MATH 108 Winter 2019 - **Problem Set 5 solutions**

due February 22

1. Using modular arithmetic, prove that for all postive integers n,

   (a) $10^n - 1$ is divisible by 3.
   Since $10 \equiv 1 \pmod 3$, then

   $$10^n - 1 \equiv 1^n - 1 \equiv 0 \pmod 3$$

   for all positive integers n.

   (b) $n^4 + 2n^3 - n^2 - 2n$ is divisible by 4.
   There are four cases, depending on the equivalence class of n.
   If $n \equiv 1 \pmod 4$ then

   $$n^4 + 2n^3 - n^2 - 2n \equiv 1^4 + 2 \cdot 1^3 - 1^2 - 2 \cdot 1 \equiv 0 \pmod 4.$$

   If $n \equiv 2 \pmod 4$ then

   $$n^4 + 2n^3 - n^2 - 2n \equiv 2^4 + 2 \cdot 2^3 - 2^2 - 2 \cdot 2 \equiv 24 \equiv 0 \pmod 4.$$

   If $n \equiv 3 \pmod 4$ then

   $$n^4 + 2n^3 - n^2 - 2n \equiv 3^4 + 2 \cdot 3^3 - 3^2 - 2 \cdot 3 \equiv 120 \equiv 0 \pmod 4.$$

   If $n \equiv 0 \pmod 4$ then

   $$n^4 + 2n^3 - n^2 - 2n \equiv 0^4 + 2 \cdot 0^3 - 0^2 - 2 \cdot 0 \equiv 0 \pmod 4.$$

   (c) $1^n + 2^n + 3^n + 4^n$ is a multiple of 5 or one less than a multiple of 5.
   We proceed by induction on n, with base cases $1, 2, 3, 4$. For $n = 1$, we have

   $$1^1 + 2^1 + 3^1 + 4^1 \equiv 10 \equiv 0 \pmod 5.$$

   For $n = 2$, we have

   $$1^2 + 2^2 + 3^2 + 4^2 \equiv 30 \equiv 0 \pmod 5.$$

   For $n = 3$, we have

   $$1^3 + 2^3 + 3^3 + 4^3 \equiv 100 \equiv 0 \pmod 5.$$

   For $n = 4$, we have

   $$1^4 + 2^4 + 3^4 + 4^4 \equiv 354 \equiv 4 \pmod 5.$$

For $n > 4$, assume that $1^{n-4} + 2^{n-4} + 3^{n-4} + 4^{n-4}$ is a multiple of 5 or one less than a multiple of 5. Note that

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod 5.$$

Therefore,

$$1^n + 2^n + 3^n + 4^n \equiv 1^4 \cdot 1^{n-4} + 2^4 \cdot 2^{n-4} + 3^4 \cdot 3^{n-4} + 4^4 \cdot 4^{n-4}$$

$$\equiv 1^{n-4} + 2^{n-4} + 3^{n-4} + 4^{n-4} \pmod 5.$$

So $1^n + 2^n + 3^n + 4^n$ is also a multiple of 5 or one less than a multiple of 5.

2. The "Cancellation Law" for $\mathbb{Z}/m\mathbb{Z}$ is the statement: For all $x, y, z \in \mathbb{Z}$, if $xy \equiv xz \pmod m$ and $x \not\equiv 0 \pmod m$ then $y \equiv z \pmod m$.

   (a) Prove that if m is prime then the Cancellation Law for $\mathbb{Z}/m\mathbb{Z}$ is true.

   Suppose that m is prime, that $xy \equiv xz \pmod m$ and that $x \not\equiv 0 \pmod m$. Then $x(y - z)$ is divisible by m and x is not divisible by m. Since m is prime, by Euclid's Lemma $y - z$ must be divisible by m. Therefore $y \equiv z \pmod m$.

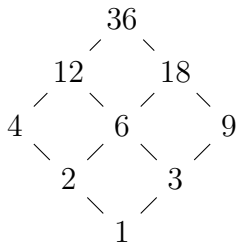
   (b) Prove that if m is composite then the Cancellation Law for $\mathbb{Z}/m\mathbb{Z}$ is false.

   Supposing m is composite, we produce a counterexample to the Cancellation Law. Since m is composite, $m = xy$ for some x and y that are both not divisible by m. So $xy \equiv 0 \pmod m$ but $x \not\equiv 0 \pmod m$ and $y \not\equiv 0 \pmod m$. Let $z = 0$. Then $xy \equiv xz \pmod m$ since they are both conguent to zero. However $y \not\equiv z \pmod m$ since z is congruent to zero but y is not.

3. Let A and B be subsets of $\mathbb{Z}$. In the poset $(\mathcal{P}(\mathbb{Z}), \subseteq)$, prove that the greatest lower bound of $\{A, B\}$ is $A \cap B$.

   Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, it follows that $A \cap B$ is a lower bound for $\{A, B\}$. To show that it is the greatest lower bound, let C be another lower bound for $\{A, B\}$. Therefore $C \subseteq A$ and $C \subseteq B$. This implies that if $x \in C$, then $x \in A$ and $x \in B$, and so $x \in A \cap B$. This shows that $C \subseteq A \cap B$. Therefore $A \cap B$ is the largest lower bound because every other lower bound for $\{A, B\}$ is a subset of $A \cap B$.

4. Let A be the set of divisors of 36, $A = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Draw the Hasse diagram for the poset $(A, |)$.



5. For each function f, determine if it is injective. If yes, find a *left-inverse* of f, which is a function g such that $g \circ f$ is the identity.

(a) $f : \mathbb{R} \to \mathbb{R}^2$ defined by $f(x) = (x, x)$.
Yes. A left-inverse is $g : \mathbb{R}^2 \to \mathbb{R}$ defined by $g(x, y) = x$.

(b) $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = x + y$.
No.

(c) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$.
Yes. A left-inverse is $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(x) = \lfloor \frac{x}{2} \rfloor$.

(d) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$.
Yes. A left-inverse is $g : \mathbb{R} \to \mathbb{R}$ defined by

$$g(x) = \begin{cases} \ln(x) & \text{if } x > 0 \\ 0 & \text{if } x \leq 0 \end{cases}$$

(e) $f : \mathbb{Z} \to \{0\}$ defined by $f(x) = 0$.
No.

6. For each function f in Problem 5, determine if it is surjective. If yes, find a *right-inverse* of f, which is a function g such that $f \circ g$ is the identity.

(a) $f : \mathbb{R} \to \mathbb{R}^2$ defined by $f(x) = (x, x)$.
No.

(b) $f : \mathbb{R}^2 \to \mathbb{R}$ defined by $f(x, y) = x + y$.
Yes. A right-inverse is $g : \mathbb{R} \to \mathbb{R}^2$ defined by $g(x) = (x, 0)$.

(c) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 2x$.
No.

(d) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$.
No.

(e) $f : \mathbb{Z} \to \{0\}$ defined by $f(x) = 0$.
Yes. A right-inverse is $g : \{0\} \to \mathbb{Z}$ defined by $g(0) = 0$.

7. Let $f : A \to B$ and $g : B \to C$.

(a) Prove that if $g \circ f$ is injective then f is injective.
Suppose that $g \circ f$ is injective. Let $x, y \in A$ with $f(x) = f(y)$. Then applying g to both sides gives $g \circ f(x) = g \circ f(y)$. Since $g \circ f$ is injective, this implies $x = y$. Therefore f is injective.

(b) Find an example of f and g where $g \circ f$ is injective but g is not injective.
Let $f : \{1\} \to \{1, 2\}$ defined by $f(1) = 1$ and let $g : \{1, 2\} \to \{1\}$ defined by $g(1) = g(2) = 1$. Then $g \circ f = I_{\{1\}}$ which is injective, but g is not injective.

8. For each pair of sets, find a bijection from the first to the second.

(a) $\mathbb{N}_1$ and $\mathbb{N}_0$.
Define $f : \mathbb{N}_1 \to \mathbb{N}_0$ by $f(x) = x - 1$.

(b) $\mathbb{R}^2$ and $\mathbb{C}$.
Define $f : \mathbb{R}^2 \to \mathbb{C}$ by $f(x, y) = x + iy$.

(c) $\mathbb{Z}$ and $\mathbb{N}_0$.
Define $f : \mathbb{Z} \to \mathbb{N}_0$ by

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}$$

(d) $\{x \in \mathbb{R} \mid -1 < x < 1\}$ and $\mathbb{R}$.
Define $f : (-1, 1) \to \mathbb{R}$ by $f(x) = \frac{1}{x+1} + \frac{1}{x-1}$.