Math 319/320 Solutions to Homework 2

Problem 1. Show that the set $S_{\text{odd}}$ of odd (positive and negative) integers is denumerable by (a) enumerating them and (b) giving an explicit formula for the corresponding bijection $f : S_{\text{odd}} \to \mathbb{N}$.

(a) An enumeration: $S_{\text{odd}} = \{1, -1, 3, -3, 5, -5, \ldots \}$

(b) A bijection $f : S_{\text{odd}} \to \mathbb{N}$:

$$f(2k + 1) = 2k + 1, \ k \geq 0, \quad f(-2k + 1) = 2k + 2, \ k \geq 0.$$ 

Problem 2. (i) Show that for all $n \geq 1$ there is no injection of $\mathbb{N}_n$ onto a proper subset of $\mathbb{N}_n$.

Let’s prove this by induction. When $n = 1$ $\mathbb{N}_n = \{1\}$ has one element and there is only one map $f : \mathbb{N}_n \to \mathbb{N}_n$, namely the identity (which is bijective.)

Suppose this is true when $n = k$ and consider the case $n = k + 1$. Let $f : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ be injective but not surjective. We show below that we can always use $f$ to construct a new map $g : \mathbb{N}_k \to \mathbb{N}_k$ which is injective but not surjective. This contradicts the inductive hypothesis. Hence $f$ cannot exist.

To define $g$;

- case (i): $k + 1 \notin f(\mathbb{N}_{k+1})$. Then $f(j) < k + 1$ for all $j \leq k + 1$. Define $g : \mathbb{N}_k \to \mathbb{N}_k$ by setting $g(j) = f(j), j \in \mathbb{N}_k$. This is injective because $f$ is. I claim that the element $p := f(k + 1)$ is not in $g(\mathbb{N}_k)$. To see this, note that because $f$ is injective, there is only one element of $\mathbb{N}_{k+1}$, namely $k + 1$ itself, that is mapped to $p$ by $f$. Therefore $g^{-1}(p)$ is the empty set.

- case (ii): suppose that $k + 1 = f(j)$ for some $j \leq k + 1$. Then because $f$ is not surjective there is $p \leq k$ that is not in the image of $f$. Define a new map $F : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$ by setting:

$$F(i) = f(i), i \in \mathbb{N}_{k+1}, i \neq j, \quad F(j) = p.$$ 

Then $F$ is injective but not surjective because $k + 1 \notin F(\mathbb{N}_{k+1})$. Now construct $g$ from $F$ as in case (i).

(ii) Deduce from (i) that if $S$ is any finite set, there is no injection of $S$ onto a proper subset of $S$.

Suppose that $f : S \to S$ is an injection. Since $S$ is finite there is a positive integer $n$ and a bijection $g : \mathbb{N}_n \to S$. Then the composite $g^{-1} \circ f \circ g : \mathbb{N}_n \to \mathbb{N}_n$ is injective, since $g, f$ and $g^{-1}$ are. Therefore $g^{-1} \circ f \circ g$ is surjective by part (i). Therefore $f$ is surjective.

(iii) Show that (ii) does not hold for the infinite set $S = \mathbb{N}$.

Define $f : \mathbb{N} \to \mathbb{N}$ by $f(k) = k + 1$ for all $k$.

Problem 3. (i) The subsets of $\{1, 2\}$ are

$$\emptyset, \{1\}, \{2\}, \{1, 2\}.$$ 

The subsets of $\{1, 2, 3\}$ are

$$\emptyset, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}.$$ 

(iii) Prove that if a set $S$ has $n$ elements, then $\mathcal{P}(S)$ has $2^n$ elements.
If $S$ has one element then it has two subsets, the empty set and the set $S$. Thus $\mathcal{P}(S)$ has 2 elements.

Now suppose the statement is true for $n = k$ and consider a set $S$ with $k + 1$ elements. Suppose $x \in S$ and let $S_0 = S \setminus \{x\}$. Then $S_0$ has $k$ elements. Every subset of $S$ either lies in $S_0$ or contains $x$. By the inductive hypothesis there are $2^k$ subsets of $S_0$. Every subset $T$ of $S$ that contains $x$ corresponds to a unique subset $T_0$ of $S_0$, namely $T_0 = T \setminus \{x\}$. Moreover, given a subset $T_0$ of $S_0$ the subset $T = S_0 \cup \{x\}$ is a subset of $S$ containing $\{x\}$. Therefore there is a bijective correspondence between the subsets of $S_0$ and the subsets of $S$ that contain $x$. Hence there are $2^k$ subsets of this kind. So altogether $\mathcal{P}(S)$ has $2^k + 2^k = 2^{k+1}$ elements. Hence the statement holds for $n = k + 1$, and so holds for all $n$ by induction.

**Problem 4.** Prove that $\sqrt{3}$ is irrational.

Suppose that $\sqrt{3}$ is rational are write it as $p/q$ where $p, q$ are positive integers with no common divisor. Then $3 = p^2/q^2$, that is $3q^2 = p^2$. Therefore 3 divides $p^2$. We claim that 3 must divide $p$. If not, we may write $p = 3k + r$ for some integer $k$ and where $r = 1$ or 2. Then $p^2 = (3k + r)^2 = 9k^2 + 6kr + r^2$. Since 3 divides $p^2$, 3 must divide $r^2 = p^2 - 3(3k^2 + 2k)$. But $r^2$ is either 1 or 4. So this is impossible. Hence 3 divides $p$. Therefore $p = 3k$ and the equation $3q^2 = p^2 = 9k^2$ gives $q^2 = 3k^2$. Therefore 3 divides $q^2$. Arguing as above, it follows that 3 divides $q$. But this contradicts our assumption that $p$ and $q$ have no common divisor. Hence the original assumption was wrong: $\sqrt{3}$ cannot be rational.

**Problem 5.** Show that $a^2 + b^2 = 0$ iff $a = 0$ and $b = 0$.

If $a = 0 = b$ then $a^2 = 0 = b^2$, so $a^2 + b^2 = 0$.

Therefore we need to show the converse: if $a^2 + b^2 = 0$ then $a = 0 = b$. We will do this by proving the contrapositive. That is, if at least one of $a, b$ is nonzero then $a^2 + b^2 \neq 0$. (In fact in this case we will see that $a^2 + b^2 > 0$.)

To do this, suppose first that $a \neq 0$. Then either $a > 0$ or $-a > 0$ by the trichotomy rule (Def 2.1.5(iii)). If $a > 0$ then $a^2 > 0$ by Def 2.1.5(ii). Similarly, if $-a > 0$ then $(-a)^2 > 0$. Since $(-a)^2 = a^2$, we find that for any $a \neq 0 a^2 > 0$. Also, $a^2 \geq 0$ for all $a \in \mathbb{R}$.

Now suppose that at least one of $a, b$ is nonzero. By renaming them if necessary, we may suppose that $a \neq 0$. Then $a^2 > 0$ and $b^2 \geq 0$. Hence $a^2 + b^2 > 0$. (This follows from Def 2.1.5 (i) if $b^2 > 0$ and is obvious if $b^2 = 0$ since in this case $a^2 + b^2 = a^2 > 0$ by hypothesis.)

This completes the proof.

**Bonus Problem 6.** Show that if $S$ is a subset of $\mathbb{N}$ that is not contained in any of the sets $\mathbb{N}_n$ then $S$ is denumerable.

We will define a bijection $\mathbb{N} \to S$ using the principle of induction. The statement $P(n)$ is: there is an injection $f : \mathbb{N}_n \to S$ so that

i) $f(n) \geq n$, and

ii) if $s \in S$ is not in the image $f(\mathbb{N}_n)$ then $s > f(j)$ for all $j \in \mathbb{N}_n$.

By the well ordering principle $S$ has a smallest element, say $s_1$. Define $f(1) = s_1$. This map satisfies $P(1)$. Suppose by induction that $f$ is defined on $\mathbb{N}_k$ and satisfies (i), (ii) above. Set $f(k + 1)$ equal to the smallest element in the set $S \setminus f(\mathbb{N}_k)$. Then $f(k + 1)$ is larger that all the elements $f(j)$, $j \leq k$ by (ii). Hence $f(k + 1) > f(k) \geq k$ by (i). Hence $f(k + 1) \geq k + 1$. So (i) holds for $f$ on $\mathbb{N}_{k+1}$. Also because $f(k + 1)$ is the smallest element in $S \setminus f(\mathbb{N}_k)$, every element in $S \setminus f(\mathbb{N}_{k+1})$ is larger than every element in $f(\mathbb{N}_{k+1})$. So (ii) holds for $f$ on $\mathbb{N}_{k+1}$. 
Therefore we may define \( f : \mathbb{N}_n \to S \) satisfying (i) and (ii) for all \( n \).
It follows from (ii) and the inductive construction that
\[
f(1) < f(2) < f(3) < \ldots
\]
ie if \( i < j \) then \( f(i) < f(j) \). Hence \( f \) is injective. Suppose that \( f \) is not surjective and let \( s \in S \subset \mathbb{N} \) be not in its image. Consider properties (i) and (ii) in the case \( k = s \). By hypothesis \( s \) is not in the image \( f(\mathbb{N}_s) \). Therefore by (ii) \( s \) is strictly larger than all elements in the image \( f(\mathbb{N}_s) \). Hence \( s > f(s) \). But this contradicts (i).