Math 109, Fall 2017
Homework 9 Solutions

A. By a proposition in class, a set $A$ is enumerable $\iff$ ($A$ is infinite) and ($\exists g : \mathbb{N} \to A$ a surjection).

If $Y$ is finite, then $Y$ is countable by definition. Assume that $Y$ is infinite. We need to show that $Y$ is enumerable.

Since $X$ is enumerable, by definition this means that there exists a bijection $g : \mathbb{N} \to X$. Then $f \circ g : \mathbb{N} \to Y$ is a surjective function, because a composition of two surjective functions is surjective (see Exam 2 practice solutions, functions problem number 5(b) for a proof of this.)

Thus, by the proposition restated above, $Y$ is enumerable.

B. Let $A = \{f \mid f : \mathbb{N} \to \{0,1\}\}$. Suppose for contradiction that $A$ is countable. Then $A$ is either finite or enumerable. To see that $A$ is not finite, for $n \in \mathbb{N}$ define $f_n : \mathbb{N} \to \{0,1\}$ by

\[ f_n(m) = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases} \]

Then $f_n(n) \neq f_m(n)$ if $n \neq m$, showing that each natural number defines a different function in $A$, namely $f_n$. Since $\mathbb{N}$ is infinite, it follows that $A$ is also infinite (we constructed an injective function from $\mathbb{N} \to A$ given by $n \mapsto f_n$)

Since $A$ is not finite, it must be enumerable. This means we can write it as $A = \{g_1, g_2, \ldots\} = \{g_n \mid n \in \mathbb{N}\}$. (This is because if we have a bijection $g : \mathbb{N} \to A$, we can write $A = \{g(1), g(2), \ldots\}$.

We write $g_1$ for the function given by $g(1)$.

We will construct a function $F \in A$ such that $F \neq g_n$ for all $n \in \mathbb{N}$, which contradicts the claim that $A = \{g_n \mid n \in \mathbb{N}\}$. This is similar to the diagonalization argument for $\mathbb{R}$ being uncountable.

Define $F : \mathbb{N} \to \{0,1\}$ by $F(n) = \begin{cases} 1 & \text{if } g_n(n) = 0 \\ 0 & \text{if } g_n(n) = 1 \end{cases}$. Then for any $n \in \mathbb{N}$, $g_n(n) \neq F(n)$, so $F \neq g_n$. This contradicts that $A = \{g_n \mid n \in \mathbb{N}\}$, so it must be that $A$ was uncountable.

C. Problems IV

1. We prove by cases. Suppose that $n = a^2 + b^2$. For the first case, suppose that $a$ and $b$ are both even, so there exist $k, \ell \in \mathbb{Z}$ such that $a = 2k$ and $b = 2\ell$. Then $n = 4k^2 + 4\ell^2 = 4(k^2 + \ell^2)$ is of the form $4q$.

   For the second case, suppose one of $a$ and $b$ is even and the other is odd. Without loss of generality, we may assume that $a$ is even and $b$ is odd (else, swap the names of $a$ and $b$ to make this true). Let $k, \ell \in \mathbb{Z}$ be such that $a = 2k$ and $b = 2\ell + 1$. Then $n = a^2 + b^2 = 4k^2 + 4\ell^2 + 4\ell + 1 = 4(k^2 + \ell^2 + 1) + 1$ is of the form $4q + 1$.

   For the final case, suppose both are odd, and let $k, \ell \in \mathbb{Z}$ be such that $a = 2k + 1, b = 2\ell + 1$. Then $n = 4k^2 + 4k + 1 + 4\ell^2 + 4\ell + 1 = 4(k^2 + k + \ell^2 + \ell) + 1$ is of the form $4q + 2$.

   We see that in every case, we get a number of the form $4q, 4q + 1$, or $4q + 2$, as desired.

2. First, suppose that $5 \mid a$. Then there exists $k \in \mathbb{Z}$ such that $a = 5k$. Then $a^2 = 5(5k^2)$, so $5 \mid a^2$.

   For the other direction, we will prove by contrapositive. Suppose that $5 \nmid a$, and prove that $5 \nmid a^2$. By the division algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $a = 5q + r$ and $0 \leq r \leq 4$. Since $5 \nmid a$, $r \neq 0$. We prove this again by cases: $r = 1, 2, 3, \text{ or } 4$. 

1
Compute $a^2 = (5q + r)^2 = 25q^2 + 10qr + r^2$. If $r = 4$, then $a^2 = 25q^2 + 40q + 16 = 5(5q^2 + 8q + 3) + 1$ is of the form $5q + 1$. Since the remainder here $(+1)$ is not zero, this means $5 \nmid a^2$. The other cases are similar.

3. Assume for contradiction that $\exists q \in \mathbb{Q}$ such that $q^2 = 5$. Then by definition of $\mathbb{Q}$, there exist integers $a, b, b \neq 0$, such that $q = \frac{a}{b}$. We may assume that $\frac{a}{b}$ is in lowest terms, i.e. that $\gcd(a, b) = 1$.

Since $q^2 = 5$, this means that $a^2 = 5b^2$. Thus, $5 \mid a^2$, so by the previous problem, $5 \mid a$. By definition of divides, this means there exists $k \in \mathbb{Z}$ such that $a = 5k$. Then $(5k)^2 = 5b^2$, so $5k^2 = b^2$. Thus, $5 \mid b^2$, and so $5 \mid b$ by the previous problem. Then we have that $5 \mid a \land 5 \mid b$. This contradicts the fact that $\gcd(a, b) = 1$. Thus, no such $q$ can exist.