today's Contents

Quotient Set over Left/Right Coset

Definition 8

Let H be a subset of G.

- We write G/H to denote $\{aH\}_{a \in G}$.
- We write $G \backslash H$ to denote $\{Ha\}_{a \in G}$.

Index (指数) of Subgroup

Theorem 9

$$|G/H| = |G\backslash H|.$$

If G is commutative, then trivial. However, the above holds even for any group G and any subgroup H.

Proof.

1. $a \in G \mapsto a^{-1} \in G$ is bijective (全単射) (due to the uniquenss of inverse in Monoid).
2. So, $ah \mapsto (ah)^{-1} = h^{-1} \circ a^{-1}$ is bijective and hence $aH = Ha^{-1}$.
3. There is a subset A of G such that $\{aH\}_{a \in A}$ partitions G and for all $a, b \in A$ ($a \neq b$), $aH \bigcap bH = \emptyset$.
4. By $aH = Ha^{-1}$, $\{Ha^{-1}\}_{a \in A}$ also partions G. Since $aH = Ha^{-1}$, $\{aH\}_{a \in A}$ and $\{Ha^{-1}\}_{a \in A}$ are the same partion of G.
5. Hence, $|A| = |G/H| = |G\backslash H|$. Regardless of the choice of A, G/H and $G\backslash H$ are unique.

□

Definition 10

We say that $[G : H] \triangleq |G/H| = |G\backslash H|$ is *the index of H in G*.

Lagrange's Theorem

Theorem 11 (Lagrange's Theorem)

Let H be a subset of G. Then,

- $|G| = [G : H]|H|$.
- *Let G be a finite group. Then, the order of H divides the order of G, i.e., $|H|$ divides $|G|$.*

Proof.

Let $\{aH\}_{a \in A}$ be the partion of G by the left coset of H such that for all $a, b \in A$ $(a \neq b)$, $aH \bigcap bH = \emptyset$. Then $[G : H] = |A|$. For all $a \in A$, $h (\in H) \mapsto ah (\in aH)$ is bijective. Therefore, $|G| = [G : H]|H|$. $\square$

Today's Contents

Cyclic Group (巡回群)

Let G be a group. For $a \in G$, define $a^n \triangleq \overbrace{a \circ \cdots \circ a}^{n}$ and write $\{\ldots, a^{-1}, a^0, a^1, \ldots\}$ as $\langle a \rangle$, i.e., $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.

Theorem 12

$\langle a \rangle$ is a subgroup of G.

- Even for non-commutative G, $\langle a \rangle$ is a commutative group.
- $\langle a \rangle$ is called *a cyclic group*.
- a is called *a generator* of $\langle a \rangle$. In general, a is not unique.

Definition 13

The smallest positive number n such that $a^n = 1$ (where 1 is the identity) is called *the order* of a. If such a positive number does not exist, the order of a is said *infinite*.

The order of a is equivalent to the order of $\langle a \rangle$.

Fermat's Little Theorem

Theorem 14 (Fermat's Little Theorem)

Let p be a prime. For $a \in \mathbb{N}$, the following holds.

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof.

$(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$ and $\langle a \rangle$ is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's Theorem, the order of a (i.e., the order of $\langle a \rangle$) divides $p-1$. Hence, $a^{p-1} = 1 \in (\mathbb{Z}/p\mathbb{Z})^\times$. $\square$

Euler's Totient Function (オイラー関数)

Definition 15

$\phi(n) \triangleq \{x \in \mathbb{N} \mid 1 \leq x \leq n-1 \text{ and } (x,n) = 1\}$ (for $2 \leq n$) is called *Euler's ϕ function* or *Euler's totient function*. For $n = 1$, we define $\phi(1) = 1$.

Proposition 6

- For $(m,n) = 1$, it holds that $\phi(mn) = \phi(m)\phi(n)$.
- For prime p and positive integer e, it holds that $\phi(p^e) = p^{e-1}(p-1)$.
- Let $n = \prod_{i=1}^{s} p_i^{e_i}$. Then, it holds that

$$\phi(n) = n\prod_{i=1}^{s}(1 - \frac{1}{p_i}).$$

Euler's Theorem (オイラーの定理)

Theorem 16 (Euler's Theorem)

For $a, n \in \mathbb{N}$,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof.

From the fact that the order of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is $\phi(n)$. $\square$

Today's Contents

Group (群)

Definition 17 (Axiom of Group)

Let G be a set associated with a binary operation $\circ$. G is called a *group* if the it satisfies the following axioms:

- G_0 （二項演算） $\circ : G \times G \to G$ is a binary operation on G.
- 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 （全て可逆元） $\forall a \in G, \exists a^{-1} \in G \quad [a \circ a^{-1} = a^{-1} \circ a = e]$.

Definition 18

Group G is called *abelian* or *commutative* if the following condition holds:

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

Subgroup (部分群)

Definition 19

H is called a *subgroup* of group G if:

- $H \subseteq G$ (i.e., H is a subset of G).
- $\forall a, b \in H \quad [a \circ b \in H]$ (i.e., $\circ$ is a binary operation on H).
- $\forall a \in H \quad [a^{-1} \in H]$.

Theorem 20

H is a subgroup of G if and only if

$$\forall a, b \in H \quad [a \circ b^{-1} \in H]$$