CSE 20 Spring 2022
Homework 8 solutions
Due date: Thursday, June 2, 2022 at 11:59pm

In this assignment,

You will construct relations, identify properties of relations, identify if a relation is an equivalence relation and what are the equivalence classes, apply the rules of modular arithmetic to applications.

In this class, unless the instructions explicitly say otherwise, you are required to justify all your answers.

1. (24 points)

   (a) Define the relation $\mathbf{L} \subseteq \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$ given by the following rule:
   $\forall S \in \mathcal{P}(\mathbb{N})((\emptyset, S) \in \mathbf{L})$
   and if $A \neq \emptyset$ and $B \neq \emptyset$ then $(A, B) \in \mathbf{L}$ iff $\min(A) \leq \min(B)$.

      i. Prove or disprove that $\mathbf{L}$ is reflexive.

         Solution: True:
         $(\emptyset, \emptyset) \in \mathbf{L}$.
         Let S be an arbitrary element of $\mathcal{P}(\mathbb{N})$ and assume $S \neq \emptyset$. Then $min(S) \leq min(S)$ so $(S, S) \in \mathbf{L}$.

      ii. Prove or disprove that $\mathbf{L}$ is symmetric.

         Solution: False:
         $(\{1\}, \{2\}) \in \mathbf{L}$ and $(\{2\}, \{1\}) \notin \mathbf{L}$.

      iii. Prove or disprove that $\mathbf{L}$ is transitive.

         Solution: True.
         Let S, T, U be arbitrary non-empty elements of $\mathcal{P}(\mathbb{N})$.
         Suppose that (S, T) and (T, U) are in $\mathbf{L}$. Then $min(S) \leq min(T)$ and $min(T) \leq min(U)$. Therefore $min(S) \leq min(U)$ so $(S, U) \in \mathbf{L}$.
         Suppose that S is empty, then since the emptyset relates to all other elements, then if (T, U) then $(\emptyset, T) \in \mathbf{L}$, $(T, U) \in \mathbf{L}$ and $(\emptyset, U) \in \mathbf{L}$.

      iv. Prove or disprove that $\mathbf{L}$ is antisymmetric.

         Solution: False.
         $(\{1, 2\}, \{1, 3\}) \in \mathbf{L}$ and $(\{1, 3\}, \{1, 2\}) \in \mathbf{L}$ but $\{1, 2\} \neq \{1, 3\}$

   (b) Define the relation $\mathbf{B} \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ given by the following rule:
   $((w, x), (y, z)) \in \mathbf{B}$ iff $(w = y) \vee (x = z)$.

      i. Prove or disprove that $\mathbf{B}$ is reflexive.

         Solution: True.
         Let (a, b) be an arbitrary element of $\mathbb{N} \times \mathbb{N}$. Then $a = a$ so $((a, b), (a, b)) \in \mathbf{B}$.

      ii. Prove or disprove that $\mathbf{B}$ is symmetric.

         Solution: True.
         Let (a, b) and (c, d) be arbitrary elements of $\mathbb{N} \times \mathbb{N}$ and assume that $((a, b), (c, d)) \in \mathbf{B}$. Then $a = c$ or $b = d$. If $a = c$ then $c = a$ so $((c, d), (a, b)) \in \mathbf{B}$ and if $b = d$ then $d = b$ so $((c, d), (a, b)) \in \mathbf{B}$.

      iii. Prove or disprove that $\mathbf{B}$ is transitive.

         Solution:
         False.
         $((1, 2), (1, 3)) \in \mathbf{B}$ and $((1, 3), (2, 3)) \in \mathbf{B}$ but $((1, 2), (2, 3)) \notin \mathbf{B}$.

      iv. Prove or disprove that $\mathbf{B}$ is antisymmetric.

         Solution:
         False.
         $((1, 2), (1, 3)) \in \mathbf{B}$ and $((1, 3), (1, 2)) \in \mathbf{B}$ but $(1, 2) \neq (1, 3)$.

(c) Define the relation $\mathbf{W} \subseteq (\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})) \times (\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}))$ given by the following rule: $((A, B), (C, D)) \in \mathbf{W}$ iff $A \cap B = C \cap D$.

i. Prove or disprove that $\mathbf{W}$ is reflexive.

Solution:
True. Let (A, B) be an arbitrary element of $\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$.
Then $A \cap B = A \cap B$ so $((A, B), (A, B)) \in \mathbf{W}$.

ii. Prove or disprove that $\mathbf{W}$ is symmetric.

Solution:
True. Let (A, B) and (C, D) be arbitrary elements of $\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$. Assume that $((A, B), (C, D)) \in \mathbf{W}$. Then $A \cap B = C \cap D$, so $C \cap D = A \cap B$ therefore $((C, D), (A, B)) \in \mathbf{W}$.

iii. Prove or disprove that $\mathbf{W}$ is transitive.

Solution:
True. Let $(A, B), (C, D), (E, F)$ be arbitrary elements of $\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$. Assume that $((A, B), (C, D)) \in \mathbf{W}$ and $((C, D), (E, F)) \in \mathbf{W}$. Then $A \cap B = C \cap D$ and $C \cap D = E \cap F$. Therefore $A \cap B = E \cap F$, so $((A, B), (E, F)) \in \mathbf{W}$.

iv. Prove or disprove that $\mathbf{W}$ is antisymmetric.

Solution: False.
$((\{1, 2\}, \{1, 3\}), (\{1, 3\}, \{1, 2\})) \in \mathbf{W}$ and $((\{1, 3\}, \{1, 2\}), (\{1, 2\}, \{1, 3\})) \in \mathbf{W}$ but $(\{1, 2\}, \{1, 3\}) \neq (\{1, 3\}, \{1, 2\})$

2. (20 points) For each pair of sets, determine whether they are **disjoint, equal, proper subset** or **none of the above.** Give a justification for each answer.

- In order to justify that A and B are equal, you will need to show that any arbitrary element of A is in B and any arbitrary element of B is in A.
- In order to justify that A is a proper subset of B, you will need to show that any arbitrary element of A is in B and there exists an element in B that is not in A.
- In order to justify that A and B are disjoint then you will need to show that any arbitrary element of A is not in B (or vice versa)
- In order to justify **none of the above** then you will need to show that there exists an element that is in both sets A and B and that there exists an element of A that is not in B and there exists an element in B that is not in A.

Recall that $[a]_m = \{x \in \mathbb{Z} \mid a \textbf{ mod } m = x \textbf{ mod } m\}$.

(a) $A = [2]_4$ and $B = [6]_8$

Solution:
$B \subseteq A$.
Let x be an arbitrary element of B. Then $x = 8k + 6$ for some integer k. Then $x = 4(2k + 1) + 2$. Therefore $x \in [2]_4$.
$2 \in A$ and $2 \notin B$.

(b) $A = [4]_{10}$ and $B = [2]_4$

Solution:
none of the above.
$4 \in A$ and $4 \notin B$
$2 \notin A$ and $2 \in B$
$14 \in A$ and $14 \in B$.

(c) $A = [3]_9$ and $B = [6]_9$

Solution:
Disjoint
Assume by way of contradiction that there exists an element x in the intersection of A and B. Then $x = 9k + 3$ and $x = 9m + 6$ for integers k, m.
Then $9k + 3 = 9m + 6$.

$$9k + 3 = 9m + 6$$
$$9(k - m) = 3$$
$$(k - m) = 3/9$$

the left side $(k - m)$ is an integer and the right side $3/9$ is not an integer which is a contradiction. Therefore the assumption is false which means that the original claim is true.

(d) $A = [2]_5 \cap [2]_4$ and $B = [2]_{20}$

Solution:
Equal
Let $x \in A$. Then $x = 5k + 2$ and $x = 4m + 2$ for integers k, m. Then

$$5k + 2 = 4m + 2$$
$$5k = 4m$$

Since 5 and 4 do not share any common factors, then k must be a multiple of 4 and so $k = 4n$ for some integer n.
Therefore $x = 5(4n) + 2$ so $x \in [2]_{20}$.
Let $x \in B$. then $x = 20k + 2$ for some integer k. Then $x = 4(5k) + 2$ so $x \in [2]_4$ and $x = 5(4k) + 2$ so $x \in [2]_5$. Therefore $x \in [2]_5 \cap [2]_4$.

3. (a) (2 points) Use the regular Euclidean algorithm to show that $\gcd(3021, 131) = 1$. (Show your work as a table)

Solution:

r	x	y
	3021	131
8	131	8
3	8	3
2	3	2
1	2	1
0	1	0

(b) (4 points) Use the modified Euclidean algorithm to find the (mod 3021)-multiplicative inverse of 131. (Show your work as a table)

k	q_k	r_k	p_k
0		3021	0
1		131	1
2	23	8	23
3	16	3	369
4	2	2	761
5	1	1	1130
6	2	0	3021

Therefore the (mod 3021)-multiplicative inverse of 131 is $(-1)^6 * 1130 = 1130$.

$$(131)(1130) = (49)(3021) + 1$$

4. *Read the introduction to cryptographic protocols on page 302 of the textbook.*

Cryptography is the process of hiding a message by encoding it in a reverseable (decodable) way. Many cryptographic schemes rely on modular arithmetic. Often, the two parties who want to communicate in secret need to share a common piece of information, called a key. Since messages are often encoded as numbers, the key is typically an integer. The Diffie-Hellman algorithm lets Alice and Bob agree on a shared secret number, without each one revealing their own secret to the other. Here is the algorithm:

- Alice and Bob agree (in public) to use a prime p and an integer a with $0 \leq a < p$.
  The numbers p and a are not secret.
- Alice chooses a secret integer k_1 and sends $y_a = a^{k_1} \mod p$ to Bob.
- Bob chooses a secret integer k_2 and sends $y_b = a^{k_2} \mod p$ to Alice.
- Alice computes $s_a = (y_b)^{k_1} \mod p$.
- Bob computes $s_b = (y_a)^{k_2} \mod p$.

(a) (4 points) Describe each step (write out the results of all computations) that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key, using the prime $p = 19$ and $a = 10$. Assume that Alice selects $k_1 = 12$ and Bob selects $k_2 = 3$. *You may use a calculator, MATLAB, Wolfram Alpha, etc. so long as you include the results of intermediate calculations.*

Solution:

- Alice computes 10^{12} **mod** $19 = 7$
- Bob computes 10^3 **mod** $19 = 12$
- Alice shares 7 and Bob shares 12.
- Alice computes 12^{12} **mod** $19 = 1$
- Bob computes 7^3 **mod** $19 = 1$
- Bob and Alice share 1 as the secret key.

(b) (2 points) Given that $(x^y \textbf{ mod } z)^n \textbf{ mod } z = x^{yn} \textbf{ mod } z$, Explain why in the Diffie-Hellman protocol, s_a will always equal s_b. *This value is Alice's and Bob's "shared secret number", which they can use as a key for further cryptography.*

Solution:
The reason that the shared secret number is the same is because Alice computes: $(a^{k_2} \mod p)^{k_1} = a^{k_2 k_1} \mod p$ and Bob computes: $(a^{k_1} \mod p)^{k_2} = a^{k_1 k_2} \mod p$.
And these are the same number because $a^{k_2 k_1} = a^{k_1 k_2}$ by the commutative property of multiplication.

(c) (5 points) Bob and Alice want to do the Diffie-Hellman key exchange again with the same p and a but they will choose different secret numbers from part (a). Alice chooses the secret integer ℓ_1 and Bob chooses the secret integer ℓ_2. Let's say that Charlie is listening in on the conversation of Bob and Alice. So Charlie knows that $p = 19$, $a = 10$, and a^{ℓ_1} **mod** $19 = 4$ and a^{ℓ_2} **mod** $19 = 3$. Charlie wants to know ℓ_1 and ℓ_2. Help Charlie figure out ℓ_1 and ℓ_2 by creating a table with results for each power of 10 from 0 to 18:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
10^n **mod** 19	1	10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1

(d) (2 points) What is Alice and Bob's *shared key* for part (c)?

Solution:
Alice's secret integer is 16 (according to the table) and Bob's secret integer is 5 (according to the table)
So Alice computes 3^16 **mod** $19 = 17$ and Bob computes 4^5 **mod** $19 = 17$ so their shared number is 17.

(e) (for fair effort completeness) Explain why this table is enough for Charlie to intercept Alice and Bob's secret integers whenever they use $p = 19$ and $a = 10$.

[This particular problem is called the *Discrete Log Problem* because essentially you are trying to solve for the exponent of the equation a^x **mod** $p = y$ when you know a, p and y. This is extremely difficult if p is large (like when $p > 2^{100}$). This is the reason that Diffie Hellman is so secure when you use a large value for p.]

Solution:
The table essentially gives you a way to reverse-engineer Alice and Bob's secret number for any secret numbers they choose when $p = 19$ and $a = 10$. Then with the secret numbers, you can act as either Alice or Bob to figure out the secret key.
This was easy enough to do for $p = 19$ but if p is much larger, this table would be too big to compute and so this method (although still technically viable) would not be feasible (would take too many resources.)