Solutions to homework 10:

1. Prove that there is no integer a so that $a \equiv 2(\mod 6)$ and $a \equiv 7(\mod 9)$.

    - Assume, by contrary, that there is an integer a so that $a \equiv 2(\mod 6)$ and $a \equiv 7(\mod 9)$.
    - Therefore, $a = 6k + 2$ and $a = 9\ell + 7$ for $k, \ell \in \mathbb{Z}$.
    - Then

$$\begin{aligned} a - a &= (6k + 2) - (9\ell + 7) && (1) \\ &= 3(2k - 3\ell) - 5 && (2) \\ &= 0 && (3) \\ 5 &= 3(2k - 3\ell) && (4) \end{aligned}$$

    - We know that $2k - 3\ell \in \mathbb{Z}$, hence no $k, \ell \in \mathbb{Z}$ exists such that $2k - 3\ell = \frac{5}{3}$.
    - This contradicts our assumption, hence the result holds.

2. The equation $5y^2 - 4x^2 = 7$ has no integer solutions.
   Hint: Consider the equation modulo 4.

    - $y^2 = 4(x^2 - y^2) + 7$. Hence, $y^2 \equiv 7(\mod 4)$.
    - Let's consider the case when y is even or odd.
    - Case 1: y is even.
    - Then $y = 2k, k \in \mathbb{Z}$, therefore $y^2 = 4k^2$ showing us that $y^2 \equiv 0(\mod 4)$.
    - Case 2: y is odd.
    - $y = 2k + 1, k \in \mathbb{Z}$, thus $y^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
    - As we know that $k^2 + k \in \mathbb{Z}$, $y^2 \equiv 1(\mod 4)$.
    - In either cases, $y^2 \not\equiv 7(\mod 4)$. In which contradicts are assumption.
    - Hence, there are no integer solutions for $5y^2 - 4x^2 = 7$.

3. Let $f : X \to Y$ be a function. Suppose that f admits an inverse function.

    - (a) Prove that the inverse function is unique.
        - Suppose that g is a left inverse of f and h is a right inverse of f.
        - Then, $g \circ f = i_X$ and $f \circ h = i_Y$.

$$\begin{aligned} g &= g \circ i_Y && (5) \\ &= g \circ (f \circ h) && (6) \\ &= (g \circ f) \circ h && (7) \\ &= i_X \circ h && (8) \\ &= h && (9) \end{aligned}$$

- Therefore, $g = h$ and the inverse function is unique.

- (b) Let $g : Y \to Z$ be another function with an inverse. Show that the inverse function of $g \circ f$ is given by $f^{-1} \circ g^{-1}$
  - We can see that

$$\begin{aligned} g &= g \circ i_Y && (10)\\ &= g \circ (f \circ f^{-1}) && (11)\\ g \circ g^{-1} &= g \circ (f \circ f^{-1}) \circ g^{-1} && (12)\\ i_Z &= (g \circ f) \circ (f^{-1} \circ g^{-1}) && (13) \end{aligned}$$

  - And

$$\begin{aligned} f^{-1} &= f^{-1} \circ i_Y && (14)\\ &= f^{-1} \circ (g^{-1} \circ g) && (15)\\ f^{-1} \circ f &= f^{-1} \circ (g^{-1} \circ g) \circ f && (16)\\ i_X &= (f^{-1} \circ g^{-1}) \circ (g \circ f) && (17) \end{aligned}$$

  - Hence we can see that the left and right inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$.

4. Prove that $\sqrt[3]{25}$ is irrational.
   - Let's assume, by contrary, that $\sqrt[3]{25}$ is rational.
   - Then $a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}$, such that $\sqrt[3]{25} = \frac{a}{b}$ and $\gcd(a, b) = 1$.
   - We can express this such as $a =^3 \sqrt{25}b$.
   - Hence, $a^3 = 25b^3$. We can see that $25 \mid a^3$ thus $5 \mid a^3$, and we know that 5 is prime, therefore, $5 \mid a$.
   - $a = 5n, n \in \mathbb{Z}$. Then $25b^3 = 125n^3$, and $b^3 = 5n^3$.
   - $5 \mid b^3$ proves that $5 \mid b$, hence $\gcd(a, b) = 5$ which contradicts our assumption.
   - Therefore, $\sqrt[3]{25}$ is irrational.

5. Let $n \in \mathbb{N}$. Suppose that n is a perfect square, that is $n = m^2$ for some $m \in \mathbb{Z}$. Show that $2n$ is not a perfect square. You may use the fact that $\sqrt{2}$ is irrational without proof.
   - Let's assume, by contrary, that 2n is a perfect square, hence, $2n = 2m^2 = (\sqrt{2}m)^2$.
   - Now let's assume, by contrary, that $\sqrt{2}m$ is an integer.
   - Thus we can make the expression $\sqrt{2}m = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$.
   - Then $\sqrt{2} = \frac{a}{mb}$ $(m \neq 0)$ showing that $\sqrt{2}$ is a rational number, which contradicts with the fact that $\sqrt{2}$ is an irrational number, therefore showing that $\sqrt{2}m$ is not an integer.
   - This fact contradicts with our assumption that $2n$ is a perfect square.

- Therefore, the result holds.

6. Let $f : \mathbb{Z} \to \mathbb{Z}$ defined so that

$$f(n) = \{ \begin{array}{ll} 3-n & n \text{ is even} \\ 7+n & n \text{ is odd} \end{array}$$

Prove that f is bijective and give its compositional inverse f^{-1}.

- Let $n_1, n_2 \in \mathbb{Z}$ such that n_1, n_2 are even numbers and $f(n_1) = f(n_2)$.
- Then

$$f(n_1) = f(n_2) \tag{18}$$
$$3 - n_1 = 3 - n_2 \tag{19}$$
$$n_1 = n_2 \tag{20}$$

- Hence, $n_1 = n_2$.
- Now let $n_1, n_2 \in \mathbb{Z}$ such that n_1, n_2 are odd numbers and $f(n_1) = f(n_2)$.
- Then

$$f(n_1) = f(n_2) \tag{21}$$
$$7 + n_1 = 7 + n_2 \tag{22}$$
$$n_1 = n_2 \tag{23}$$

- Hence, $n_1 = n_2$.
- Now let $n_1 \in \mathbb{Z}$ such that n_1 is odd and $n_2 \in \mathbb{Z}$ such that n_2 is even.
- Because n_1 is odd and n_2 is even, $n_1 \neq n_2$.
- Then

$$f(n_1) - f(n_2) = (7 + n_1) - (3 - n_2) \tag{24}$$
$$= 4 + n_1 + n_2 \tag{25}$$

- We know that $n_1 + n_2$ is odd hence $4 + n_1 + n_2 \neq 0$.
- Therefore, $f(n_1) \neq f(n_2)$ showing us that f is injective.
- Now let $k \in \mathbb{Z}$ and k is even and let $n = k - 7$.
- We can see that n is odd thus $f(n) = f(k-7) = 7 + (k-7) = k$.
- Now let $k \in \mathbb{Z}$ be odd and $p = 3 - k$.
- We can also see that p is even and $f(p) = f(3-k) = 3 - (3-k) = k$.
- Hence f is surjective therefore f is bijective.
- Let us define $f^{-1}(n) = 3 - n$ when n is even.
- $f(f^{-1}(n)) = f(3-n) = 3 - (3-n) = n$.

- And let us define $f^{-1}(n) = n - 7$ when n is odd.
- $f(f^{-1}(n)) = f(n-7) = 7 + (n-7) = n$.

$$f^{-1}(n) = \{ \begin{array}{ll} 3-n & n \text{ is even} \\ 7+n & n \text{ is odd} \end{array}$$

7. Let $A = \mathbb{R} - \{0, 1\}$ and let $f : A \to A$ be defined by $f(x) = 1 - \frac{1}{x}$.
   - (a) Show that $f \circ f \circ f = i_A$ and let $f : A \to A$ be defined by $f(x) = 1 - \frac{1}{x}$.
     - $f(f(f(x)))$ is

$$\begin{aligned} f(f(f(x))) &= f(f(1 - \frac{1}{x})) && (26) \\ &= f(1 - \frac{1}{1 - \frac{1}{x}}) && (27) \\ &= f(\frac{-1}{x-1}) && (28) \\ &= 1 - \frac{1}{\frac{1}{1-x}} && (29) \\ &= 1 - (1-x) && (30) \\ &= x && (31) \end{aligned}$$

     - Hence, $f(f(f(x))) = x$ showing us that $f \circ f \circ f = i_A$.
   - (b) Prove that any function $g : A \to A$ satisfying $g \circ g \circ g = i_A$ is bijective.
     - Let $x, y \in A$ s.t. $g(x) = g(y)$.
     - Then $g(g(x)) = g(g(y))$, and $g(g(g(x))) = g(g(g(y)))$.
     - $g(g(g(x))) = x = y = g(g(g(y)))$.
     - Therefore, g is injective.
     - Now let $a \in A$, then $g(g(g(a))) = a$.
     - Let $g(a) = b$, then $g(b) = a$.
     - Hence we can declare that g is surjective.
     - Therefore, g is bijective.
   - (c) Use part (b) to conclude that f is bijective and determine f^{-1}.
     - As we proved in (a), $f(f(f(x))) = x$ hence f is bijective.
     - Now let $f^{-1}(x)$ be defined as $f^{-1}(x) = \frac{1}{1-x}$.
     - As f is bijective it is sufficient to f^{-1} is a right inverse of f.
     - Thus, $f(f^{-1}(x)) = f(\frac{1}{1-x}) = 1 - \frac{1}{\frac{1}{1-x}} = 1 - (1-x) = x$.
     - Therefore, $f^{-1}(x) = \frac{1}{1-x}$.

8. Prove that if k is a positive integer and $\sqrt{k}$ is not an integer, then $\sqrt{k}$ is an irrational number.
   Hint :Bézout's identity will help you.

- Assume to contrary that when $k \in \mathbb{N}$ and $\sqrt{k} \notin \mathbb{Z}$, then $\sqrt{k} \in \mathbb{Q}$.
- Then this implies that $\sqrt{k} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b \neq 0$.
- We know that $\sqrt{k} \notin \mathbb{Z}$ so $\gcd(a, b) = 1$.
- $k = (\sqrt{k})^2 = (\frac{a}{b})^2$, and we know that $\gcd(a, b) = 1$ therefore $k \notin \mathbb{N}$.
- This contradicts with our assumption hence $\sqrt{k}$ is an irrational number.