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, January 25th, 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 $a \in \mathbb{Z}$.

   (a) Prove that when a square integer is divided by 3, the remainder can never be 2.

   (b) Prove that a cubic integer can be written in the form $9k, 9k+1$, or $9k-1$ for some $k \in \mathbb{Z}$.

(a) We know that $0 \leq r < 6$ by definition of the Division Algorithm. We notice that $2 \mid 6q+0, 6q+2$ and $6q+4$, and $3 \mid 6q+3$. Since p is a prime larger than 3, we know $2 \nmid p$ and $3 \nmid p$, so r can only possibly be 1 or 5. In fact, both of these values are possible (consider $p = 7$ or $p = 5$).

(b) Since $p \equiv 1$ or 5 mod 6 we have that $p^2 \equiv 1^2 \equiv 1 \bmod 6$ or $p^2 \equiv 5^2 \equiv 25 \equiv 1 \bmod 6$ as desired. Alternatively, notice that $p^2 - 1 = (p+1)(p-1)$ and at least one of these will be of the form $6n$ by the previous part, so $6 \mid p^2 - 1$ and $p^2 \equiv 1 \bmod 6$.

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.

The set of all positive numbers that are common multiples of a and b is a set of positive integers. Furthermore, it is nonempty, since it contains the element ab. Thus it must have a least element.

   (b) Let $d = \gcd(a, b)$. Prove that there is some integer m such that $dm = ab$.

Since $d = \gcd(a, b)$, d divides a, so there is some integer n such that $dn = a$. Thus $dnb = ab$, so nb is such an integer, m.

   (c) Prove that m from part (b) is a divisible by a and divisible by b.

Suppose that $dm = ab$. Then $m = \frac{a}{d}b$, and $\frac{a}{d}$ is an integer, because d divides a. Thus b divides m. Also, $m = a\frac{b}{d}$, and $\frac{b}{d}$ is an integer, since d divides b. Thus m is a multiple of a and a multiple of 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).

$$\frac{M}{m} = \frac{\gcd(a,b)}{ab}M$$

By Bezout's identity, there exists integers x and y such that $\gcd(a,b) = ax + by$. Thus

$$\begin{aligned}\frac{M}{m} &= \frac{M(ax+by)}{ab} \\ &= \frac{M}{b}x + \frac{M}{a}y\end{aligned}$$

By assumption, M is a multiple of b and M is a multiple of a, so the numbers $\frac{M}{b}$ and $\frac{M}{a}$ are integers. Thus $\frac{M}{b}x + \frac{M}{a}y$ is an integer, which means that $\frac{M}{m}$ is an integer. Therefore, $m|M$.

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]

Let's first prove a lemma.

Let A be a 2x2 matrix with $\mathbb{Z}$-coefficients:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Let v be a 2D column vector **with integer entries** denoted by x and y respectively. Define the gcd of such a column vector to be just $\gcd(x,y)$.

Lemma. $\gcd(v) | \gcd(A \cdot v)$.

Proof. We have $A \cdot v$ has 1st-coordinate $ax+by$ and 2nd-coordinate $cx+dy$. So any divisor of x and y is also a divisor of both coordinates of $A \cdot v$. □

We complete the proof by applying the Lemma twice.

$$\gcd(x,y) | \gcd(A \cdot v) = \gcd(ax+by, cx+dy) \qquad \text{(by applying the Lemma)}$$
$$\gcd(A \cdot v) | \gcd(A^{-1} \cdot A \cdot v) = \gcd(x,y) \qquad \text{(applying the Lemma again)}$$

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

(a) 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.

(b) 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.]

1.
$$\begin{aligned}\binom{n-1}{d}+\binom{n-1}{d-1} &= \frac{(n-1)!}{(n-1-d)!d!}+\frac{(n-1)!}{(n-1-(d-1))!(d-1)!}\\ &= \frac{(n-1)!}{(n-1-d)!d!}+\frac{(n-1)!}{(n-d)!(d-1)!}\\ &= \frac{(n-1)!\cdot(n-1-d)}{(n-d)!d!}+\frac{(n-1)!\cdot d}{(n-d))!d!}\\ &= \frac{(n-1)!\cdot((n-d)+d)}{(n-d))!d!}\\ &= \frac{(n-1)!\cdot n}{(n-d))!d!}\\ &= \binom{n}{d}.\end{aligned}$$

2. First, note that for any n, $\binom{n}{0}=\frac{n!}{n!0!}=1$ is also an integer, and so is $\binom{n}{n}=\frac{n!}{n!0!}=1$. We will use induction on n; note that by our conditions, our statement is about $n\geqslant 2$. When $n=2$, the only d that remains is $d=1$; $\binom{2}{1}=\frac{2!}{1!1!}=2$, which is an integer. Now suppose that we have a fixed value of $n\geqslant 2$ for which we have already shown $\binom{n}{d}$ us an integer for all $0\leqslant d\leqslant n$. Now consider $n+1$, and fix any $0\leqslant d\leqslant n+1$.We have already done the cases $d=0$ and $d=n+1$, so we might as well assume $1\leqslant d<n+1$. By part (a),
$$\binom{n+1}{d}=\binom{n}{d}+\binom{n}{d-1}$$
By induction hypothesis, $\binom{n}{d}$ and $\binom{n}{d-1}$ are both integers; their sum must also be an integer.

3. We have shown that $\binom{p}{d}$ is an integer. On the other hand, $\binom{p}{d}=\frac{p!}{d!(p-d)!}$. By the Fundamental Theorem of Arithmetic, we can write $p!=q_1\cdots q_s$ as a product of primes, and p appears as one of the q_i's. We observe that $d!$ and $(n-d)!$ are products of integers that are all smaller than p. Each of the prime factors of these terms must be smaller than p, so p cannot be a prime factor of either $d!$ or $(n-d)!$. Now, $p|p!=\binom{p}{d}\cdot d!\cdot(n-d)!$. By a property of primes from the worksheet, we must have that $p|\binom{p}{d}$.

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"):

- $\sim$ 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 $x - y = w - z$.

This is an equivalence relation!

Reflexive: Note that $\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} x \\ y \end{bmatrix}$ for all $x, y \in \mathbb{R}$, because $x - y = x - y$.

Symmetric: Suppose $\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} w \\ z \end{bmatrix}$. Then by definition, $x-y = w-z$, so $w-z = x-y$, so $\begin{bmatrix} w \\ z \end{bmatrix} \sim \begin{bmatrix} x \\ y \end{bmatrix}$.

Transitive: Suppose $\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} w \\ z \end{bmatrix}$ and $\begin{bmatrix} w \\ z \end{bmatrix} \sim \begin{bmatrix} u \\ v \end{bmatrix}$. Then by definition, $x - y = w - z$ and $w - z = u - v$, so $x - y = u - v$, which gives that $\begin{bmatrix} x \\ y \end{bmatrix} \sim \begin{bmatrix} u \\ v \end{bmatrix}$

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

$$a \sim b$$

if $ab \geq 0$.

This is NOT an equivalence relation, because of 0! It is reflexive and symmetric, but not quite transitive. Note that $0(-1) \geq 0$, so $0 \sim -1$. However, $0 \cdot 1 \geq 0$, so $0 \sim 1$ as well. However, $1 \cdot -1 < 0$, so $1 \not\sim -1$.

(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 $a \in X$, $[a] \neq \emptyset$.

$a \in [a]$!

(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**.

[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?

Suppose that $[a] \cap [b] \neq \emptyset$. Then there exists a $c \in [a] \cap [b]$, that is, $c \in [a]$ and $c \in [b]$. By definition of equivalence class, this means that $c \sim a$ and $c \sim b$. But using the symmetric and transitive properties, that implies that $a \sim b$.
Thus if $x \in [a]$, then $x \sim a$ so $x \sim b$ by transitivity, so $x \in [b]$. Thus $[a] \subseteq [b]$. Similarly, if $x \in [b]$, then $x \sim b$ so $x \sim a$, so $x \in [a]$. Thus $[b] \subseteq [a]$, showing that $[a] = [b]$.

(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**.

The fact that $\sqcup_{Y \in \mathcal{S}} Y$ is disjoint was already shown in part d. Hence all we really need to show is $X = \cup_{Y \in \mathcal{S}} Y$.
The fact that $\cup_{Y \in \mathcal{S}} Y \subseteq X$ follows from the definition of $\mathcal{S}$.
On the other hand, if $x \in X$, then $x \in [x]$ and $[x] \in \mathcal{S}$. This finishes the proof.