Homework Assignment 1

Due: Friday, January 29

1. Let S and T be sets, and suppose that $T \subseteq S$. Describe the following sets, proving the correctness of your answers.
   (a) $T \cap S$.
   (b) $T \cup S$.
   (c) $T \cap (S \setminus T)$
   (d) $T \cup (S \setminus T)$.

2. Let S be a set with 3 elements (say {0,1,2}) and T be a set with 5 elements (say {a,b,c,d,e}).
   (a) Give an example of an injection $f : S \to T$.
   (b) Give an example of a surjection $g : T \to S$.
   (c) Can there be a bijection between S and T? Why or why not?

3. A subset $T \subset S$ is called a *proper subset* if $T \neq S$. This is often denoted $T \subsetneq S$. Give an example of a set S and a bijection between S and a *proper* subset of S.

4. Let S and T be two sets, and $f : S \to T$ a function between them.
   (a) Show that f is injective if and only if it has a left inverse.
   (b) Show that f is surjective if and only if it has a right inverse
   (c) Show that f is bijective if and only if it has an inverse.
   (d) Show that if f has a (two-sided) inverse, that inverse is unique.

   Remark. *Because of part (c) and (d) of the question 4, we see that if f is bijective, then f has a unique inverse, which we call the inverse of f and denote by f^{-1}.*

5. Let S and T be finite sets and suppose that $|S| = |T|$. Let $f : S \to T$ be a function. Prove that
$$f \text{ is injective } \Leftrightarrow f \text{ is surjective } \Leftrightarrow f \text{ is bijective.}$$

6. Show that equivalence relations are partitions are equivalent. Explicitly, let S be a set, construct a natural bijection between the partitions on S and the equivalence relations on S in the following way.
   (a) Let $\sim$ be an equivalence relation. Show that the equivalence classes of $\sim$ form a partition of S.
   (b) Conversely, let $\{X_i\}$ be a partition of S. Show that the relation $\sim$ given by the rule
$$x \sim y \text{ if } x, y \in X_i \text{ for the same } i$$
   is an equivalence relation for S.
   (c) Show that parts (a) and (b) give a bijection between the sets:
$$\{\text{Equivalence relations on } S\} \longleftrightarrow \{\text{Partitions of } S\}.$$
   (Hint: Part (a) gives a function from the left to the right. Part (b) gives a function from the right to the left. Show that these are inverses to eachother).

7. Let $a, b, c \in \mathbb{Z}$. Prove the following divisibility facts.
   (a) If $a|b$ and $a|c$ then $a|(b+c)$
   (b) If $a|b$ then $a|bc$.

8. In this exercise we prove the existence and uniqueness of division with remainder. Let $a, b \in \mathbb{Z}$, and suppose that $b \neq 0$. We start with existence.
   (a) We begin by considering the set of numbers $a - bq$ as q varies over the integers. Prove that the set
   $$S = \{a - bq : q \in \mathbb{Z}\},$$
   has at least one nonnegative element.
   (b) Let r be the minimal nonnegative element of S. Show that $0 \leq r < |b|$.
   (c) Use (b) to conclude that $a = bq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |b|$. This proves existence.
   (d) Show that the division with remainder from part (c) is unique. That is, suppose there are $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that
   $$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2.$$
   Suppose further that $0 \leq r_i < |b|$ for $i = 1, 2$. Then show $q_1 = q_2$ and $r_1 = r_2$.

9. In this exercise we prove the Euclidean algorithm works.
   (a) Suppose $a, b \in \mathbb{N}$ are two positive integers, and let $a = bq + r$ for $0 \leq r < b$ (as in the previous exercise). Show that:
   $$\gcd(a, b) = \gcd(b, r).$$
   (b) Let $a \neq 0$ be an integer. What is $\gcd(a, 0)$? Justify your answer.
   (c) Prove the correctness of the Euclidean algorithm. That is, suppose $a, b \in \mathbb{N}$ are two positive integers, and suppose you iterate the division algorithm as follows:
   $$\begin{array}{rcll} a &=& bq_0 + r_0 & 0 \leq r_0 < b \\ b &=& r_0 q_1 + r_1 & 0 \leq r_1 < r_0 \\ r_0 &=& r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\ &\vdots& & \\ r_{n-2} &=& r_{n-1} q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} &=& r_n q_{n+1}. & \end{array}$$
   Show that $\gcd(a, b) = r_n$.

10. Let d be the greatest common divisor of 792 and 275. Using Euclid's algorithm, find d and write $d = 792x + 275y$ for some x and y.