Problem 1. (Image of Intersection)
Let $f : X \to Y$ and let $A, B \subset X$.

(a) Show that $f(A \cap B) \subset f(A) \cap f(B)$.

(b) Give an example where $f(A \cap B) \neq f(A) \cap f(B)$.

Solution. We show that $f(A \cap B) \subset f(A) \cap f(B)$.

Let $y \in f(A \cap B)$. Then there exists $x \in A \cap B$ such that $y = f(x)$. Now $x \in A$ and $x \in B$, so $y = f(x) \in f(A)$ and $y = f(x) \in f(B)$. Therefore $y \in f(A) \cap f(B)$.

However, the reverse inclusion is false. For example, let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = x^2$, let $A = \{0, 1\}$, and let $B = \{0, -1\}$. In this case, $f(A \cap B) = f(\{0\}) = \{0\}$, but $f(A) \cap f(B) = \{0, 1\} \cap \{0, 1\} = \{0, 1\}$. So $f(A \cap B) \neq f(A) \cap f(B)$. □

Definition 1. Let $\mathcal{C}$ and $\mathcal{D}$ be partitions of a set X. A *congruence* from $\mathcal{C}$ to $\mathcal{D}$ is a bijective function $\alpha : X \to X$ such that $\mathcal{D} = \{\alpha(C) \mid C \in \mathcal{C}\}$.

We say that $\mathcal{C}$ and $\mathcal{D}$ are *congruent* if there exists a congruence between them.

Problem 2. (Congruent Partitions)
Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Consider the partitions

- $\mathcal{A} = \{\{1\}, \{2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}\}$
- $\mathcal{B} = \{\{1\}, \{2\}, \{3, 4\}, \{5, 6\}, \{7, 8, 9\}\}$
- $\mathcal{C} = \{\{1\}, \{2, 3\}, \{4, 5\}, \{6, 7\}, \{8, 9\}\}$

Each of the following partitions $\mathcal{D}$, is congruent to either $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$. State which of the above is congruent to $\mathcal{D}$, and find a bijection $\alpha \in S_9$ which maps $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$ to $\mathcal{D}$.

Solution. We use array notation and cycle notation for permutations.

(a) $\mathcal{D} = \{\{1, 2\}, \{3, 4\}, \{5\}, \{6, 7, 8\}, \{9\}\}$
This is congruent to $\mathcal{B}$. We define a function which sends $\mathcal{B}$ to $\mathcal{D}$ as follows:

$$\alpha : X \to X \quad \text{given by} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 1 & 2 & 3 & 4 & 6 & 7 & 8 \end{pmatrix} = \texttt{(1 5 3)(2 9 8 7 6 4)}.$$

(b) $\mathcal{D} = \{\{1, 5, 6\}, \{2\}, \{3, 8\}, \{4\}, \{7, 9\}\}$ This is congruent to $\mathcal{B}$ via

$$\alpha : X \to X \quad \text{given by} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 3 & 8 & 7 & 9 & 1 & 5 & 6 \end{pmatrix} = \texttt{(1 2 4 8 5 7)(6 9)}.$$

(c) $\mathcal{D} = \{\{1, 9\}, \{2, 4\}, \{3, 5\}, \{6, 8\}, \{7\}\}$ This is congruent to $\mathcal{C}$ via

$$\alpha : X \to X \quad \text{given by} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 9 & 2 & 4 & 3 & 5 & 6 & 8 \end{pmatrix} = \texttt{(1 7 5 3 2)(3 9 8 6)}.$$

□

Problem 3. (Permutations)
Let $\alpha \in S_n$. Recall that the order of α is the least common multiple of the lengths of its disjoint cycles. Recall also that the *shape* of α is the sorted list of the lengths of its disjoint cycles.

(a) Find all possible shapes of elements in S_4, and how many of each shape exists.

(b) Find all possible shapes of elements in S_6, and find the order of an element of each shape.

(c) Let $\alpha =$ `(1 3 5 7)(2 4 6)` and $\beta =$ `(1 2 3 4 5)`. Compute $\beta\alpha\beta^{-1}$.

(d) Find $\beta \in S_9$ such that β`(1 5 3 2)` $=$ `(4 9 7 6)`β.

Solution. **(a)** The shapes of S_4. There are $4! = 24$ total elements in S_4.

- `[1]` 1 This is the identity only.
- `[2]` 6 There are $\binom{4}{2} = 6$ two-cycles.
- `[3]` 8 There are $\binom{4}{3} = 4$ orbits of three elements, each with two possible cycles.
- `[4]` 6 There is one set of four elements, and $3! = 6$ ways of arranging them into cycles.
- `[2,2]` 3 There are $24 - (1 + 6 + 8 + 6) = 3$ remaining elements in S_4.

(b) We list the shapes of S_6 and there lcm's.

- `[1]` 1
- `[2]` 2
- `[3]` 3
- `[4]` 4
- `[5]` 5
- `[6]` 6
- `[2,2]` 2
- `[2,2,2]` 2
- `[2,3]` 6
- `[2,4]` 4
- `[3,3]` 3

(c) $\beta\alpha\beta^{-1} =$ `(1 2 3 4 5)(1 3 5 7)(2 4 6)(1 5 4 3 2)` $=$ `(1 7 2 4)(3 5 6)`. Notice that conjugating by β has the effect of replacing each x in the support of α with $\beta(x)$.

(d) We need a permutation which sends `(1 5 3 2)` to `(4 9 7 6)`. There are many possibilities, such as

$\beta =$ `(1 4 5 9 3 7 2 6)` or $\beta =$ `(1 4)(5 9)(3 7)(2 6)`.

□

Problem 4. (Modular Integers)
Let $n \geq 2$. Let $\mathbb{Z}_n$ denote the set of congruence classes modulo n. Define $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. We know the $\mathbb{Z}_n^*$ consists of the elements in $\mathbb{Z}_n$ which are invertible.

(a) Find the (additive) order of $\overline{10}$ in $\mathbb{Z}_{35}$.

(b) Find the (multiplicative) order of $\overline{7}$ in $\mathbb{Z}_{20}$.

(c) Find the cardinality of $\mathbb{Z}_{50}^*$.

(d) Circle all of the groups below which are cyclic.

$$\mathbb{Z}_8^* \qquad \mathbb{Z}_9^* \qquad \mathbb{Z}_{10}^* \qquad \mathbb{Z}_{11}^* \qquad \mathbb{Z}_{12}^* \qquad \mathbb{Z}_{14}^*.$$

Solution. We point out that since $\mathbb{Z}_n$ is a group under addition and not multiplication, the order of an element in this group is additive order. Similarly, $\mathbb{Z}_n^*$ is a group under multiplication and not addition, so the the order of an element in this group is its multiplicative order.

(a) Find the (additive) order of $\overline{10}$ in $\mathbb{Z}_{35}$.
The order is $\dfrac{n}{\gcd(a,n)} = \dfrac{35}{\gcd(35,10)} = \dfrac{35}{5} = 7$.

(b) Find the (multiplicative) order of $\overline{7}$ in $\mathbb{Z}_{20}$.
Here we compute $\overline{7}^2 = \overline{49} = \overline{9} = \overline{-1}$, so $\overline{7}^4 = \overline{-1}^2 = \overline{1}$. Thus the order is 4.

(c) Find the cardinality of $\mathbb{Z}_{50}^*$.
We remove from the set of positive integer less than 50 all multiples of 2 and of 5. If $0 \leq a < 50$ and $\overline{a} \in \mathbb{Z}_{50}$, then a mod 10 is 1, 3, 7, and 9, and a div 10 is 0 through 4. So, there are $4 \times 5 = 20$ elements in $\mathbb{Z}_{50}$.

(d) Find the groups which are cyclic. We do this by attempting to find and element of order $\phi(n)$ in $\mathbb{Z}_n^*$. We will write without bars.

- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. Now $3^2 = 9 = 1$, $5^2 = 25 = 1$, $7^2 = 49 = 1$. There is no element of order 4, so this group is not cyclic.
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$. We have $2^3 = 8 = -1$, so $2^6 = 1$. Thus 2 is an element of order 6, and $\mathbb{Z}_9^* = \langle 2 \rangle$ is cyclic.
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. Here $3^2 = -1$, so $\text{ord}(3) = 4$, so $\mathbb{Z}_{10}^* = \langle 3 \rangle$ is cyclic.
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. All elements have order two, so this group is not cyclic.
- $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$. We have $3^3 = 27 = -1$, so $\text{ord}(3) = 6$, and $\mathbb{Z}_{14}^* = \langle 3 \rangle$ is cyclic.

□

Problem 5. (Euclidean Algorithm)
Let $m = 508$ and $n = 1029$.

(a) Find $x, y \in \mathbb{Z}$ such that $mx + ny = 1$.

(b) Solve the equation $\overline{508}x + \overline{979} = \overline{0}$ in $\mathbb{Z}_{1029}$.

Solution. First we perform the Euclidean algorithm to find x and y.

$$\begin{aligned} 1029 &= 508(2) + 13 \\ 508 &= 13(39) + 1 \\ 1 &= 508 - 13(39) \\ &= 508 - [1029 - 508(2)](39) \\ &= 508(79) + 1029(-39) \end{aligned}$$

So, $x = 79$ and $y = -39$.

Next, we use what we have discovered: $\overline{79}$ is the inverse of $\overline{508}$ in $\mathbb{Z}_{1029}$. Thus

$$\overline{508}x + \overline{979} = \overline{0} \quad \Rightarrow \quad \overline{508}x = \overline{-979} = \overline{50} \quad \Rightarrow \quad x = \overline{79 \cdot 50} = \overline{863}.$$

□