Problem 1

Prove or disprove: For each $n \in \mathbb{N}, n^2 - n + 41$ *is prime.*

Solution. This claim is not true. We provide a counterexample: $n = 41$. Then $n^2 - n + 41 = 41^2$ which is obviously not prime since it has the factor 41.

Problem 2

If A, B, and C are sets, prove that

(a). $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

(b). $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$,

(c). $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$,

(a). *Solution.* Let $x \in A \cap (B \cup C)$. Then x is in both A and $B \cup C$. But then x is in at least one of B or C. So x is either in both A and B, or both A and C. Thus, either $x \in A \cap B$ or $x \in A \cap C$. Therefore, $x \in (A \cap B) \cup (A \cap C)$. Thus, every element in the set on the LHS is in the RHS, so $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.

We now prove the other direction. Let $y \in (A \cap B) \cup (A \cap C)$. Then y is in either in $(A \cap B)$ or $(A \cap C)$. If $y \in (A \cap B)$, then y is in both A and B. Thus y is in both A and $B \cup C$. Now if $y \in (A \cap C)$, then y is in both A and C. Thus y is in both A and $B \cup C$ as well. So $y \in A \cap (B \cup C)$ in either case. So $A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$, and so $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(b). *Solution.* Let $x \in C \setminus (A \cup B)$. Then x is in C but is not in $A \cup B$. This means x is not in A nor B. This means x is in both $C \setminus A$ and $C \setminus B$. But then $x \in (C \setminus A) \cap (C \setminus B)$. So $C \setminus (A \cup B) \subset (C \setminus A) \cap (C \setminus B)$.

We now prove the other direction. Let $y \in (C \setminus A) \cap (C \setminus B)$. Then y is in both $C \setminus A$ and in $C \setminus B$. So $y \in C$ and $y \notin A$ and $y \notin B$. Thus $y \notin A \cup B$. Thus $y \in C \setminus (A \cup B)$. So $C \setminus (A \cup B) \supset (C \setminus A) \cap (C \setminus B)$. Therefore $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

(c). *Solution.* Let $x \in C \setminus (A \cap B)$. Then x is in C but is not in $A \cap B$. This means x is not in A or is not in B. This means x is in at least one of $C \setminus A$ and $C \setminus B$. But then $x \in (C \setminus A) \cup (C \setminus B)$. So $C \setminus (A \cap B) \subset (C \setminus A) \cup (C \setminus B)$.

We now prove the other direction. Let $y \in (C \setminus A) \cup (C \setminus B)$. Then y is in at least one of $C \setminus A$ or $C \setminus B$. So $y \in C$, and $y \notin A$ or $y \notin B$. Thus $y \notin A \cup B$. Thus $y \in C \setminus (A \cup B)$. So $C \setminus (A \cup B) \supset (C \setminus A) \cap (C \setminus B)$. Therefore $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

Problem 3

Let $f\colon A \to B$. Let C, C_1, and C_2 be subsets of A, and let D be a subset of B. Prove:

(a). If f is one-to-one, then $f(C_1 \cap C_2) = f(C_1) \cap f(C_2)$.

(b). If f is 1-1, *then $f^{-1}(f(C)) = C$.*

(c). If f is onto, then $f(f^{-1}(D)) = D$.

In each part, find an inclusion relation (either "$\subseteq$" or "$\supseteq$") that can be used to replace the symbol "$=$" and produce a true statement even without the given hypothesis. [Recall that $f^{-1}(y) = \{x \in A\colon f(x) = y\}$ is, in general, a set-valued operation. It is not safe to infer that f is invertible just because the symbol f^{-1} appears.]

(a). *Solution.* Let $y \in f(C_1 \cap C_2)$. Let $y \in f(C_1 \cap C_2)$. Then there is some $x \in C_1 \cap C_2$ such that $f(x) = y$. We know $x \in C_1$ and $x \in C_2$ as well. Thus, $f(x) = y \in f(C_1)$ and $f(x) = y \in f(C_2)$, so $y \in f(C_1) \cap f(C_2)$. This means $f(C_1 \cap C_2) \subset f(C_1) \cap f(C_2)$.

We now prove the other direction. Let $y \in f(C_1) \cap f(C_2)$ now. Then there is some $x_1 \in C_1, x_2 \in C_2$ such that $f(x_1) = f(x_2) = y$. But since f is 1-1, we have that $x_1 = x_2$ since $f(x_1) = f(x_2)$; we let $x = x_1 = x_2$. But since $x = x_1 \in C_1$ and $x = x_2 \in C_2$, we have $x \in C_1 \cap C_2$. Thus $f(x) = y \in f(C_1 \cap C_2)$. Therefore, $f(C_1) \cap f(C_2) \subset f(C_1 \cap C_2)$, and so $f(C_1) \cap f(C_2) = f(C_1 \cap C_2)$.

Note that we only used f being 1-1 in proving $f(C_1) \cap f(C_2) \subset f(C_1 \cap C_2)$ and not the other direction, and so we can still say $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$.

(b). *Solution.* Let $x \in f^{-1}(f(C))$. Then, there is some $c \in C$ such that $f(x) = f(c)$. But since f is 1-1, this implies that $x = c$. So $x \in C$, implying that $f^{-1}(f(C)) \subset C$.

Proving the other direction, note that trivially, C maps to $f(C)$, and so C is at least a subset of the set that maps to $f(C)$. This means that $C \subset f^{-1}(f(C))$, therefore $f^{-1}(f(C)) = C$.

Note that we only used f being 1-1 in proving $f^{-1}(f(C)) \subset C$ and not the other direction, and so we can still say $f^{-1}(f(C)) \supseteq C$.

(c). *Solution.* Consider the inverse image of D, $f^{-1}(D)$. If $f^{-1}(D)$ has no elements, then $f(f^{-1}(D)) = \emptyset \subset D$ and we are done this direction. If $f^{-1}(D) \neq \emptyset$, then we can pick an element $x \in f^{-1}(D)$. Then, by definition, $f(x) \in D$. Since this is true for all $x \in f^{-1}(D)$ since x was arbitrary, we have $f(f^{-1}(D)) \subset D$.

Proving the other direction, since f is onto, we have $D \subset f(A)$, or more specifically $D \subset f(A_1)$, where $A_1 \subset A$ is exactly the set of elements in A that map to D. But this is just the definition of $f^{-1}(D)$, so $A_1 = f^{-1}(D)$, and thus $D \subset f(f^{-1}(D))$. Therefore, $f(f^{-1}(D)) = D$.

Note that we only used f being onto in proving $D \subset f(f^{-1}(D))$ and not the other direction, and so we can still say $f(f^{-1}(D)) \subseteq D$.

Problem 4

For Question 3(a), construct a specific example in which the indicated equation fails. (Of course the given hypothesis will have to be false too.) Repeat for parts 3(b) and 3(c).

(a). *Solution.* Consider x^2 (and so $A, B = \mathbb{R}$). Let $C_1 = [-1, 2]$ and $C_2 = [-2, 1]$. Note that x^2 is not 1-1, since it maps multiple elements in the domain to the same element in the codomain (eg. $f(-1) = f(1)$ but $-1 \neq 1$), so the hypothesis fails. Note that $f(C_1 \cap C_2) = f([-1, 1]) = [0, 1]$, however $f(C_1) \cap f(C_2) = [0, 4] \cap [0, 4] = [0, 4]$. Thus $f(C_1 \cap C_2) \neq f(C_1) \cap f(C_2)$, specifically $f(C_1 \cap C_2) \subset f(C_1) \cap f(C_2)$ as mentioned previously.

(b). *Solution.* Consider x^2 (and so $A, B = \mathbb{R}$). Let $C = [0, 1]$. Like before, x^2 is not 1-1 and so the hypothesis fails. Note that $f^{-1}(f(C)) = f^{-1}([0, 1]) = [-1, 1]$, however $C = [0, 1]$. Thus $f^{-1}(f(C)) \neq C$, specifically $f^{-1}(f(C)) \supset C$ as mentioned previously.

(c). *Solution.* Consider x^2 (and so $A, B = \mathbb{R}$). Let $D = [-1, 1]$. Note that x^2 is not onto $B = \mathbb{R}$ and so the hypothesis fails. See that $f(f^{-1}(D)) = f(f^{-1}([-1, 1])) = f([0, 1]) = [0, 1] \neq [-1, 1] = D$, where $f^{-1}([-1, 1]) = [0, 1]$, since the only elements in $A = \mathbb{R}$ that map to an element in $[-1, 1]$ are in $[0, 1]$ (specifically only mapping to $[0, 1]$). Thus $f(f^{-1}(D)) \neq D$, specifically $f(f^{-1}(D)) \subset D$ as mentioned previously.

Problem 5

Prove that there is no (a, b) *in* $\mathbb{Z} \times \mathbb{Z}$ *for which* $a^2 = 4b + 3$*. (Hint: Every integer* a *must be either even or odd.)*

Solution. For the sake of contradiction, assume there do exist such (a, b). Then either a is even or a is odd, since it is an integer. First consider the case when a is even. Then a^2 is even (since an even number squared is also even: an even number can be written as $2k$, $k \in \mathbb{Z}$, and $(2k)^2 = 4k^2 = 2(2k^2)$, which is also of the form of an even number, since $2k^2 \in Z$). Note that $4b$ is also always even, so $4b + 3$ is always odd (the form of an odd number is $2k - 1$, $k \in \mathbb{Z}$, and $4b + 3 = 2(2b + 2) - 1$). But a number can't both be odd and even simultaneously, and so $a^2 \neq 4b + 3$, a contradiction, thus a cannot be even.

Now consider when a is odd. Then we can write $a = 2k + 1$, $k \in \mathbb{Z}$. We can see $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so

$$\begin{aligned} 4b &= a^2 - 3 \\ &= 2(2k^2 + 2k) + 1 - 3 \\ &= 2(2k^2 + 2k - 1) \\ 2b &= 2(k^2 + k) - 1 \end{aligned}$$

But the LHS of the equation is of the form of an even number, and the RHS is of the form of an odd number (since $k^2 + k \in \mathbb{Z}$), and we cannot have an even number be equal to an odd number, so we get a contradiction, thus a cannot be odd. This has exhausted all possiblities of a, thus there cannot exist any such $a \in \mathbb{Z}$ that satisfies the equation, and so there is no $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ either. $\square$

Problem 6

Let $f: A \to B$ and $g: B \to C$ be given functions. Use the symbol $g \circ f$ to denote the function from A to C defined by $(g \circ f)(x) = g(f(x))$ for all $x \in A$. Prove:

(a). *If f and g are one-to-one, then $g \circ f$ is one-to-one.*

(b). *If $g \circ f$ is one-to-one, then f is one-to-one.*

(c). *If f is onto and $g \circ f$ is one-to-one, then g is one-to-one.*

(d). *It can happen that $g \circ f$ is one-to-one, but g is not. (To "prove" this, simply provide a specific example with the indicated properties.)*

(a). *Solution.* Let $x_1, x_2 \in A$ and $(g \circ f)(x_1) = (g \circ f)(x_2)$. Recall the property that for a 1-1 function f, if $f(x) = f(x')$, then $x = x'$. Since g is 1-1, this means $f(x_1) = f(x_2)$. Then since f is 1-1, this means $x_1 = x_2$, which is enough to show that $(g \circ f)(x)$ is 1-1.

(b). *Solution.* Let $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Recall the property that for a 1-1 function f, if $f(x) = f(x')$, then $x = x'$. Trivially, $g(f(x_1)) = g(f(x_2))$ because g is a function. Since $g \circ f$ is 1-1, this means $x_1 = x_2$, which is enough to show that f is 1-1.

(c). *Solution.* Let $y_1, y_2 \in B$ and $g(y_1) = g(y_2)$. Since f is onto, we know that there exists $x_1, x_2 \in A$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$. So we have $g(f(x_1)) = g(f(x_2))$, but $g \circ f$ is 1-1, so we know that $x_1 = x_2$. But if $x_1 = x_2$, then $f(x_1) = f(x_2)$ since f is a function, and so $y_1 = f(x_1) = f(x_2) = y_2$, which is enough to show that g is 1-1.

(d). *Solution.* Let $A, B, C = \mathbb{R}$, and $f(x) = e^x$ and $g(y) = y^2$. Obviously g is not 1-1, since it maps multiple elements in the domain to the same element in the codomain (eg. $f(-1) = f(1)$ but $-1 \neq 1$). But see that $g \circ f$ is 1-1: since the range of e^x is only $(0, \infty)$, and $x^2: (0, \infty) \to (0, \infty)$ is one-to-one, then by part (a) of this problem, $g \circ f$ is 1-1 (apply the statement of 6(a) with $f = e^x$, $g = y^2$, $A = \mathbb{R}$, $B = (0, \infty)$, and $C = (0, \infty)$; our definition for B, C might be different than the rest of the problem, but this is fine, since in the context of $g \circ f$, g is only taking $(0, \infty)$ as an input). Thus $g \circ f$ is 1-1, but g is not.

Problem 7

(a). Suppose $f\colon X \to X$ is a function, and define $g = f \circ f$. Prove: If $g(x) = x$ for all $x \in X$, then f is one-to-one and onto.

(b). Extend the result in (a) to the function $g = f \circ f \circ \cdots \circ f$ defined by composing f with itself n times. Show that the result is valid for each $n \in \mathbb{N}$.

(a). *Solution.* We start by showing f is 1-to-1. Let $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$. Since f is a function, we have then $f(f(x_1)) = f(f(x_2))$. But we know $(f \circ f)(x) = x$, so $x_1 = x_2$, which shows f is 1-1. Now we show f is onto. Let $x \in X$. Then $f(f(x)) = x$. But then $f(x) \in X$ maps to x under f, so there is always an element in X (namely $f(x)$) that maps to any $x \in X$, which shows that f is onto.

(b). *Solution.* Let $g = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}} = \underbrace{f \circ \cdots \circ f}_{n-1 \text{ times}} \circ f$ where $n \in \mathbb{N}$ is arbitrary, so that $g(x) = x$. Note that $g(x)$ is 1-1: Let $x_1, x_2 \in X$ and $g(x_1) = g(x_2)$. But then we have $g(x_1) = x_1 = x_2 = g(x_2)$ as well; thus g is 1-1. But problem 6(b) implies then that f is 1-1 as well, since $g = \underbrace{f \circ \cdots \circ f}_{n-1 \text{ times}} \circ f$ is 1-1. We now show that f is onto. Let $x \in X$. Then $\underbrace{(f \circ \cdots \circ f)}_{n \text{ times}}(x) = x$. But then $\underbrace{(f \circ \cdots \circ f)}_{n \text{ times}}(x)$ maps to x under f, so there is always an element in X (namely $\underbrace{(f \circ \cdots \circ f)}_{n \text{ times}}(x)$) that maps to any $x \in X$, which shows that f is onto. Note that in all of this, n was an arbitrary element in $\mathbb{N}$, and so f is 1-1 and onto for all $n \in \mathbb{N}$.

Problem 8

Let $f\colon A \to B$ and let $C \subseteq A$.

(a). Proof or counterexample: $f(A \setminus C) \subseteq f(A) \setminus f(C)$.

(b). Proof or counterexample: $f(A \setminus C) \supseteq f(A) \setminus f(C)$.

(c). What condition on f will gaurantee $f(A \setminus C) = f(A) \setminus f(C)$? (Choose between "$f$ is 1-1" and "f is onto": prove that your answer is correct.)

(a). *Solution.* We provide a counterexample. Consider $f = x^2$, $A, B = \mathbb{R}$, and $C = [0, 1]$. Then, $f(A \setminus C) = f((-\infty, 0) \cup (1, \infty)) = (0, \infty)$. On the other hand, $f(A) \setminus f(C) = f(\mathbb{R}) \setminus f([0, 1]) = [0, \infty) \setminus [0, 1] = (1, \infty)$. But then some elements in $f(A \setminus C)$ are not in $f(A) \setminus f(C)$ (consider 0.5) and so $f(A \setminus C) \not\subseteq f(A) \setminus f(C)$.

(b). *Solution.* This is true, we provide a proof. Let $y \in f(A) \setminus f(C)$. Then $y \in f(A)$, but $y \notin f(C)$. So there exists some element, call it x, such that $x \in A$ but $x \notin C$, and $f(x) = y$. We have then that $x \in A \setminus C$. Thus $f(x) = y \in f(A \setminus C)$ (since the $\in$ operation is preserved when applying functions). Since y was an arbitrary element in $f(A) \setminus f(C)$, we have $f(A \setminus C) \supseteq f(A) \setminus f(C)$.

(c). *Solution.* We give the condition that f is 1-1. Note that we already have $f(A \setminus C) \supseteq f(A) \setminus f(C)$ from 8(b), so we need only to show that $f(A \setminus C) \subseteq f(A) \setminus f(C)$. Let $y \in f(A \setminus C)$. Then there exists some unique $x \in A \setminus C$ such that $f(x) = y$. $x \in A$ but $x \notin C$. So $f(x) = y \in A$. Since f is 1-1, there is no $x' \in C$ such that $f(x) = f(x')$, since otherwise $x = x'$ but $x \notin C$. Thus $f(x) = y \notin C$. But then $y \in f(A) \setminus f(C)$. Since y was an arbitrary element in $f(A \setminus C)$, we have that $f(A \setminus C) \subseteq f(A) \setminus f(C)$. Therefore, we get $f(A \setminus C) = f(A) \setminus f(C)$ when f is 1-1.