Solution Set 2

Problem 1

(1) $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes of $\mathbb{Z} \mod n$. Equivalence is determined by the following rule: $[a] = [b]$ if and only if $b - a = k \cdot n$ for some $k \in \mathbb{Z}$. The operations $+$ and $\cdot$ are defined by $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [a \cdot b]$.

(2) Axiom 1: Commutivity

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

$$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$$

Axiom 2: Associativity

$$([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c] = [a] + ([b + c])$$

$$([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [a \cdot b \cdot c] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$$

Axiom 3: Distributivity

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [a \cdot b + a \cdot b] = [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c]$$

Axiom 4: Existance of identities

$[0]$ is the additive identity, since $[a] + [0] = [a + 0] = [a]$.
$[1]$ is the multiplicative identity, since $[a] \cdot [1] = [a \cdot 1] = [a]$.

Axiom 5: Existance of negatives

The negative for $[a]$ is $[-a]$, since $[a] + [-a] = [a + (-a)] = [0]$, which is the additive identity.

If $n = 1$, Axiom 4 fails, because there is only one equivalence class, so $[a] = 0$ for all $a \in \mathbb{Z}$, and there cannot be a multiplicative identity distinct from $[0]$.

(3) Assume that $n = ab$, where $a, b \in \mathbf{Z}$ and neither a nor b is 1. Then, $\mathbb{Z}/n\mathbb{Z}$ cannot be a field because $[a]$ doesn't have a reciprocal.

Proof: Assume $[c] \cdot [a] = [1]$. Then $ac \equiv 1 \mod n$, so $ac = 1 + kn$ for some $k \in \mathbb{Z}$. However, since $n = ab$, this implies that $ac + kab = 1$, or $a(c + kb) = 1$. Since the left side is divisible by a and the right side is not (since $a \neq 1$), this is a contradiction. Therefore, a does not have a reciprocal, and so $\mathbb{Z}/n\mathbb{Z}$ cannot be a field.

(4) If $[a] \cdot [b] = 0$, by definition $ab = kn$ for some $k \in \mathbb{Z}$. So, n divides ab, and since n is prime, it must divide either a or b. If $n \mid a$, then $[a] = [0]$, which is not the case. Therefore, $n \mid b$, so $[b] = [0]$. Therefore, if $[a] \cdot [b] = [0]$ and $[a] \neq [0]$, then $[b] = [0]$.

Conversely, if $[b] = [0]$, then $[a] \cdot [b] = [a] \cdot [0] = [a \cdot 0] = [0]$. Therefore, $[a] \cdot [b] = [0]$ if and only if $[b] = 0$.

(5) Since $[a] \cdot [b_1] = [a] \cdot [b_2]$, we know $[a] \cdot [b_1] - [a] \cdot [b_2] = [0]$. So:

$$[0] = [a] \cdot ([b_1] - [b_2])$$
$$[0] = [a] \cdot ([b_1 - b_2])$$
$$[0] = [a \cdot (b_1 - b_2)]$$

Therefore, n divides $a(b_1 - b_2)$. Since n is prime, it must therefore divide either a or $b_1 - b_2$. Since $[a] \neq [0]$, n does not divide n, so it must divide $b_1 - b_2$. Therefore, $[b_1] = [b_2]$.

(6) From (5), we know that $[a] \cdot [b_1] = [a] \cdot [b_2]$ only if $[b_1] = [b_2]$. Therefore, as $[b]$ ranges through the n distinct values $\{[0], [1], ..., [n-1]\}$, the product $[a] \cdot [b]$ must also range through n different values. Since there are exactly n equivalence classes in $\mathbb{Z}/n\mathbb{Z}$, the set $\{[a] \cdot [0], [a] \cdot [1], ..., [a] \cdot [n-1]\}$ must equal $\mathbb{Z}/n\mathbb{Z}$.

(7) If $[a]$ is non-zero, as shown in [6], the set $\{[a] \cdot [0], [a] \cdot [1], ..., [a] \cdot [n-1]\} = \mathbb{Z}/n\mathbb{Z}$. Therefore $[a] \cdot [b] = [1]$ for some $[b] \in \{[0], [1], ..., [n-1]\}$.

(8) By (7), $\mathbb{Z}/n\mathbb{Z}$ satisfies the 6th field axiom. Since it satisfies field axioms 1-5, as shown in (2), $\mathbb{Z}/n\mathbb{Z}$ is a field.

Problem 2

Part 1

$a < c$, so we can add b on both sides to get $a + b < c + b$. But $b < d$, so we can add c on both sides to get $b + c < c + d$. Hence, by transitivity, $a + b < c + d$.

Part 2

By the order axioms, $0 \leq a^2$ for all a, so $0 + 1 \leq a^2 + 1$. But then, since $0 < 1$, $0 < a^2 + 1$ for all a, so the original equation has no solutions.

Part 3

$a < 0$, so we can add b on both sides and get $a + b < b$. But $b < 0$, so $a + b < 0$.

Part 4

By contradiction. If $a > 0$, assume $a^{-1} < 0$. Then $-a^{-1} > 0$, and since $a > 0$, then $a \cdot -a^{-1} > 0$. This implies that $-1 > 0$, which is false. Hence $a^{-1} > 0$.
If $a < 0$, we proceed similarly (but you had to show it).

Part 5

Assume $a^{-1} < b^{-1}$. We can add $-a^{-1}$ on both sides to get $0 < b^{-1} - a^{-1}$. Hence we can multiply by a on both sides to get $0 < ab^{-1} - 1$. Now we can multiply on both sides by b to get $0 < a - b$, from which we conclude that $b < a$. This is a contradiction.
From both claims we conclude that $0 < b^{-1} < a^{-1}$.

Part 6
If $a = 0$, we are done. Take $a > 0$. We have $b > a$ for all $a > 0$ and, in particular, for $b = a$. Hence $a > a$, which is false.

Problem 3

1. Assume, as in the hint, that $\mathbb{N}$ is bounded above by some $r \in \mathbb{R}$. Then it has some least upper bound, x. Now, there must be some natural number n between x and $x - 1$, $x - 1 < n \leq x$, or else $x - 1$ would be a new least upper bound, and $x - 1 < n \Rightarrow x < n + 1$. But $n + 1$ is a natural number, and x the least upper bound of the natural numbers. Thus, we have a contradiction, and we conclude that the natural numbers are unbounded.

2. Take $x \in \mathbb{R}^+$. Assume, contrary to the claim, that there are no positive integers n such that $1/n < x$, that is, that $x \leq 1/n$, $\forall\ n$ in the positive integers, or the natural numbers (they are the same set). This implies $1/x \geq n$ (we can conclude this because x and n are positive and so have positive inverses). However, that would make $1/x$ an upper bound for the natural numbers, which is clearly bogus from part 1. Thus, we conclude that there is always some positive integer n s.t. $1/n < x$, $\forall\ x \in \mathbb{R}$.

Problem 4

We shall prove the statement by contradiction. Assume there is a rational number x such that $x^2 = 2$. Write x in lowest terms: $x = a/b$, where a and b are relatively prime integers.

$a^2/b^2 = 2$, which tells us that $a^2 = 2b^2$, and, since b is an integer, 2 divides a^2. Then a must be even because 2 is prime. (Alternatively, one could assume that a is odd and arrive at a contradiction: if $a = 2k+1$ for some integer k, then $a^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd).

So we can write $a = 2m$, where m is a non-zero integer. Then, $a^2 = 2b^2 \Leftrightarrow (2m)^2 = 2b^2 \Leftrightarrow 4m^2 = 2b^2 \Leftrightarrow 2m^2 = b^2$ and thus b^2 is even, which, by the same argument as above, implies that b is even. This contradicts our assumption that a/b is the expression of x in lowest terms.

Notes: Many people claimed that for x to be rational, a and b must be relatively prime. This statement betrays a rather poor understanding of the idea behind the proof: we choose a and b to be relatively prime (which is always possible because we can reduce x to lowest terms) in order to arrive at a contradiction. It is by no means necessary for a and b to have no common factors, unless we pick them this way.

I did not take points off for assuming that the square of an even number is even, but I have been substracting points for assuming that the square root of an even number is even. It is a rather obvious fact indeed, but, to my surprise, some of you tried to prove it and failed, which forced me to penalize those who have not provided some (valid) justification for the statement.

Problem 5

(1) We need to prove that $1 + 2 + 3 + \cdots + (2n - 1) = n^2$.
First we need to check the base case where $n = 1$. $1 = 1^2$ is obviously true.
Next, we assume that for some $n = k$ that

$$1 + 2 + 3 + \cdots + (2k - 1) = k^2$$

. Our goal is to show that this implies that our statement is true for $n = k + 1$. We start with:

$$1 + 2 + 3 + \cdots + (2k - 1) = k^2$$

$$1 + 2 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1)$$

$$1 + 2 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) = k^2 + 2k + 1$$

$$1 + 2 + 3 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$$

Therefore, our statement is then true for $n = k + 1$.

(2) We want to prove that

$$1^2 + 2^2 + 3^2 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$$

First, we need to check the base case where $n = 1$. This is obvious as $1^3 = 1^2$. Next, we will assume that our statement is true for $n = k$ and show that it implies that our statement is true for $n = k + 1$. Before completing the induction step, I would like to note that I allowed people to use the fact that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ without proving it, as the proof is given in Gerardo's handout. So, we begin as follows

$$1^2 + 2^2 + 3^2 + \cdots + k^3 = (1 + 2 + \cdots + k)^2$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = (1 + 2 + \cdots + k)^2 + (k + 1)^3$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = \Big(\frac{k(k + 1)}{2}\Big)^2 + (k + 1)^3$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = \frac{k^2(k + 1)^2 + 4(k + 1)^3}{4}$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = \frac{(k + 1)^2(k^2 + 4(k + 1))}{4}$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = \frac{(k + 1)^2(k + 2)^2}{4}$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = \Big(\frac{(k + 1)(k + 2)}{2}\Big)^2$$

$$1^2 + 2^2 + 3^2 + \cdots + k^3 + (k + 1)^3 = (1 + 2 + 3 + \cdots + k + (k + 1))^2$$

We have proved the statement for $n = k + 1$ and we're done.

(3) First, we need to prove our base case. In this instance, our base case is $n = 0$ NOT $n = 1$ as many of you thought. If we let n=0, then we know that our statement is true because we can let

$q = 0$ and $r = 0$ as $0 = 0\dot{b}$.
We will now assume that our statement holds for $n = k$. There exist non negative integers q and r such that

$$k = qb + r \text{ and } 0 \leq r < b$$

If we add 1 to both sides, we get

$$k + 1 = qb + r + 1$$

Now, it seems as though we have proved our assumption for $n = k + 1$. But, this is not true as we don't know whether or not $r + 1 < b$. We need to consider 2 cases.

Case 1: $r + 1 < b$
Since $k + 1 = qb + (r + 1)$, q and $r + 1$ are precisely the non negative integers that satisfy our inductive hypothesis because $0 \leq r + 1 < b$.

Case 2: $r + 1 = b$
$k + 1 = qb + (r + 1) = qb + b = (q + 1)b + 0$. Therefore, $q + 1$ and 0 are precisely the non negative integers that satisfy our inductive hypothesis because $0 \leq 0 < b$.