MATH 108 Winter 2019 - **Problem Set 4 solutions**

due February 8

1. Nim is a two-player game involving piles of coins. The players alternate taking turns, and on each turn the player chooses a nonempty pile and chooses a positive number of coins to remove from that pile. This continues until there are no coins left. In this version of Nim, at the start of the game there are two piles, each with n coins. Whoever takes the last coin loses. Prove by induction that for all $n \geq 2$, the second player has a winning strategy, i.e. they can always win no matter what the first player does.

   We proceed by strong induction. Assume for some $n \geq 2$ that player 2 has a winning strategy when the two piles start with k coins for all $2 \leq k < n$.

   Let the starting number of coins in each pile be n. Player 1 must remove m coins for some $0 < m \leq n$ from one of the piles. Call the pile that player 1 chooses pile 1, and the other pile 2. If $m = n$, then pile 1 is empty. Player 2 should remove $n - 1$ coins from pile 2, leaving only one coin. Now player 1 must remove the last coin, and loses. If $m = n-1$, then player 2 should remove all n coins from pile 2, leaving only one coin. Then player 1 loses. If $m < n-1$, then player 2 should remove m coins from pile 2. Now both piles have $n - m$ coins with $n - m \geq 2$ and it is player 1's turn again. By the induction hypothesis, player 2 has a winning strategy from this position. Therefore player 2 can always win, no matter what player 1 does.

2. For positive integers a and b, the *greatest common divisor* of a and b is the largest postive integer that divides both a and b, denoted $\gcd(a, b)$. For p a prime number, prove that p divides a and p divides b if and only if p divides $\gcd(a, b)$.

   Suppose p divides $\gcd(a, b)$. Since $\gcd(a, b)$ divides a and b, and divisibility is transitive, p divides a and b.

   Suppose p divides a and b. We argue by contradiction, so assume that p does not divide $d = \gcd(a, b)$. Since d divides a, $a = dx$ for some integer x. By Euclid's Lemma, p either divides d or x, so it must divide x. Therefore $x = py$ for integer y. Similarly $b = dz$ for some integer z and then p divides z so $z = pw$. Then $a = dpy$ and $b = dpw$ so dp divides both a and b. This is a contradiction because $dp > d$ but d is the greatest common divisor of a and b. Therefore p divides d.

   Alternative proof: Suppose p divides a and b. By the result of Problem 3, $\gcd(a, b) = as + bt$ for some $s, t \in \mathbb{Z}$. Since both as and bt are divisible by p, $\gcd(a, b)$ is also divisible by p.

3. For positive integers a and b with $\gcd(a, b) = d$, prove that

$$\{as + bt \mid s, t \in \mathbb{Z}\} = d\mathbb{Z}.$$

   Let $S = \{as + bt \mid s, t \in \mathbb{Z}\}$. Since d divides a and b, we have $a = dx$ and $b = dy$ for integers x and y. If x and y have a common factor c, then dc would be a common factor

of a and b which contradicts the fact that d is their greatest common factor. Therefore x and y have no common factor. By Bézout's Identity, there exist integers u and v such that $xu + yv = 1$. For any $n \in \mathbb{Z}$,

$$xnu + ynv = n$$

so

$$anu + bnv = dxnu + dynv = dn.$$

Therefore $dn \in S$. This proves that $d\mathbb{Z} \subseteq S$. Now suppose that $n \in S$, so

$$as + bt = n$$

for some integers s and t. Then $n = dxs + dyt$, so n is divisible by d. Therefore $S \subseteq d\mathbb{Z}$.

4. For each relation, list which of the following properties it has: symmetric, antisymmetric, transitive, reflexive, irreflexive.

   (a) $\leq$ on $\mathbb{Z}$.
   Antisymmetric, transitive, reflexive.

   (b) $\neq$ on $\mathbb{Z}$.
   Symmetric, irreflexive.

   (c) $\subseteq$ on $\mathcal{P}(\mathbb{Z})$.
   Antisymmetric, transitive, reflexive.

   (d) "is the child of" on people.
   Antisymmetric, irreflexive.

   (e) $\{(1,5),(5,1),(1,1)\}$ on $A = \{1,2,3,4,5\}$.
   Symmetric.

   (f) $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x + y = 10\}$ on $\mathbb{Z}$.
   Symmetric.

5. Let $A = \{1,2,3,4,5\}$ and let $\sim$ be the relation on $\mathcal{P}(A)$ defined by $S \sim T$ if $|S| = |T|$. Prove that $\sim$ is an equivalence relation. How many equivalence classes does $\sim$ have and how big is each class?

   To show that $\sim$ is an equivalence relation, we must prove it is reflexive, symmetric and transitive. For any $S \in \mathcal{P}(A)$, $|S| = |S|$ so $\sim$ is reflexive. For any $S, T \in \mathcal{P}(A)$, if $|S| = |T|$ then $|T| = |S|$ so $\sim$ is symmetric. For any $S, T, U \in \mathcal{P}(A)$, if $|S| = |T|$ and $|T| = |U|$ then $|S| = |U|$ so $\sim$ is transitive. Therefore $\sim$ is an equivalence relation.

   There are 6 equivalence classes of $\sim$, which are the sets of size $0, 1, 2, 3, 4, 5$. The sizes of the equivalence classes are $1, 5, 10, 10, 5, 1$ respectively.

6. Let R and S be relations on A. The *composition* of R and S, denoted $R \circ S$, is defined as

$$R \circ S = \{(x,z) \in A \times A \mid \exists y \in A \text{ with } x\, R\, y \text{ and } y\, S\, z\}.$$

(a) Find a counterexample to the following statement: If R and S are symmetric, then $R \circ S = S \circ R$.

A counterexample is $A = \{1, 2, 3\}$ wtih symmetric relations $R = \{(1, 2), (2, 1)\}$ and $S = \{(2, 3), (3, 2)\}$. Then $(1, 3) \in R \circ S$ but $(1, 3) \notin S \circ R$.

(b) Prove that R is transitive if and only if $R \circ R \subseteq R$.

Suppose R is transitive. For any $(x, z) \in R \circ R$, there exists $y \in A$ such that $x \, R \, y$ and $y \, R \, z$. By transitivity, $x \, R \, z$, meaning $(x, z) \in R$.

Suppose that $R \circ R \subseteq R$. For any x, y, z with $x \, R \, y$ and $y \, R \, z$, by definition $(x, z) \in R \circ R$. Since $R \circ R \subseteq R$, we have $x \, R \, z$, so R is transitive.

7. Find an equivalence relation on $\mathbb{N}_1$ with set of equivalence classes equal to each partition.

(a) $\{\{1, 4, 7, \ldots\}, \{2, 5, 8, \ldots, \}, \{3, 6, 9, \ldots\}\}$.
Define $\sim$ by $x \sim y$ iff $x - y$ is divisible by 3.

$$\sim = \{(x, y) \in \mathbb{N}_1^2 \mid x - y \in 3\mathbb{Z}\}.$$

(b) $\{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \ldots\}$.
Define $\sim$ by $x \sim y$ iff $\lceil x/2 \rceil = \lceil y/2 \rceil$.

$$\sim = \{(x, y) \in \mathbb{N}_1^2 \mid \lceil x/2 \rceil = \lceil y/2 \rceil\}.$$

(c) $\{\{1\}, \{2, 3\}, \{4, 5, 6, 7\}, \{8, \ldots, 15\}, \{16, \ldots, 31\}, \ldots\}$.
Define $\sim$ by $x \sim y$ iff $\lfloor \log_2(x) \rfloor = \lfloor \log_2(y) \rfloor$.

$$\sim = \{(x, y) \in \mathbb{N}_1^2 \mid \lfloor \log_2(x) \rfloor = \lfloor \log_2(y) \rfloor\}.$$

(d) $\{\mathbb{N}_1\}$.
Define $\sim$ by $x \sim y$ for all $x, y \in \mathbb{N}_1$.

$$\sim = \mathbb{N}_1^2.$$