Math 412 Homework 1

Submission Instructions: You are responsible to read these instructions. Failure to submit correctly as described below will result in point deductions or loss of credit for entire problems. Submit these problems on Gradescope by Thursday, September 7th, at 11:59pm. Each problem should be on a separate page (or pages). **You will need to scan a PDF of the assignment AND select the pages belonging to each problem when you submit on gradescope.**

1. A **square** (respectively **cubic**) integer is an integer that factors as a^2 (respectively a^3) for $a \in \mathbb{Z}$.
   1. Prove that when a square integer is divided by 3, the remainder can never be 2.
   2. Prove that a cubic integer can be written in the form $9k, 9k+1$, or $9k-1$ for some $k \in \mathbb{Z}$.
2. Analogous to the idea of "greatest common divisor" is the idea of "least common multiple." The least common multiple of two (positive) integers, a and b, is the smallest (positive) integer m such that $a|m$ and $b|m$.
   (a) Use the well-ordering principle to prove that the least common multiple of two integers always exists.
   (b) Let $d = \gcd(a, b)$. Prove that there is some integer m such that $dm = ab$.
   (c) Prove that m from part (b) is a divisible by a and divisible by b.
   (d) Prove that for all integers M such that M is a common multiple of a and b, the number $m = \frac{ab}{\gcd(a,b)}$ (from parts b and c) divides M, making m the least common multiple. (Hint: prove that $\frac{M}{m}$ is an integer using Bezout's identity).
3. Let $a, b, c, d \in \mathbb{Z}$ such that the matrix
   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
   has an inverse whose entries are all integers. Let $x, y \in \mathbb{Z}$ such that at least one of them is not zero. Prove that $\gcd(x, y) = \gcd(ax + by, cx + dy)$.[1]
4. For any integer m, we can use the Fundamental Theorem of Arithmetic to write $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ where the p_i's are distinct primes in an (essentially) unique way. The natural number a_i is said to be the multiplicity of the prime p_i in m. [By convention, the multiplicity of p in m is 0 if p does not divide m.]
   1. Let d and n be positive integers. Prove that n is a d-th power of some other integer if and only if for every prime p, the multiplicity of p in n is divisible by d.
   2. Prove that if n is not a d-th power of some other integer, then $\sqrt[d]{n}$ is irrational. [Hint: try proof by contradiction.]
5. **We will see many equivalence relations in this course, and we will apply this problem many times during the semester**. Let X be a non-empty set, and let $\sim$ be an equivalence relation on the set X, that is, a rule used to compare pairs of elements of X which satisfies the following properties (we read "$a \sim b$" as "a is related to b"):

[1] How can we relate x and y with $ax + by$ and $cx + dy$ using the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$?

- $\sim$ is reflexive: $a \sim a$ for all $a \in X$.
- $\sim$ is symmetric: let $a, b \in X$ such that $a \sim b$. Then $b \sim a$.
- $\sim$ is transitive: let $a, b, c \in X$ such that $a \sim b$ and $b \sim c$. Then, $a \sim c$.

For example, before you start this problem note that the relation $=$ (being equal to) is an equivalence relation on any non-empty set X. However, the relation $\leq$ (being less or equal to) on the set $\mathbb{R}$ is not an equivalence relation, as it is not symmetric. Determine whether the following rules are equivalence relations on the given sets.

(a) Let X be $\mathbb{R}^2$, and $\sim$ is the rule

$$\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} w \\ z \end{bmatrix}$$

if $x - y = w - z$.

(b) Let X be the set of integers, $\mathbb{Z}$, and let $\sim$ be the rule

$$a \sim b$$

if $ab \geq 0$.

(c) Given an equivalence relation $\sim$ in X, we define the **equivalence class of** a (denoted by $[a]$) for all $a \in X$ as

$$[a] := \{x \in X \ : \ x \sim a\} \subseteq X.$$

Show that, for all $a \in X$, $[a] \neq \emptyset$.

(d) Let $a, b \in X$. Show that either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.[2] That is, prove that **equivalence classes are either disjoint or equal**.

(e) Let $\mathcal{S} := \{[a] \ : \ a \in X\}$ the set of all equivalence classes with respect to the relation $\sim$. Prove that

$$X = \bigsqcup_{Y \in \mathcal{S}} Y,$$

(the symbol $\sqcup$ means *disjoint union*). In other words, prove that **equivalence classes partition X into disjoint sets**.

[2]Hint: Suppose that $[a] \cap [b] \neq \emptyset$, that is, there exists $c \in X$ such that $c \in [a] \cap [b]$. Do you remember how to prove "or" statements?