Problem 1. Prove each of the following.

1. (2 points) The number $\sqrt[3]{2}$ is not a rational number.
   Solution We use proof by contradiction. Suppose $\sqrt[3]{2}$ is rational. Then we can write $\sqrt[3]{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b > 0$. We can assume further that $\gcd(a, b) = 1$. We have
   \[
   \sqrt[3]{2} = \frac{a}{b} \quad \Rightarrow \quad 2 = \frac{a^3}{b^3} \quad \Rightarrow \quad 2b^3 = a^3.
   \]
   So $a^3$ is even. Since any product of odd number is odd, we must have $a$ is even. Hence we can write $a = 2c$ for some $c \in \mathbb{Z}$. Now we have
   \[
   2b^3 = (2c)^3 = 8c^3 \quad \Rightarrow \quad b^3 = 2(2c^3).
   \]
   Hence $b^3$ is even. Again since any product of odd number is odd, we must have $b$ is even. So $2$ divides both $a$ and $b$, contradicting $\gcd(a, b) = 1$. Therefore, $\sqrt[3]{2}$ is irrational.

2. (2 points) The number $\log_2(3)$ is not a rational number.
   Solution We use proof by contradiction. Suppose $\log_2(3)$ is rational. Then we can write $\log_2(3) = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b > 0$. Since $\log_2(3)$ is positive, we can also assume $a > 0$. So we have
   \[
   \log_2(3) = \frac{a}{b} \quad \Rightarrow \quad 3 = 2^{\frac{a}{b}} \quad \Rightarrow \quad 3^b = 2^a.
   \]
   Since $b$ is an integer and the product of odd integers is odd, $3^b$ is odd. Since $a \geq 1$ is an integer, $2^a$ is divisible by 2, hence it is even. This is a contradiction since a number cannot be both even and odd. Thus, $\log_2(3)$ is irrational.

3. (2 points) Let $x \in \mathbb{R}$ satisfy $x^7 + 5x^2 - 3 = 0$. Then $x$ is not a rational number.
   Solution We use proof by contradiction. Suppose $x^7 + 5x^2 - 3 = 0$ and $x$ is rational, so we can write $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b > 0$ where $a$ and $b$ have no common factors. Then
   \[
   \left(\frac{a}{b}\right)^7 + 5\left(\frac{a}{b}\right)^2 - 3 = 0 \quad \Rightarrow \quad a^7 + 5a^2b^5 - 3b^7 = 0
   \]
   Since $a$ and $b$ have no common factors, they cannot both be even. We consider the other cases.
   - If $a$ and $b$ are both odd, then $a^7, 5a^2b^5$, and $-3b^7$ are all odd. Since the sum of odd numbers is odd, $a^7 + 5a^2b^5 - 3a^7$ is odd. Since $0$ is even, we get a contradiction.
• If \( a \) is even and \( b \) is odd, then \( a^7 \) and \( 5a^2b^5 \) are both even \(-3b^7 \) and \( b \) is odd. So \( a^7 + 5a^2b^5 - 3a^7 \) is odd. Since 0 is even, we get a contradiction.

• If \( a \) is odd and \( b \) is even, then \( a^7 \) is odd and \( 5a^2b^5 \) and \(-3b^7 \) are both even. So \( a^7 + 5a^2b^5 - 3a^7 \) is odd. Since 0 is even, we get a contradiction.

In each case we get a contradiction, so \( x \) is not rational.

4. (2 points) Let \( a, b, c \in \mathbb{Z} \). If \( a^2 + b^2 = c^2 \), then \( a \) or \( b \) is even.

**Solution** Let \( a, b, c \in \mathbb{Z} \) and assume for a contradiction that \( a^2 + b^2 = c^2 \) and \( a \) and \( b \) are both odd namely there exist \( k, m \in \mathbb{Z} \) such that \( a = 2k + 1 \) and \( b = 2m + 1 \) for some \( m \in \mathbb{Z} \).

Then we see that \( a^2 + b^2 = (2k + 1)^2 + (2m + 1)^2 = 4k^2 + 4k + 4m^2 + 4m + 2 \).

*First way of concluding:* Since \( a^2 + b^2 = 2(2k^2 + 2m^2 + 2k + 2m + 1) \), \( a \) or \( b \) has to be even.

*Second way of concluding:* We have \( a^2 + b^2 = 2(2k^2 + 2m^2 + 2k + 2m + 1) \). Since, \( (2k^2 + 2m^2 + 2k + 2m + 1) \in \mathbb{Z} \), we see that \( c^2 \) is even, which implies \( c \) is even. So there exists \( n \in \mathbb{Z} \) such that \( c = 2n \) and we get

\[
a^2 + b^2 = (2k + 1)^2 + (2m + 1)^2 = 4k^2 + 4k + 4m^2 + 4m + 2 = 4n^2 = c^2,
\]

which implies that

\[
2 = 4n^2 - (4k^2 + 4k + 4m^2 + 4m) = 4(n^2 - k^2 - m^2 - k - m).
\]

Since \((n^2 - k^2 - m^2 - k - m) \in \mathbb{Z} \), this implies \( 4 \mid 2 \), which is a contradiction. Therefore \( a \) or \( b \) has to be even.

5. (2 points) There do not exist \( a, n \in \mathbb{N} \) such that \( a^2 + 35 = 7^n \).

*For \( k \in \mathbb{N} \), we admit that \( 7 \mid k^2 \) implies \( 7 \mid k \).*

**Solution:** Assume for a contradiction that there exist \( a, n \in \mathbb{N} \) such that \( a^2 + 35 = 7^n \). Then we see that \( a^2 = 7(7^{n-1} - 5) \) and \( 7 \mid a^2 \) so \( 7 \mid a \) namely there exist \( m \in \mathbb{Z} \) such that \( a = 7m \). But then plugging this into the original equation, we get \( 49m^2 + 35 = 7^n \). Dividing both sides by 7, we get \( 7m^2 + 5 = 7^{n-1} \). Now, we have two cases for \( n \).

• If \( n = 1 \), then we see that the equation becomes \( 7m^2 + 5 = 1 \), which is a contradiction since the left hand side is greater than 5.

• If \( n \) is greater than 1, then \( n - 1 > 0 \) and hence \( 7 \mid 7^{n-1} \). Since \( 7m^2 + 5 = 7^{n-1} \), we see that \( 7^{n-1} - 7m^2 = 5 \). This is also a contradiction since left hand side is divisible by 7 whereas the right hand side is not.

Therefore we see that there do not exist \( a, n \in \mathbb{N} \) such that \( a^2 + 35 = 7^n \).

**Problem 2.**

1. (2 points) Show that \( \sqrt{3} \) is not a rational number.

**Solution:** Proof by contradiction. Suppose that \( \sqrt{3} \) is a rational number. Then we may write it in the form \( \frac{a}{b} \) where \( a \in \mathbb{Z} \), \( b \in \mathbb{N} \) and \( \gcd(a, b) = 1 \). So

\[
3b^2 = a^2.
\]
This implies that 3 divides $a^2$ and therefore 3 divides $a$ (this is because if $3 \nmid a$ then $a \equiv 1 \mod 3$ or $a \equiv 2 \mod 3$ and in any case $a^2 \equiv 1 \mod 3$ so $3 \nmid a^2$). Saying 3 divides $a$ means that there exists $k \in \mathbb{Z}$ such that $a = 3k$. But then

$$3b^2 = 3^2k^2$$

so $b^2 = 3k^2$ and 3 divides $b^2$ and therefore 3 divides $b$ (as we just verified in the above brackets). So 3 divides both $a$ and $b$ which contradicts the fact that gcd$(a, b) = 1$. Since we found a contradiction, it means that our initial hypothesis was false namely it is false that $\sqrt{3}$ is a rational number.

2. (2 points) Deduce that $\sqrt{3} + \sqrt{43}$ is not a rational number.

**Solution:** Assume $\sqrt{3} + \sqrt{43}$ is a rational number and call it $r$. Then $(r - \sqrt{3}) = 43$ so

$$r^2 - 2\sqrt{3}r = 40$$

and

$$r^2 - 40 = 2\sqrt{3}r .$$

Then

- either $r = 0$ but then plugging this above gives $0 = 40$, contradiction.
- or $r \neq 0$ and $\sqrt{3} = \frac{r^2 - 40}{2r} \in \mathbb{Q}$. Contradiction.

In any case we have a contradiction so $r$ is not in $\mathbb{Q}$.

**Problem 3. (2 points)** Prove the equation $4x^2 + 5y^2 = 7$ has no integer solutions. (Hint: Think about this equation modulo 4.)

**Solution** Suppose there are integers $x$ and $y$ satisfying $4x^2 + 5y^2 = 7$. Then

$$4x^2 + 5y^2 \equiv 7 \mod 4$$

$$0x^2 + 1y^2 \equiv 3 \mod 4$$

$$y^2 \equiv 3 \mod 4$$

However, we are in one of the four following cases:

**Case 1** If $y \equiv 0 \mod 4$, then $y^2 \equiv 0^2 \equiv 0 \mod 4$.

**Case 2** If $y \equiv 1 \mod 4$, then $y^2 \equiv 1^2 \equiv 1 \mod 4$.

**Case 3** If $y \equiv 2 \mod 4$, then $y^2 \equiv 2^2 \equiv 0 \mod 4$.

**Case 4** If $y \equiv 3 \mod 4$, then $y^2 \equiv 3^2 \equiv 1 \mod 4$.

This is a contradiction. Hence, the equation has no integer solutions.

**Problem 4. For this problem, we are going to use the following result: if**

$$f : A \rightarrow B$$

**is a bijection between finite sets $A$ and $B$, then $A$ and $B$ have the same number of elements. In fact we say that they have the same cardinality and we write $|A| = |B|$.

For any set $X$, denote by $\{0, 1\}^X$ the set of all functions $X \rightarrow \{0, 1\}$. That is,

$$\{0, 1\}^X = \{ f : f \text{ is a function from } X \text{ to } \{0, 1\} \}.$$
1. For \( n \in \mathbb{N} \), define the set \( X_n = \{1, \ldots, n\} \). How many elements are there in \( \{0,1\}^{X_n} \)? We could actually prove this by induction but feel free to just give the answer without justification based on your intuition.

**Solution:** this cardinality is \( 2^n \) (same as number of possible outcomes if you play heads and tails \( n \)-times).

2. Let \( X \) be any set. For each subset \( Y \subseteq X \), define \( f_Y \) to be the function

\[
  f_Y : X \rightarrow \{0,1\} \\
  x \mapsto \begin{cases} 
    1 & \text{if } x \in Y \\
    0 & \text{if } x \in X \setminus Y
  \end{cases}
\]

This is called the characteristic of \( Y \) (see how it keeps track of the elements in \( Y \)).

(a) (1 point) When \( X = \mathbb{R} \) and \( Y = [0, 1] \), draw the graph of \( f_Y \).

(b) (1 point) When \( X = \mathbb{R} \) and \( Y = [0, +\infty) \), draw the graph of \( f_Y \).

**Solution:** see last page.

(c) (2 points) Now back to the general case of \( X \). Prove that the function

\[
  F : \mathcal{P}(X) \rightarrow \{0,1\}^X \\
  Y \mapsto f_Y
\]

is a bijection by giving the inverse of \( F \).

**Solution:** We define the following function:

\[
  G : \{0,1\}^X \rightarrow \mathcal{P}(X) \\
  f \mapsto f^{-1}(\{1\})
\]

We prove that \( F \circ G = \text{id}_{\{0,1\}^X} \) and \( G \circ F = \text{id}_{\mathcal{P}(X)} \).

- Proof that \( F \circ G = \text{id}_{\{0,1\}^X} \): Let \( f \in \{0,1\}^X \). By definition, \( F \circ G(f) = F(f^{-1}(\{1\})) \) is the function

\[
  F(f^{-1}(\{1\})) : X \rightarrow \{0,1\} \\
  x \mapsto \begin{cases} 
    1 & \text{if } x \in f^{-1}(\{1\}) \text{ namely if } f(x) = 1 \\
    0 & \text{if } x \notin f^{-1}(\{1\}) \text{ namely if } f(x) \neq 1 \text{ namely if } f(x) = 0
  \end{cases}
\]

so we see that in fact \( F(f^{-1}(\{1\})) = f \) and \( F \circ G(f) = f \).

- Proof that \( G \circ F = \text{id}_{\mathcal{P}(X)} \): Let \( Y \in \mathcal{P}(X) \) namely \( Y \subseteq X \). By definition,

\[
  G \circ F(Y) = F_Y^{-1}(\{1\}) = \{x \in X : F_Y(x) = 1\} = \{x \in X : f_Y(x) = 1\}.
\]

But by definition of \( F_Y \), we have \( Y = \{x \in X : f_Y(x) = 1\} \) (\( f_Y \) is precisely the function that takes value 1 at elements of \( Y \) and value 0 outside of \( Y \)). So \( G \circ F(Y) = Y \).

3. Prove that \( \mathcal{P}(X_n) \) has cardinality \( 2^n \).

**Solution:** We proved in 2.(c) that \( \mathcal{P}(X_n) \) and \( \{0,1\}^{X_n} \) have the same cardinality and in 1. that \( \{0,1\}^{X_n} \) has cardinality \( 2^n \).
graph of $f_Y$

$x = \mathbb{R}$
$y = [0, 1]$