Homework 3 Partial Solutions
Problems IV

1. Prove that if an integer $n$ is the sum of two squares ($n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$) then $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ for some $q \in \mathbb{Z}$. Deduce that 1234567 cannot be written as the sum of two squares.

Proof. Suppose $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. By exercise 15.5, any perfect square is equal to $4q$ or $4q + 1$ for some $q \in \mathbb{Z}$. This gives three cases for $a^2, b^2$:

- If $a^2 = 4p$ and $b^2 = 4q$ for some $p, q \in \mathbb{Z}$, then
  
  $$n = a^2 + b^2 = 4p + 4q = 4(p + q).$$

- If $a^2 = 4p$ and $b^2 = 4q + 1$ for some $p, q \in \mathbb{Z}$, then
  
  $$n = a^2 + b^2 = 4p + 4q + 1 = 4(p + q) + 1.$$  
  
  We obtain a similar result when $a^2 = 4p + 1$ and $b^2 = 4q$ for some $p, q \in \mathbb{Z}$.

- If $a^2 = 4p + 1$ and $b^2 = 4q + 1$ for some $p, q \in \mathbb{Z}$, then
  
  $$n = a^2 + b^2 = 4p + 1 + 4q + 1 = 4(p + q) + 2.$$

Therefore, $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ for some $q \in \mathbb{Z}$. Since 1234567 = 4(308641) + 3, 1234567 is not the sum of two squares. 

2. Let $a$ be an integer. Prove that $a^2$ is divisible by 5 if and only if $a$ is divisible by 5.

Proof. ($\Rightarrow$) Suppose $a^2$ is divisible by 5. We may express $a$ in one of the following ways:

- If $a = 5q$ for some $q \in \mathbb{Z}$, then 5 divides $a$.

- If $a = 5q + 1$ for some $q \in \mathbb{Z}$, then
  
  $$a^2 = (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1,$$

  which is a contradiction since 5 divides $a^2$.

- If $a = 5q + 2$ for some $q \in \mathbb{Z}$, then
  
  $$a^2 = (5q + 2)^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4,$$

  which is a contradiction since 5 divides $a^2$.

- If $a = 5q + 3$ for some $q \in \mathbb{Z}$, then
  
  $$a^2 = (5q + 3)^2 = 25q^2 + 30q + 9 = 25q^2 + 30q + 5 + 4 = 5(5q^2 + 6q + 1) + 4,$$
which is a contradiction since 5 divides \(a^2\).

- If \(a = 5q + 4\) for some \(q \in \mathbb{Z}\), then
  \[
  a^2 = (5q + 4)^2 = 25q^2 + 40q + 16 = 25q^2 + 40q + 15 + 1 = 5(5q^2 + 8q + 3) + 1,
  \]
  which is a contradiction since 5 divides \(a^2\).

Therefore, 5 must divide \(a\).

(\(\Leftarrow\)) Assume \(a\) is divisible by 5. Then \(a = 5q\) for some \(q \in \mathbb{Z}\). Then \(a^2 = (5q)^2 = 25q^2 = 5(5q^2)\), so 5 divides \(a^2\). \(\square\)