Math 300 E - Winter 2019
Final Exam
March 18, 2019
Answers

1. *Let A, B, and C be sets. Suppose $f : A \to B$ and $g : B \to C$.*

   (a) *Prove that, if $g \circ f$ is one-to-one, then f is one-to-one.*
   Proof: Suppose $f(x_1) = f(x_2)$ for some x_1 and $x_2 \in A$.
   Then $g(f(x_1)) = g(f(x_2))$.
   Since $g \circ f$ is one-to-one, $x_1 = x_2$.
   Hence, $f(x_1) = f(x_2)$ implies $x_1 = x_2$, and so f is one-to-one. ■

   (b) *Give an example to show that, if $g \circ f$ is one-to-one, g need not be one-to-one.*
   Proof: Let $A = \{a\}, B = \{b_1, b_2\}$, and $C = c$.
   Let $f = \{(a, b_1)\}$, and $g = \{(b_1, c), (b_2, c)\}$.
   Then $f : A \to B$ and $g : B \to C$.
   Further, $g \circ f = \{(a, c)\}$ is one-to-one, but g is not one-to-one. ■

2. *Use induction to prove that $2^n > n^2$ for all integers $n \geq 5$.*

   Proof: Let $P(n)$ be the statement "$2^n < n^2$".

   Base case: Let $n = 5$.

   Then $2^n = 2^5 = 32 > 25 = 5^2 = n^2$.

   Hence, $P(5)$ is true.

   Induction case: Suppose $P(k)$ is true for some $k \in \mathbb{Z}_{\geq 5}$.

   Then $2^k > k^2$.

   We need to show that $2^{k+1} > (k+1)^2$. (There are many ways to do this: this answer just shows one of them! The important thing is that you can come up with a way to show it.)

   We have

$$\begin{aligned}
2^{k+1} &= 2 \cdot 2^k \\
&> 2k^2 \\
&= k^2 + k^2 \\
&\geq k^2 + 5k \text{ since } k \geq 5 \\
&= k^2 + 2k + 3k \\
&\geq k^2 + 2k + 15 \text{ since } k \geq 5 \\
&> k^2 + 2k + 1 \\
&= (k+1)^2.
\end{aligned}$$

   Thus, $2^{k+1} > k^2$.

   Hence, $P(k)$ implies $P(k+1)$.

   Therefore, since $P(k)$ implies $P(k+)$, and $P(5)$ is true, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 5}$. ■

3. (a) *Let m be a positive integer.*
Suppose a, b, c and d are integers and $a \equiv b \,(mod\ m)$ and $c \equiv d \,(mod\ m)$.
Prove that $ac \equiv bd \,(mod\ m)$.
Proof:
Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we have

$$m \mid (b-a) \text{ and } m \mid (d-c).$$

Therefore, there exist integers s and t with $b - a = ms$ and $d - c = mt$.
Hence, $a = b - ms$ and $c = d - mt$, and so

$$\begin{aligned} ac &= (b - ms)(d - mt) \\ &= bd - dsm + btm + m^2 t \\ &= bd + m(bt - ds + mt). \end{aligned}$$

Hence, $ac - bd = m(bt - ds + mt)$, and since $bt - ds + mt$ is an integer, we conclude that m divides $ac - bd$.
Thus, $ac \equiv bd \pmod{m}$. ■

(b) *Prove that* $11 \mid 4^{1234} - 3$. **Proof:** We begin by investigating powers of 4 modulo 11:

$$\begin{aligned} 4^1 &\equiv 4 \pmod{11} \\ 4^2 &\equiv 5 \pmod{11} \\ 4^3 &\equiv 9 \pmod{11} \\ 4^4 &\equiv 3 \pmod{11} \\ 4^5 &\equiv 1 \pmod{11} \end{aligned}$$

Since $1234 = 5 \cdot 246 + 4$, we have

$$4^{1234} = (4^5)^{246} \cdot 4^4 \equiv 4^4 \equiv 3 (\text{mod}\, 11).$$

Thus $11 \mid 4^{1234} - 3$. ■

4. *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by*

$$f(x) = \begin{cases} \frac{1}{2}x + 3 & \text{if } x \geq 0 \\ 5x + 3 & \text{if } x < 0. \end{cases}$$

Prove that f is a bijection from $\mathbb{R}$ to $\mathbb{R}$.

Proof:

Let $y \in \mathbb{R}$.

Suppose $y \geq 3$.

Let $\hat{x} = 2(y - 3)$.

Then $\hat{x} \geq 0$, and $f(\hat{x}) = f(2(y - 3)) = \frac{1}{2}(2(y - 3)) + 3 = y$.

Suppose $y < 3$.

Let $\hat{x} = \frac{1}{5}(y - 3)$.

Then $\hat{x} < 0$ and $f(\hat{x}) = f(\frac{1}{5}(y - 3)) = 5(\frac{1}{5}(y - 3)) + 3 = y$.

Hence, for all $y \in \mathbb{R}$ there exists $\hat{x} \in \mathbb{R}$ with $f(\hat{x}) = y$, so f is surjective.

If $x \geq 0$, then $f(x) = \frac{1}{2}x + 3 \geq 0 + 3 = 3$.

If $x < 0$, then $f(x) = 5x + 3 < 0 + 3 = 3$.

Suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in \mathbb{R}$.

Suppose $f(x_1) \geq 3$.

Then $f(x_1) = \frac{1}{2}x_1 + 3 = \frac{1}{2}x_2 + 3$.

Then $\frac{1}{2}x_1 = \frac{1}{2}x_2$, so $x_1 = x_2$.

Suppose $f(x_1) < 3$.

Then $f(x_1) = 5x_1 + 3 = 5x_2 + 3$.

Then $5x_1 = 5x_2$, and so $x_1 = x_2$.

Hence, $f(x_1) = f(x_2)$ implies $x_1 = x_2$, so f is one-to-one.

Since f is one-to-one, and f is surjective, f is a bijection from $\mathbb{R}$ to $\mathbb{R}$. ■

5. *Let $A = \{a, b, c\}$. Give an example of each of the following.*

   (a) *An equivalence relation on A.*
   The simplest possible example is $\{(a, a), (b, b), (c, c)\}$.

   (b) *A relation on A that is reflexive but not symmetric.*
   One example is $\{(a, a), (b, b), (c, c), (a, b)\}$.

   (c) *A relation on A that is a function whose inverse is not a function.*
   One example is $\{(a, a), (b, b), (c, b)\}$.

6. *Let A and B be sets. Prove that $A \cap B = \varnothing$ if and only if $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\varnothing\}$.*

Proof:

Suppose $A \cap B \neq \varnothing$.

Then there exists an $x \in A \cap B$.

Then $x \in A$, so $\{x\} \subseteq A$, i.e., $\{x\} \in \mathcal{P}(A)$.

Also, $x \in B$, so $\{x\} \subseteq B$, i.e., $\{x\} in \mathcal{P}(B)$.

Hence, $\{x\} \in \mathcal{P}(A) \cap \mathcal{P}(B)$, and, since $\{x\} \neq \varnothing$, we conclude that $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

Now, suppose $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \{\varnothing\}$.

Then there exists $s \in \mathcal{P}(A) \cap \mathcal{P}(B)$ such that $S \neq \varnothing$.

Hence, there exists $x \in S$.

Then $S \in \mathcal{P}(A)$, i.e., $S \subseteq A$, and so $x \in A$.

Similarly, $S \in \mathcal{P}(B)$, i.e., $S \subseteq B$, and so $x \in B$.

Thus $x \in A \cap B$, so $A \cap B \neq \varnothing$. ■