Math 23aTheoretical Linear Algebra and Multivariable Calculus I

PROBLEM SET 2

Problem 1: Let n be a positive integer. By the end of this problem we'll have proved the following

Theorem 1. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

(1) Recall the definition of the set $\mathbb{Z}/n\mathbb{Z}$, and of the operations $+$ and $\cdot$ on the set $\mathbb{Z}/n\mathbb{Z}$.
(2) Prove that Axioms 1–5 of fields hold for $\mathbb{Z}/n\mathbb{Z}$, for $n \neq 1$. Which axiom fails for $n = 1$?
(3) Prove that, if n is a *composite* number (i.e. $n = ab$ for a, b positive integers not equal to 1), then $\mathbb{Z}/n\mathbb{Z}$ is not a field.
(4) From now on we let $n = p$ be a *prime* number (i.e. not composite) not equal to 1. Let $[a]$, $[b] \in \mathbb{Z}/p\mathbb{Z}$, with $[a] \neq 0$. Prove that $[a] \cdot [b] = [0]$ if and only if $[b] = 0$.
Hint. You can use the following property of prime integers: if a prime p divides a product of integers ab, then p divides either a or b.
(5) Let $[a]$, $[b_1]$, $[b_2] \in \mathbb{Z}/p\mathbb{Z}$, with $[a] \neq 0$. Prove that $[a] \cdot [b_1] = [a] \cdot [b_2]$ if and only if $[b_1] = [b_2]$.
(6) Fix $[a] \in \mathbb{Z}/p\mathbb{Z}$, a non zero element. Show that

$$\left\{ [a] \cdot [b] \;\middle|\; b = 0, 1, \ldots, n-1 \right\} \;=\; \mathbb{Z}/p\mathbb{Z} \; .$$

(7) Prove that, if $[a] \in \mathbb{Z}/p\mathbb{Z}$ is non zero, there exists $[b] \in \mathbb{Z}/p\mathbb{Z}$ such that $[a][b] = [1]$.
(8) Conclude that $\mathbb{Z}/p\mathbb{Z}$ is a field.

Problem 2: Let F be an ordered field. Prove the following statements. (You can use the axioms of ordered fields and/or the properties previously proved in class).
(1) If $a < c$ and $b < d$, then $a + b < c + d$.
(2) There is no $x \in F$ such that $x^2 + 1 = 0$.
(3) If $a < 0$ and $b < 0$, then $a + b < 0$.
(4) If $a > 0$ then $a^{-1} > 0$. If $a < 0$, then $a^{-1} < 0$.
(5) If $0 < a < b$, then $0 < b^{-1} < a^{-1}$.
(6) If $a \geq 0$, and $a < b$ for every $b > 0$, then $a = 0$.

Problem 3: (1) Prove that there is no real number which is bigger than every positive integer.
Hint. Assume, by contradiction, that $\mathbb{N}$ is bounded above in $\mathbb{R}$ and consider its least upper bound.
(2) Prove that, if $x > 0$ is a positive real number, then there exists a positive integer n such that $1/n < x$.
Hint. Use Part (1).

Problem 4: Prove that there is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.
Hint. Prove the statement by contradiction. You can use the following fact: every rational number $x \in \mathbb{Q}$ can be written as $x = a/b$, with a and b integers relatively prime to each other (i.e. there is no integer $n \geq 2$ which divides both a and b). In particular, either a or b is odd.

Problem 5: Prove by induction the following statements:

(1) $1 + 3 + 5 + \cdots + (2n - 1) \;=\; n^2$

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

(3) Fix $b \in \mathbb{N}$. For every integer $n \geq 0$ there exist non negative integers q and r such that

$$n = qb + r \quad \text{and} \quad 0 \leq r < b \; .$$