Mathematical Proof: Problem Set 8

Koichiro Takahashi

May 1, 2024

Problem.1

Given a relation $\mathcal{R}$ on a set A, the inverse relation is defined by

$$\mathcal{R}^{-1} = \{(b, a) \in (A \times A) \mid (a, b) \in \mathcal{R}\}$$

Since $\mathcal{R} \subseteq (A \times A)$, the cardinality of $\mathcal{R}$ has an upper bound given by $|\mathcal{R}| \leq |A \times A|$.
First, we show a lemma

$$\text{Lemma1: } \mathcal{R} \cap \mathcal{R}^{-1} = \emptyset \Leftrightarrow \forall (a, b) \in \mathcal{R}, (b, a) \notin \mathcal{R}.$$

Proof: Let $\mathcal{R}$ be a relation on a set A, and $\mathcal{R}^{-1}$ is its inverse relation.

($\Rightarrow$) Suppose $\mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$. We prove by contradiction.

Assume, to the contrary, that $\exists (a, b) \in \mathcal{R}$ *s.t.* $(b, a) \in \mathcal{R}$. Then immediately, by definition of the inverse relation, $(a, b) \in \mathcal{R}^{-1}$. Therefore, $(a, b) \in (\mathcal{R} \cap \mathcal{R}^{-1})$, which is a contradiction since $\mathcal{R} \cap \mathcal{R}^{-1} = \emptyset$.

($\Leftarrow$) Suppose $\forall (a, b) \in \mathcal{R}, (b, a) \notin \mathcal{R}$.
We prove by contradiction. Assume, to the contrary, that $\mathcal{R} \cap \mathcal{R}^{-1} \neq \emptyset$. Then,

$$\exists (x, y) \in (\mathcal{R} \cap \mathcal{R}^{-1})$$

Therefore, $(x, y) \in \mathcal{R}$, but also $(x, y) \in \mathcal{R}^{-1}$. Then, by definition of the inverse relation, $(x, y) \in \mathcal{R}^{-1}$, which is a contradiction since $\forall (a, b) \in \mathcal{R}, (b, a) \notin \mathcal{R}$.

From the above, the statement is true. ■

Now, we prove the conjecture that $|\mathcal{R}_{max}| = 6$.

Proof: Suppose A is a set with exactly 4 elements, which defined in general by

$$A = \{x, y, z, w\}$$

where x, y, z, w are distinct elements.
Without loss of generality, by using Lemma 1, $\mathcal{R}_{max}$, which has a largest cardinality in the possible $\mathcal{R} \subseteq (A \times A)$ is given by

$$\mathcal{R}_{max} = \{(x, y), (x, z), (x, w), (y, z), (y, w), (z, w)\}$$

Therefore, $|\mathcal{R}_{max}| = 6$. ■

Problem.2

Here, $A = \{1, 2, 3, 4\}$. Let $\mathcal{R}$ be a relation on a set A, which satisfy a certain condition on each problem.

(a)

$$\mathcal{R} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 1), (3, 3), (4, 4)\}$$

(b)

$$\mathcal{R} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3), (4, 4)\}$$

(c)

$$\mathcal{R} = \{(1, 1), (1, 2), (2, 1)\}$$

(d)

$$\mathcal{R} = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3), (4, 4)\}$$

(e)

$$\mathcal{R} = \{(1, 2), (2, 1)\}$$

(f)

$$\mathcal{R} = \{(1, 2)\}$$

Problem.3

Let $A = \{a, b, c\}$, and let $\mathcal{R}$ be a relation on A such that $\mathcal{R}$ has none of the properties reflexive, symmetric and transitive.

Now, we prove the conjecture that $|\mathcal{R}_{max}| = 7$ *Proof*: Since $\mathcal{R} \subset (A \times A)$, any elements in possible relations $\mathcal{R}$ on A is in $(A \times A)$

Here,

$$A \times A = \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}$$

which is an equivalence relation on A.
To break its reflexivity, we remove (c, c).
Then, $\{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b)\}$, which still has its symmetry and transitivity.
To break its symmetry and transitivity, we remove (c, b).
Then, $\{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a)\}$, which still has its symmetry and transitivity. Note that (c, a) and (a, b) is in the modified relation.
Therefore, we define $\mathcal{R}_{max}$ as below:

$$\mathcal{R}_{max} = \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a)\}$$

and $\mathcal{R}_{max}$ gives the maximum number of a relation $\mathcal{R}$, where $|\mathcal{R}_{max}| = 7$.

From the above, the statement is true. ■

Problem.4

(a)
Proof: Let $\mathcal{R}_1, \mathcal{R}_2$ be equivalence relations on a set A.

Since $\mathcal{R}_1$ and $\mathcal{R}_2$ are both equivalent relations, they are reflexive. Thus, $\forall a \in A, \exists (a, a) \in (\mathcal{R}_1 \cap \mathcal{R}_2)$. Therefore, $\mathcal{R}_1 \cap \mathcal{R}_2$ is reflexive.

Let $(a, b) \in (\mathcal{R}_1 \cap \mathcal{R}_2) \subseteq (A \times A)$, where $a, b \in A$. By definition, $(a, b) \in \mathcal{R}_1$ and $(a, b) \in \mathcal{R}_2$. Since $\mathcal{R}_1$ and $\mathcal{R}_2$ are both equivalent relations, they are symmetric. Thus, $(b, a) \in \mathcal{R}_1$ and $(b, a) \in \mathcal{R}_2$. Therefore, $(b, a) \in (\mathcal{R}_1 \cap \mathcal{R}_2)$, so that $\mathcal{R}_1 \cap \mathcal{R}_2$ is symmetric.

Let $(a, b), (b, c) \in (\mathcal{R}_1 \cap \mathcal{R}_2) \subseteq (A \times A)$, where $a, b, c \in A$. By definition, $(a, b) \in \mathcal{R}_1$ and $(a, b), (b, c) \in \mathcal{R}_2$. Since $\mathcal{R}_1$ and $\mathcal{R}_2$ are both equivalent relations, they are transitive. Thus, $(a, c) \in \mathcal{R}_1$ and $(a, c) \in \mathcal{R}_2$. Therefore, $(a, c) \in (\mathcal{R}_1 \cap \mathcal{R}_2)$, so that $\mathcal{R}_1 \cap \mathcal{R}_2$ is transitive.

From the above, $\mathcal{R}_1 \cap \mathcal{R}_2$ is an equivalence relation on A, so that the statement is true. ■

(b)
Disproof: We disprove by counterexample.

Let A be a non-empty set defined by

$$A = \{1, 2, 3\}$$

Let $\mathcal{R}_1, \mathcal{R}_2$ be equivalence relations on a set A given by

$$\mathcal{R}_1 = \{(1,1), (1,2), (2,1), (2,2), (3,3)\}$$

and

$$\mathcal{R}_2 = \{(1,1), (2,2), (2,3), (3,2), (3,3)\}$$

Then

$$\mathcal{R}_1 \cup \mathcal{R}_2 = \{(1,1), (1,2), (2,1), (2,2), (2,3), (3,2), (3,3)\}$$

Immediately, $(1,2), (2,3) \in \mathcal{R}_1 \cup \mathcal{R}_2$, but $(1,3) \notin \mathcal{R}_1 \cup \mathcal{R}_2$. Therefore, $\mathcal{R}_1 \cup \mathcal{R}_2$ is not transitive, so that $\mathcal{R}_1 \cup \mathcal{R}_2$ is not an equivalence relation on A. Thus $\mathcal{R}_1 \cup \mathcal{R}_2$ forms a counterexample. ♦

Problem.5

Define an equivalence relation $\mathcal{R}$ on $\mathbb{Z}$ given by

$$\mathcal{R} = \{(x, y) \in (\mathbb{Z} \times \mathbb{Z}) \mid x^3 \equiv y^3 \pmod 4\}$$

First we consider the divisibility of y^3 for $y \in \mathbb{Z}$ by four cases.
Case 1: $y \equiv 0 \pmod 4$. Then, $\exists k \in \mathbb{Z}$ $s.t.$ $y = 4k$. Thus $y^3 = (4k)^3 = 4 \cdot 16k^3$, $y^3 \equiv 0 \pmod 4$.

Case 2: $y \equiv 1 \pmod 4$. Then, $\exists k \in \mathbb{Z}$ $s.t.$ $y = 4k + 1$. Thus $y^3 = (4k+1)^3 = 64k^3 + 48k^2 + 12k + 1 = 4(16k^3 + 12k^2 + 3k) + 1$, $y^3 \equiv 1 \pmod 4$.

Case 3: $y \equiv 2 \pmod 4$. Then, $\exists k \in \mathbb{Z}$ $s.t.$ $y = 4k + 2$. Thus $y^3 = (4k+2)^3 = 64k^3 + 96k^2 + 48k + 8 = 4(16k^3 + 24k^2 + 12k + 2)$, $y^3 \equiv 0 \pmod 4$.

Case 4: $y \equiv 3 \pmod 4$. Then, $\exists k \in \mathbb{Z}$ $s.t.$ $y = 4k + 3$. Thus $y^3 = (4k+3)^3 = 64k^3 + 144k^2 + 108k + 27 = 4(16k^3 + 36k^2 + 27k + 6) + 3$, $y^3 \equiv 3 \pmod 4$.

Therefore, in summary, for $y \in \mathbb{Z}$

$$y \equiv 0 \pmod 4 \Rightarrow y^3 \equiv 0 \pmod 4$$

$$y \equiv 1 \pmod 4 \Rightarrow y^3 \equiv 1 \pmod 4$$

$$y \equiv 2 \pmod 4 \Rightarrow y^3 \equiv 0 \pmod 4$$

$$y \equiv 3 \pmod 4 \Rightarrow y^3 \equiv 3 \pmod 4$$

Now, we determine the distinct equivalence classes, starting from the integer $0, 1, 3, \ldots$.

$$[0] = \{x \in \mathbb{Z} \mid x\mathcal{R}0\} = \{x \in \mathbb{Z} \mid x^3 \equiv 0^3 \equiv 0 \pmod 4\}$$

$$= \{0, \pm 2, \pm 4, \pm 6, \ldots\}$$

$$[1] = \{x \in \mathbb{Z} \mid x\mathcal{R}1\} = \{x \in \mathbb{Z} \mid x^3 \equiv 1^3 \equiv 1 \pmod 4\}$$

$$= \{\ldots, -11, -7, -3, 1, 5, 9, \ldots\}$$

$$[3] = \{x \in \mathbb{Z} \mid x\mathcal{R}3\} = \{x \in \mathbb{Z} \mid x^3 \equiv 3^3 \equiv 3 \pmod 4\}$$

$$= \{\ldots, -9, -5, -1, 3, 7, 11, \ldots\}$$

and obviously $[0], [1], [3]$ are a partition of $\mathbb{Z}$.

Therefore, the equivalence classes of $\mathcal{R}$ are given by $[0], [1], [3]$.

Problem.6

Define an equivalence relation $\mathcal{R}$ on $\mathbb{Z}$ given by

$$\mathcal{R} = \{(a, b) \in (\mathbb{Z} \times \mathbb{Z}) \mid a^2 \equiv b^2 \pmod 5\}$$

First, we prove that $\mathcal{R}$ is an equivalence relation on $\mathbb{Z}$.

Proof:

Let $a \in \mathbb{Z}$. Since $5 \mid 0$, it follows that $5 \mid (a^2 - a^2)$, so that $a^2 \equiv a^2 \pmod 5$. Thus, $(a, a) \in \mathcal{R}$ implying that $\mathcal{R}$ is reflexive.

Next, let $(a, b) \in \mathcal{R}$, where $a, b \in \mathbb{Z}$. Then, $5 \mid (a^2 - b^2)$. Here, $(b^2 - a^2) = -(a^2 - b^2)$. Since we know that $\forall x, n \in \mathbb{Z}\ s.t.\ n \neq 0,\ n \mid x \Rightarrow n \mid (-x)$, and $(a^2 - b^2), 5 \in \mathbb{Z}\ s.t.\ 5 \neq 0$, it

follows that $5 \mid (b^2 - a^2)$. Thus, $(b, a) \in \mathcal{R}$ implying that $\mathcal{R}$ is symmetric.

Lastly, let $(a, b), (b, c) \in \mathcal{R}$. By definition, $5 \mid (a^2 - b^2)$ and $5 \mid (b^2 - c^2)$. Here, $a^2 - c^2 = (a^2 - b^2) + (b^2 - c^2)$. Since we know that $\forall x, y, n \in \mathbb{Z}\ s.t.\ n \neq 0,\ n \mid x$ and $n \mid y \Rightarrow n \mid (x+y)$, and $(a^2 - b^2), (b^2 - c^2), 5 \in \mathbb{Z}\ s.t.\ 5 \neq 0$, it follows that $5 \mid (a^2 - c^2)$. Thus, $(a, c) \in \mathcal{R}$ implying that $\mathcal{R}$ is transitive.

From the above, the statement is true. ■

Next, we consider the divisibility of y^2 for $y \in \mathbb{Z}$ by five cases.
Case 1: $y \equiv 0 \pmod 5$. Then, $\exists k \in \mathbb{Z}\ s.t.\ y = 5k$. Thus $y^2 = (5k)^2 = 5 \cdot 5k^2$, $y^2 \equiv 0 \pmod 5$.

Case 2: $y \equiv 1 \pmod 5$. Then, $\exists k \in \mathbb{Z}\ s.t.\ y = 5k+1$. Thus $y^2 = (5k+1)^2 = 25k^2+10k+1 = 5(5k^2+2k)+1$, $y^2 \equiv 1 \pmod 5$.

Case 3: $y \equiv 2 \pmod 5$. Then, $\exists k \in \mathbb{Z}\ s.t.\ y = 5k+2$. Thus $y^2 = (5k+2)^2 = 25k^2+20k+4 = 5(5k^2+4k)+4$, $y^2 \equiv 4 \pmod 5$.

Case 4: $y \equiv 3 \pmod 5$. Then, $\exists k \in \mathbb{Z}\ s.t.\ y = 5k+3$. Thus $y^2 = (5k+3)^2 = 25k^2+30k+9 = 5(5k^2+6k+1)+4$, $y^2 \equiv 4 \pmod 5$.

Case 5: $y \equiv 4 \pmod 5$. Then, $\exists k \in \mathbb{Z}\ s.t.\ y = 5k+4$. Thus $y^2 = (5k+4)^2 = 25k^2+40k+16 = 5(5k^2+8k+3)+1$, $y^2 \equiv 1 \pmod 5$.

Therefore, in summary, for $y \in \mathbb{Z}$

$$y \equiv 0 \pmod 5 \Rightarrow y^2 \equiv 0 \pmod 5$$

$$y \equiv 1 \pmod 5 \Rightarrow y^2 \equiv 1 \pmod 5$$

$$y \equiv 2 \pmod 5 \Rightarrow y^2 \equiv 4 \pmod 5$$

$$y \equiv 3 \pmod 5 \Rightarrow y^2 \equiv 4 \pmod 5$$

$$y \equiv 4 \pmod 5 \Rightarrow y^2 \equiv 1 \pmod 5$$

Now, we determine the distinct equivalence classes, starting from the integer $0, 1, 2, \ldots$.

$$[0] = \{x \in \mathbb{Z} \mid x\mathcal{R}0\} = \{x \in \mathbb{Z} \mid x^2 \equiv 0^2 \equiv 0 \pmod 5\}$$

$$= \{0, \pm 5, \pm 10, \pm 15, \ldots\}$$

$$[1] = \{x \in \mathbb{Z} \mid x\mathcal{R}1\} = \{x \in \mathbb{Z} \mid x^2 \equiv 1^2 \equiv 1 \pmod 5\}$$

$$= \{\pm 1, \pm 4, \pm 6, \pm 9, \ldots\}$$

$$[2] = \{x \in \mathbb{Z} \mid x\mathcal{R}2\} = \{x \in \mathbb{Z} \mid x^2 \equiv 2^2 \equiv 4 \pmod 5\}$$

$$= \{\pm 2, \pm 3, \pm 5, \pm 7, \dots\}$$

and obviously $[0], [1], [2]$ are a partition of $\mathbb{Z}$.

Therefore, the equivalence classes of $\mathcal{R}$ are given by $[0], [1], [2]$.