Math 109: Winter 2014
Homework 7 Solutions

1. Let $P$ denote the set of all polynomials with coefficients in $\mathbb{Q}$. Recall that a polynomial has degree $n$ if it is of the form $a_nx^n + \cdots + a_1x + a_0$ where $a_n \neq 0$. (The zero polynomial 0 has degree zero.) For $n \in \mathbb{Z}^+$, let $P_n$ denote the set of all polynomials with coefficients in $\mathbb{Q}$ having degree $n$. We have that $P = \bigcup_{n \in \mathbb{Z}^+} P_n$, so to show that $P$ is countable it is enough to show that $P_n$ is countable for all $n \in \mathbb{Z}^+$.

Let $n \in \mathbb{Z}^+$. We define a function $i : P_n \to \mathbb{Q}^{n+1}$ by $i(a_nx^n + \cdots + a_1x + a_0) = (a_n, \ldots, a_1, a_0)$. It is clear that $i$ is an injection. Since finite Cartesian products of countable sets are countable, we know that $\mathbb{Q}^{n+1}$ is countable. Since $i$ is an injection, it follows that $P_n$ is also countable. Therefore, we have that $P$ is countable.

To see that $P$ is denumerable it is enough to show that $P$ is infinite. But this is clear because the rational numbers (viewed as constant polynomials) constitute an infinite subset of $P$.

2. Let $P'$ denote the set of all polynomials with rational coefficients other than the zero polynomial. By Problem 1 we know that $P'$ is countable. This means we can write $P' = \{f_1, f_2, \ldots\}$. For $n \in \mathbb{Z}^+$, let $R_n$ denote the set of roots of the polynomial $f_n$. By the fact we are allowed to assume, the set $R_n$ is finite for each $n \in \mathbb{Z}^+$. It follows that $\mathbb{Q} = \bigcup_{n \in \mathbb{Z}^+} R_n$ is a countable union of finite sets, and hence countable.

To see that $\mathbb{Q}$ is denumerable it is enough to show that $\mathbb{Q}$ is infinite. To do this it is enough to show that every rational number is algebraic. But if $a \in \mathbb{Q}$, then $a$ is a solution of the equation $x - a = 0$, so that $a$ is algebraic.

3. Suppose for contradiction that $\mathbb{R} - \mathbb{Q}$ were countable. We have that $\mathbb{R} = (\mathbb{R} - \mathbb{Q}) \cup (\mathbb{R} \cap \mathbb{Q})$. By Problem 2, we know that $\mathbb{R} \cap \mathbb{Q}$ is countable (as it is a subset of a countable set). Therefore, the set $\mathbb{R}$ is a union of two countable sets, and therefore countable. But we know that $\mathbb{R}$ is uncountable, which is a contradiction.

4. Suppose for contradiction that $S$ were countable. Then there would be a bijection $f : \mathbb{Z}^+ \to S$ (the set $S$ is clearly infinite). Let $f(n) = (a_1^n, a_2^n, \ldots)$. Define a new binary sequence $b = (b_1, b_2, \ldots)$, where $b_n = \begin{cases} 1 & a_n^n = 0 \\ 0 & a_n^n = 1 \end{cases}$. For any $n \in \mathbb{Z}^+$, we have that $b \neq f(n)$ because the $n^{th}$ terms of $b$ and $f(n)$ are not the same. Therefore, the sequence $b$ is not contained in the image of $f$, so $f$ is not surjective. This is a contradiction.

5. Suppose that $n$ can be written as $n = a^2 + b^2$, where $a, b \in \mathbb{Z}$. Then $a = 2k$ or $2k + 1$ and $b = 2m$ or $2m + 1$ for some integers $k$ and $m$. It follows that $a^2 + b^2$ has one of the forms $(2k)^2 + (2m)^2 = 4(k^2 + m^2)$, $(2k + 1)^2 + (2m)^2 = 4(k^2 + m^2 + k) + 1$, $(2k)^2 + (2m + 1)^2 = 4(k^2 + m^2 + m) + 1$, or $(2k + 1)^2 + (2m + 1)^2 = 4(k^2 + m^2 + k + m) + 2$. In any case, we have that $n$ is of the form $4q, 4q + 1$, or $4q + 2$ for some integer $q$. Since $1234567 = 4 \times 308641 + 3$, we conclude that $1234567$ cannot be written in the form $a^2 + b^2$ for integers $a$ and $b$. 
6. Suppose $5|a$. Then there exists $k \in \mathbb{Z}$ such that $a = 5k$. So $a^2 = 25k^2 = 5(5k^2)$ and $5|a^2$.

Suppose $5 \nmid a$. By the division theorem, $a$ has one of the forms $5k + 1, 5k + 2, 5k + 3$, or $5k + 4$ for some integer $k$. This means that $a^2$ has one of the forms
\[
(5k + 1)^2 = 5(5k^2 + 2k) + 1
\]
\[
(5k + 2)^2 = 5(5k^2 + 4k) + 4
\]
\[
(5k + 3)^2 = 5(5k^2 + 6k + 1) + 4, \text{ or}
\]
\[
(5k + 4)^2 = 5(5k^2 + 8k + 3) + 1.
\]
In any of these cases, the division theorem implies that $5 \nmid a^2$. 