Problem 1.

Suppose that A and B are non-empty finite sets of real numbers such that $A \subseteq B$.
Prove that:

$$\min(B) \leq \min(A) \leq \max(A) \leq \max(B)$$

Solutions:

As A and B are non-empty finite sets, all of $\min(A), \min(B), \max(A)$ and $\max(B)$ exist.
By the definition of $\min(B)$, for any $b \in B$, $b \geq \min(B)$.
But since $A \subseteq B$ and $\min(A) \in A$, then $\min(A) \in B$ and so $\min(A) \geq \min(B)$.
By the definition of $\max(B)$, $\max(B) \geq b$ for any $b \in B$ and again, as $\max(A) \in A$ and $A \subseteq B$, then $\max(A) \in B$ and so $\max(B) \geq \max(A)$.
The inequality $\min(A) \leq \max(A)$ is obvious from the definitions of $\max(A)$ and $\min(A)$, and so the result follows.

Problem 2.

(a) Let $f : X \to \mathbb{N}_n$ be an injection. Prove then that X is finite and $|X| \leq n$.

(b) Given non-empty finite sets X and Y with $|X| < |Y|$, prove that there does not exist a surjection $X \to Y$.
You can assume the following fact:
If $f : \mathbb{N}_n \to X$ is a surjection, then X is finite and $|X| \leq n$.

Solution:

(a) We can prove this by contrapositive.
That is, we can show that if X is either infinite or $|X| > n$, then $f : X \to \mathbb{N}_n$ is not an injection. This requires a proof by cases.
If X is infinite, then X has strictly more elements than $\mathbb{N}_n$. If there is an injection $f : X \to \mathbb{N}_n$, then every element of X must map to a unique element of $\mathbb{N}_n$. Therefore, there are exactly n elements $x_1, \ldots, x_n$ of X such that $f(x_1) = 1, \ldots, f(x_n) = n$. But since X is infinite, there is an element x_0 different from all of these. Since we assume f is injective, x_0 uniquely maps to a further element of $\mathbb{N}_n$, $f(x_0)$, which is different from all of $1, \ldots, n$ and this is impossible since these are all of the elements of $\mathbb{N}_n$. So f maps x_0 to nothing, and that is impossible by the definition of a function. Contradiction. Therefore, $f : X \to \mathbb{N}_n$ cannot be an injection.
If $|X| > n$, we have two cases: either X is finite or X is infinite. If X is infinite, then we know that $f : X \to \mathbb{N}_n$ cannot be an injection by the previous case. If X is finite, then by assumption $|X| > n = |\mathbb{N}_n|$ and the pigeonhole principle applies (since X and $\mathbb{N}_n$ are finite) and so there is no injection $f : X \to \mathbb{N}_n$.

(b) We can also prove this by contrapositive.
Assume that X and Y are finite and that $f : X \to Y$ is a surjection. Since X is finite, there exists $n \in \mathbb{N}$ with $n = |X|$ and a bijection $g : \mathbb{N}_n \to X$. As g is a bijection, it is also a surjection. Therefore, $f \circ g : \mathbb{N}_n \to Y$ is a surjection.
Thus, $|X| = n \geq |Y|$. This show the contrapositive of what we needed to show.

Problem 3. Prove that there does not exist a rational number whose square is 10.

Solution:

Proof by contradiction.

Suppose that there exists a rational number $\frac{p}{q}$ whose square 10 – where p and q have no common divisor. Then $\frac{p^2}{q^2} = 10$, and so $p^2 = 10q^2$. Therefore, 10 divides p^2. Whence p^2 is also divisible by 2 (as 2 divides 10) and so p is also divisible by 2 – i.e. there exists a p_1 such that $p = 2p_1$. But then, $(2p_1)^2 = 10q^2$ and so $2p_1^2 = 5q^2$.

As 2 does not divide 5, q^2 must be divisible by 2; which implies that q is divisible by 2. Therefore, p and q have 2 as a common divisor. Contradiction.

Problem 4.

Use the Euclidean algorithm to find the greatest common divisor of 165 and 252.

Solution:

We use the Euclidean algorithm:

$$\begin{aligned}
252 &= 165(1) + 87 \\
165 &= 87(1) + 78 \\
87 &= 78(1) + 9 \\
78 &= 9(8) + 6 \\
9 &= 6(1) + \mathbf{3} \\
6 &= 3(2) + 0
\end{aligned}$$

Therefore, gcd(252,165) = 3.

Problem 5.

Let n be an integer.

(a) Prove that n^2 is divisible by 5 **if and only if** n is divisible by 5.

(b) Use the result of (a) to prove that there does not exist a rational number number whose square is 5.

Solution:

(a) One direction is easy: if n is divisible by 5, then $n = 5q$ for some $q \in \mathbb{Z}$ and so $n^2 = 25q^2 = 5(5q^2)$ – which means that n^2 is divisible by 5.
We prove the other implication by contrapositive. If n is not divisible by 5, then $n = 5q + r$ where $1 \leq r \leq 4$. Whence $n^2 = 25q^2 + 10qr + r^2 = 5(5q^2 + 2qr) + r^2$. Now as $r = 1, 2, 3$ or 4, then $r^2 = 1, 4, 9$ or 16. In every case, r^2 is not divisible by 5 and so n^2 cannot be divisible by 5. Therefore, by contrapositive, if n^2 is divisible by 5, then n is divisible by 5.

(b) Assume that there is a rational number $\frac{p}{q}$ whose square is 5 – where p and q have no common divisor. Then $\frac{p^2}{q^2} = 25$ and so $p^2 = 25q^2 = 5(5q^2)$ which implies that p^2 is divisible by 5. Therefore, p is divisible by 5 (by (a)) – which implies that $p = 5p_1$ for some integer p_1. Thus: $(5p_1)^2 = 25q^2$ so that $p_1^2 = q^2$. But then, $q = \pm p_1$ which means that p and q have p_1 as a common divisor. Contradiction.

Problem 6.

(a) Let a be an integer. Prove that if a is even, then a^2 is even, and if a is odd, then $a^2 = 4p + 1$ for some $p \in \mathbb{Z}$.

(b) Prove that an integer n is the sum of two squares ($n = a^2 + b^2; a, b \in \mathbb{Z}$), then $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ for some $q \in \mathbb{Z}$.

Solution:

(a) Let a be an integer.
If a is even, then $a = 2a_1$ for some integer a_1. Therefore, $a^2 = (2a_1)^2 = 2(2a_1^2)$ so that a^2 is even.
If a is odd, then $a = 2a_1 + 1$ for some $a_1 \in \mathbb{Z}$.
So $a^2 = (2a_1 + 1)^2 = 4a_1^2 + 4a_1 + 1 = 4(a_1^2 + a_1) + 1 = 4p + 1$ where $p = a_1^2 + a_1 \in \mathbb{Z}$.

(b) Let n be the sum of two squares – i.e. $n = a^2 + b^2; a, b \in \mathbb{Z}$.
If a and b are both even, then $a^2 = 4a_1^2$ and $b^2 = 4b_1^2$ for some $a_1, b_1 \in \mathbb{Z}$ by the response to (a). So $n = 4(a_1^2 + b_1^2) = 4q$ where $q = a_1^2 + b_1^2 \in \mathbb{Z}$.
If a is even and b is odd or vice versa, then $a^2 = 4k^2$ and $b^2 = 4p+1$, or $a^2 = 4p+1$ and $b^2 = 4k^2$; for some $k, p \in \mathbb{Z}$ (by (a)). Therefore, $n = 4k^2+4p+1 = 4(k^2+p)+1 = 4q+1$ where $q = k^2 + p \in \mathbb{Z}$.
If a and b are both odd, then $a^2 = 4p + 1$ and $b^2 = 4p' + 1$ for some $p, p' \in \mathbb{Z}$ (by (a)) and so $n = 4p + 4p' + 2 = 4(p + p') + 2 = 4q + 2$ where $q = p + p' \in \mathbb{Z}$.
This concludes the proof.