Solutions to Homework 10:

1. *Proof.* Assume that there exists an integer a such that $a \equiv 2(\text{mod } 6)$ and $a \equiv 7(\text{mod } 9)$
So, for some $n, m \in \mathbb{Z}$ we have,

$$a = 6 \cdot n + 2 \tag{1}$$
$$a = 9 \cdot m + 7 \tag{2}$$

Hence we can say that

$$6 \cdot n + 2 = 9 \cdot m + 7 \tag{3}$$
$$6 \cdot n - 9 \cdot m = 7 - 2 \tag{4}$$
$$3 \cdot (2 \cdot n - 3 \cdot m) = 5 \tag{5}$$
$$3|5 \tag{6}$$

However 3|5, is not possible and hence our assumption is false and so by proof by contradiction there is no integer a such that $a \equiv 2(\text{mod } 6)$ and $a \equiv 7(\text{mod } 9)$

□

2. *Proof.* Let's assume that the equation $5y^2 - 4x^2 = 7$ has an integer solution

$$5y^2 - 4x^2 = 7 \tag{7}$$
$$5y^2 - 4x^2 - 7 = 0 \tag{8}$$
$$5y^2 - 3 = 4x^2 + 4 \tag{9}$$
$$y^2 - 3 = 4(x^2 + 1 - y^2) \tag{10}$$
$$y^2 = 4(x^2 + 1 - y^2) + 3 \tag{11}$$
$$y^2 \equiv 3 \quad (mod 4) \tag{12}$$

Now, we will consider two cases since y can be even or odd and so,

Case 1: y is even i.e $y = 2k$ for some $k \in \mathbb{Z}$
So, $y^2 = 2k^2 = 4k^2$
Hence $y^2 \equiv 0(\text{mod } 4)$
This contradicts the fact that $y^2 \equiv 3$ (mod 4)

Case 2: y is odd i.e $y = 2k + 1$ for some $k \in \mathbb{Z}$
So, $y^2 = (2k + 1)^2$
$y^2 = 4k^2 + 1 + 4k$
Hence $y^2 \equiv 1(\text{mod } 4)$

This contradicts the fact that $y^2 \equiv 3 \pmod 4$

Hence our initial assumption is false and by proof by contradiction the equation $5y^2 - 4x^2 = 7$ has no integer solutions. $\square$

3. (a) *Proof.* Let's assume that the inverse function is not unique i.e
$f^{-1}(y_1) \neq f^{-1}(y_2)$ for $y_1, y_2 \in Y$
Now, let $x_1, x_2 \in X$ such that

$$f(x_1) = y_1 \tag{13}$$
$$f(x_2) = y_2 \tag{14}$$

We also know that for a function's inverse to exist the function has to be bijective i.e injective and surjective, and so
$x_1 = x_2$
So, $f^{-1}(y_1) = f^{-1}(y_2)$
This contradicts our assumption and so by proof by contradiction, we have that inverse functions are unique.

$\square$

(b) **Left Inverse:**
Let's try to prove that $f^{-1} \circ g^{-1}$ is the left inverse of $g \circ f$

$$f^{-1} \circ g^{-1}(g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f \tag{15}$$
$$f^{-1} \circ g^{-1}(g \circ f) = f^{-1} \circ i_y \circ f \tag{16}$$
$$f^{-1} \circ g^{-1}(g \circ f) = f^{-1} \circ f \tag{17}$$
$$f^{-1} \circ g^{-1}(g \circ f) = i_x \tag{18}$$

Hence $f^{-1} \circ g^{-1}$ is the left inverse of $g \circ f$

Right Inverse:
Let's try to prove that $f^{-1} \circ g^{-1}$ is the right inverse of $g \circ f$

$$g \circ f(f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} \tag{19}$$
$$g \circ f(f^{-1} \circ g^{-1}) = g \circ i_y \circ g^{-1} \tag{20}$$
$$g \circ f(f^{-1} \circ g^{-1}) = g \circ g^{-1} \tag{21}$$
$$g \circ f(f^{-1} \circ g^{-1}) = i_z \tag{22}$$

Hence $f^{-1} \circ g^{-1}$ is the right inverse of $g \circ f$
And hence $f^{-1} \circ g^{-1}$ is the inverse of the function of $g \circ f$

4. *Proof.* Assume that $25^{\frac{1}{3}}$ is rational
So, $25^{\frac{1}{3}} = \frac{a}{b}$ where $a, b \in \mathbb{Z}, b \neq 0$,gcd(a,b) $= 1$
So, $25 = \frac{a^3}{b^3}$ or $25 \cdot b^3 = a^3$

We can also say that $25|a^3$, or $25|a$ or $5|a$ by Euclid's division lemma
Now let $a = 5k$ where $k \in \mathbb{Z}$
So, $25b^3 = (5)^3 \cdot k^3$
$b^3 = 25 \cdot (5k^3)$
So, $25|b^3$ or $25|b$ or $5|b$ by Euclid's division lemma
However $5|a$ and $5|b$ are not possible since gcd(a,b) = 1 and so,
our assumption is false and by proof by contradiction we have that $25^{\frac{1}{3}}$ is irrational

□

5. *Proof.* Assume that $n \in \mathbb{N}$ is a perfect square such that $n = m^2$ where $m \in \mathbb{Z}$ and 2n is also a perfect sqaure.
We have that $n = m^2$
So,

$$2n = 2m^2 \tag{23}$$
$$2n = (\sqrt{2}m)^2 \tag{24}$$

However, $\sqrt{2}m \notin \mathbb{Z}$ because $\sqrt{2}$ is an irrational number.
Hence our assumption is false and by proof by contradiction 2n is not a perfect square.

□

6. *Proof.* **Case 1:** n is even

Injective: Let $x_1, x_2 \in \mathbb{Z}$ and assume a and b are even
Now let us assume that $f(x_1) = f(x_2)$. So, we have that

$$3 - x_1 = 3 - x_2 \tag{25}$$
$$-x_1 = -x_2 \tag{26}$$
$$x_1 = x_2 \tag{27}$$

Hence f is injective.

Surjective: Let's take $x = 3 - y$
So for $f(x) = 3 - x$ we have that
$f(x) = 3 - 3 + y$
$f(x) = y$
Therefore f is surjective.

Case 2: n is odd

Injective: Let $x_1, x_2 \in \mathbb{Z}$ and assume a and b are even
Now let us assume that $f(x_1) = f(x_2)$. So, we have that

$$7 + x_1 = 7 + x_2 \tag{28}$$
$$x_1 = x_2 \tag{29}$$

Hence f is injective.

Surjective: Let's take $x = y - 7$
So for $f(x) = 7 + x$ we have that
$f(x) = 7 + y - 7$
$f(x) = y$
Therefore f is surjective.

Hence f is bijective

Since f is bijective, it should have both a left and right inverse. Therefore, f has an inverse

Case 1: n is even
Let f(n) = i. So we have that

$$i = 3 - n \tag{30}$$
$$n = 3 - i \tag{31}$$
$$f^{-1}(i) = 3 - i \tag{32}$$

Thus $f^{-1}(i)$ is the inverse function of f when n is even

Case 2: n is odd
Let f(n) = j. So we have that

$$j = 7 + n \tag{33}$$
$$n = j - 7 \tag{34}$$
$$f^{-1}(j) = j - 7 \tag{35}$$

Thus $f^{-1}(j)$ is the inverse function of f when n is even

function. □

7. (a) *Proof.* Here $f(x) = 1 - \frac{1}{x}$

Let's take $f \circ f(x)$

$$f \circ f(x) = 1 - \frac{1}{1 - \frac{1}{x}} \tag{36}$$

$$f \circ f(x) = 1 - \frac{1}{\frac{x-1}{x}} \tag{37}$$

$$f \circ f(x) = 1 - \frac{x}{x-1} \tag{38}$$

$$f \circ f(x) = \frac{x-1-x}{x-1} \tag{39}$$

$$f \circ f(x) = \frac{1}{1-x} \tag{40}$$

Now let's try to calculate $f \circ f \circ f(x)$ to get,

$$f \circ f \circ f(x) = 1 - \frac{1}{\frac{1}{1-x}} \tag{41}$$

$$f \circ f \circ f(x) = 1 - (1 - x) \tag{42}$$

$$f \circ f \circ f(x) = x \tag{43}$$

$$f \circ f \circ f(x) = i_A \tag{44}$$

Hence proved that $f \circ f \circ f(x) = i_A$

□

(b) Let's consider a function $g : A \to A$ satisfying $g \circ g \circ g = i_A$
Injective: Consider $x_1, x_2 \in A$ such that $g(x_1) = g(x_2)$
This means that $g \circ g(x_1) = g \circ g(x_2)$
This again leads to $g \circ g \circ g(x_1) = g \circ g \circ g(x_2)$
But we have that $g \circ g \circ g = i_A$ and so this means that
$i_A(x_1) = i_A(x_2)$ or $x_1 = x_2$
Thus g is injective.
Surjective: Let $y_1 \in A$.
So, we know that $g \cdot g \cdot g = i_A$, we get that $g \cdot g \cdot g(y_1) = y_1$
Therefore if we have that $x_1 = g \cdot g(y_1) = x_1$ then $g(x_1) = y_1$.
Hence g is surjective.

(c) We know that f is bijective from (a) and hence it's inverse exists similar to (b)
Let $x = f(y) = 1 - \frac{1}{y}$
So, we have that $x = \frac{y-1}{y}$
$yx = y - 1$
$y(x - 1) = -1$
$y = \frac{1}{1-x}$
Hence the inverse $f^{-1}(x) = \frac{1}{1-x}$

8. *Proof.* Let's assume that k is a positive integer and $\sqrt{k}$ is not an integer and $\sqrt{k}$ is rational

Hence, $\sqrt{k} = \frac{a}{b}$ where $a, b \in \mathbb{Z}, b \neq 0$, gcd(a,b)=1
So, $k = \frac{a^2}{b^2}$ or $k \cdot b^2 = a^2$
Now from Bezout's identity we have that if gcd(a,b) = 1 then ax + by = 1
We multiply the whole equation by a to get $a^2x + aby = a$ So, $kb^2 \cdot x + ab \cdot y = a$
Which we can write as $b(kb \cdot x + ay) = a$ or $b|a$

Case 1: $b = 1$
In that case we will have that $\sqrt{k} = a$, which is not possible since we have assumed that $\sqrt{k}$ is not an integer.

Case 2: $b \in \mathbb{Z} - \{1\}$
This will not be possible since we have that gcd(a,b) = 1

Hence our assumption is false by proof by contradiction and that if k is a positive integer and $\sqrt{k}$ is not an integer then $\sqrt{k}$ is irrational

$\square$