$Assignment\ 4$

Haohu Shen UCID: 30063099

MATH 271 - Discrete Mathematics

Instructor Jerrod Smith

March 30, 2019

Question 1

(a) Solution

Since

$$\begin{aligned} 271 &= 98 \times 2 + 75 \\ 98 &= 75 \times 1 + 23 \\ 75 &= 23 \times 3 + 6 \\ 23 &= 6 \times 3 + 5 \\ 6 &= 5 \times 1 + 1 \\ 5 &= 1 \times 5 + 0 \end{aligned}$$

We have

$$\begin{aligned} \gcd(271, 98) &= \gcd(98, 75) \\ &= \gcd(75, 23) \\ &= \gcd(23, 6) \\ &= \gcd(6, 5) \\ &= \gcd(5, 1) \\ &= \gcd(1, 0) \\ &= 1 \end{aligned}$$

Using the table method, we have

	271	98	
271	1	0	R_1
98	0	1	R_2
75	1	-2	$R_3 \leftarrow R_1 - 2R_2$
23	-1	3	$R_4 \leftarrow R_2 - R_3$
6	4	-11	$R_5 \leftarrow R_3 - 3R_4$
5	-13	36	$R_6 \leftarrow R_4 - 3R_5$
1	17	-47	$R_7 \leftarrow R_5 - R_6$

Thus when $x = 17$ and $y = -47$,

$$\begin{aligned} 271x + 98y &= 271 \times 17 + 98 \times (-47) \\ &= 4607 - 4606 \\ &= 1 \\ &= \gcd(271, 98) \end{aligned}$$

(b) Solution From part **(a)**, we can see that -47 is an inverse of 98 modulo 271, that is

$$98 \times (-47) = 1 - 271 \times 17 = 1 + 271 \times (-17) \equiv 1 \pmod{271}$$

then 224 is another inverse of 98 modulo 271 because

$$98 \times 224 = 98 \times (-47) + 98 \times 271 \equiv 98 \times (-47) \equiv 1 \pmod{271}$$

Verification Since

$$224 \times 98 = 21952 = 81 \times 271 + 1$$

we have $271 | (98 \times 224 - 1)$, thus

$$98 \times 224 \equiv 1 \pmod{271}$$

by definition, and $0 < 224 < 271$.

(c) Solution Since $98b \equiv 99 \pmod{271}$ such that $b \in \mathbb{Z}$ and $0 < b < 271$, we can see that $271|(98b - 99)$ by the definition, thus $\exists k \in \mathbb{Z}$ such that

$$98b - 99 = 271k$$

thus

$$98b - 99 = 98b - 98 - 1 = 98(b-1) - 1 = 271k$$

thus

$$271|(98(b-1) - 1)$$

that is

$$98(b-1) \equiv 1 \pmod{271}$$

From **(b)**, we can have $b - 1 = 224$, that is $b = 225$ and $0 < b < 271$.

Verification Since

$$98 \times 225 - 99 = 21951 = 271 \times 81$$

we have $271|(98 \times 225 - 99)$, thus

$$98 \times 225 \equiv 99 \pmod{271}$$

by definition, and $0 < 225 < 271$.

Question 2

(a) Proof

- ***Reflexive***

  Suppose $X \in \mathcal{P}(S)$ is arbitrarily chosen, since $|X - T| = |X - T|$, we have $(X, X) \in \mathcal{R}$, that is $X\mathcal{R}X$, thus $\mathcal{R}$ is reflexive by the definition.

- ***Symmetric***

  Suppose $X, Y \in \mathcal{P}(S)$ is arbitrarily chosen and $(X, Y) \in \mathcal{R}$, we show that $(Y, X) \in \mathcal{R}$:
  Since $(X, Y) \in \mathcal{R}$, we have $|X - T| = |Y - T|$, thus $|Y - T| = |X - T|$. Therefore, $(Y, X) \in \mathcal{R}$,

that is $Y\mathcal{R}X$, thus $\mathcal{R}$ is symmetric by the definition.

- ***Transitive***

  Suppose $X, Y, Z \in \mathcal{P}(S)$ is arbitrarily chosen and $(X, Y) \in \mathcal{R}$, $(Y, Z) \in \mathcal{R}$, we show that $(X, Z) \in \mathcal{R}$:
  Since $(X, Y) \in \mathcal{R}$, $|X - T| = |Y - T|$; since $(Y, Z) \in \mathcal{R}$, $|Y - T| = |Z - T|$. Thus $|X - T| = |Y - T| = |Z - T|$, therefore, $(X, Z) \in \mathcal{R}$, that is $X\mathcal{R}Z$, thus $\mathcal{R}$ is transitive by the definition.

Since $\mathcal{R}$ is reflexive, symmetric and transitive, $\mathcal{R}$ is an equivalence relation.

(b) Solution 6 equivalence classes.

Explain

Since $X - T = \{x \in X \text{ and } x \notin T\}$, the possible situations of $|X - T|$ are list below:

Let $A = S - T = \{x \in S \text{ and } x \notin T\} = \{1, 3, 5, 7, 9\}$, then

- When X does not choose any element from A,

$$|X - T| = 0$$

- When X chooses exactly 1 element from A,

$$|X - T| = 1$$

- When X chooses exactly 2 elements from A,

$$|X - T| = 2$$

- When X chooses exactly 3 elements from A,

$$|X - T| = 3$$

- When X chooses exactly 4 elements from A,

$$|X - T| = 4$$

- When X chooses all 5 elements from A,

$$|X - T| = 5$$

Thus, $\mathcal{R}$ has totally 6 equivalence classes.

(c) Solution 16 elements.

Explain

$$
\begin{aligned}
[\varnothing] &= \{X \in \mathcal{P}(S) \mid (X, \varnothing) \in \mathcal{R}\} \\
&= \{X \in \mathcal{P}(S) \mid |X - T| = |\varnothing - T|\}
\end{aligned}
$$

Since $\varnothing - T = \varnothing$, we have

$$|X - T| = |\varnothing - T| = |\varnothing| = 0$$

thus $X - T = \varnothing$, that is $X \subseteq T$, thus X is a subset of T. Therefore

$$|[\varnothing]| = |\mathcal{P}(T)| = 2^4 = 16$$

(d) Solution 160 elements.

Explain

$$
\begin{aligned}
[\{1,2,3,4\}] &= \{X \in \mathcal{P}(S) \mid (X, \{1,2,3,4\}) \in \mathcal{R}\} \\
&= \{X \in \mathcal{P}(S) \mid |X - T| = |\{1,2,3,4\} - T|\}
\end{aligned}
$$

Notice that

$$|X - T| = |\{1,2,3,4\} - T| = |\{1,2,3,4\} - \{2,4,6,8\}| = |\{1,3\}| = 2$$

Thus here is a recipe to make X:

- Step 1: X must choose two elements from $\{1,3,5,7,9\}$, that is $\binom{5}{2} = 10$ ways.
- Step 2: X could choose or not choose each element in $\{2,4,6,8\}$, that is $2^4 = 16$ ways.

Therefore, there are totally $10 \times 16 = 160$ ways to make X, thus

$$[\{1,2,3,4\}] = 160$$

Question 3

(a)

- The statement is false.
- Its negation is: $\exists$ function $f : A \to A$ and $\exists$ relation $\mathcal{R}$ on A such that S is reflexive but R is not reflexive. We show its negation is true.
- **Proof** (of negation)

  Let $f : A \to A$ defined by

$$f(1) = 4, f(2) = 4, f(3) = 4, f(4) = 4$$

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

Then

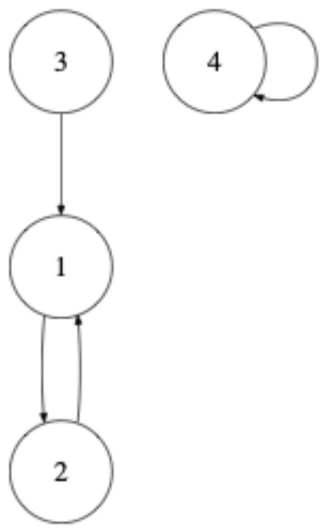
$$(f(1), f(1)) = (4,4) \in \mathcal{R}$$

$$(f(2), f(2)) = (4,4) \in \mathcal{R}$$

$$(f(3), f(3)) = (4,4) \in \mathcal{R}$$

$$(f(4), f(4)) = (4,4) \in \mathcal{R}$$

Thus, $\forall x \in A$, $(f(x), f(x)) \in \mathcal{R}$, that is $x\mathcal{R}x$, therefore S is reflexive. But $3 \in A$ and $(3,3) \notin \mathcal{R}$, that is, $3 \not\mathcal{R}\, 3$, thus $\mathcal{R}$ is not reflexive. The directed graph of $\mathcal{R}$ is shown below:



(b)

- The statement is true.
- **Proof** Suppose $\mathcal{R}$ is reflexive and $a \in A$ such that a is arbitrarily chosen. Since $f : A \to A$, $f(a) \in A$, thus $f(a)\mathcal{R}f(a)$, that is $(f(a), f(a)) \in \mathcal{R}$, thus aSa. Therefore, S is reflexive by the definition.

(c)

- The statement is false.
- Its negation is: $\exists$ function $f : A \to A$ and relation $\mathcal{R}$ on A such that S is symmetric but $\mathcal{R}$ is not symmetric. We show its negation is true.
- **Proof** (of negation)

Let $f : A \to A$ defined by

$$f(1) = 4, f(2) = 4, f(3) = 4, f(4) = 4$$

that is

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

Let $\mathcal{R} = \{(4,4), (3,1)\}$ on A. Since $\forall x, y \in A$, $f(x) = f(y) = 4$, thus $(f(x), f(y)) = (4,4) \in \mathcal{R}$ and $(f(y), f(x)) = (4,4) \in \mathcal{R}$, that is, S is symmetric. But $3 \in A$, $1 \in A$, $3\mathcal{R}1$ and $1 \not\mathcal{R}\, 3$, because $(3,1) \in \mathcal{R}$ but $(1,3) \notin \mathcal{R}$. Therefore, $\mathcal{R}$ is not symmetric.

(d)

- The statement is true.
- **Proof** Suppose $a, b \in A$ are arbitrarily chosen and $\mathcal{R}$ is symmetric and aSb, we prove that S is symmetric by showing bSa:

  Since aSb, we have $(f(a), f(b)) \in \mathcal{R}$. Because $f : A \to A$, we have $f(a) \in A$, $f(b) \in A$. Since $\mathcal{R}$ is symmetric on A, $(f(b), f(a)) \in \mathcal{R}$, thus we have bSa. Therefore, S is symmetric by the definition.