Math 412 Homework 2

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, February 1st, 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. Fix two positive integers m, n where m and n are relatively prime (meaning $\gcd(m, n) = 1$). Consider the system of congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \tag{$\clubsuit$}$$

where a and b are arbitrary integers.

   (a) Prove that if $rm + sn = 1$, then $x = asn + brm$ is a solution to system $\clubsuit$.

   (b) Prove that $\clubsuit$ has a solution for all choices of a and b.

   (c) Fix a solution x_1 to system $\clubsuit$. Show that every element in $[x_1]_{mn}$ is a solution to system $\clubsuit$.

   (d) Fix a solution x_1 to system $\clubsuit$. Show the set of all solutions to $\clubsuit$ is exactly $[x_1]_{mn}$.
   Hint: use the fundamental theorem of arithmetic to show that if two relatively prime integers divides some integer, then so does their product.]

   (e) Find **all** integer solutions $x \in \mathbb{Z}$ to the system $\{x \equiv 11 \pmod{72},\quad x \equiv 30 \pmod{169}.\}$

2. When we define a function on $\mathbb{Z}_n$, we need to check that it is well-defined; many possible "rules" we could think to assign are not well-defined.

   (a) Is the assignment

$$\begin{tikzcd} \mathbb{Z}_3 \arrow[r] & \mathbb{Z}_6 \\ {[a]_3} \arrow[r, mapsto] & {[a]_6} \end{tikzcd}$$

   a well-defined function?

   (b) Is the assignment

$$\begin{tikzcd} \mathbb{Z}_6 \arrow[r] & \mathbb{Z}_3 \\ {[a]_6} \arrow[r, mapsto] & {[a]_3} \end{tikzcd}$$

   a well-defined function?

   (c) Show that if $n|m$ then the rule

$$\begin{tikzcd} \mathbb{Z}_m \arrow[r] & \mathbb{Z}_n \\ {[a]_m} \arrow[r, mapsto] & {[a]_n} \end{tikzcd}$$

   is a well-defined function.

   (d) Show that if $n \nmid m$ then the rule

$$\begin{tikzcd} \mathbb{Z}_m \arrow[r] & \mathbb{Z}_n \\ {[a]_m} \arrow[r, mapsto] & {[a]_n} \end{tikzcd}$$

   is *not* a well-defined function.

3. Let n and a be a positive integers, let $d = (a, n)$ be the gcd of a and n, and let $b \in \mathbb{Z}$. Consider the equation

$$[a]_n y = [b]_n. \qquad (\star)$$

   (a) Prove that if d does not divide b, then the equation $\star$ has no solutions $y \in \mathbb{Z}_n$.

   (b) Assume $b = 0$. Show that $y = [x]_n$ is a solution to $\star$ if and only if x is multiple of $\frac{n}{d}$. Conclude that the equation $\star$ has exactly d solutions $y \in \mathbb{Z}_n$, given by the elements

$$[0]_n, \left[\frac{n}{d}\right]_n, \left[2 \cdot \frac{n}{d}\right]_n, \ldots, \left[(d-1) \cdot \frac{n}{d}\right]_n.$$

   Hint: It may be useful to use Theorem 1.4 of the textbook, which says that if $u, v, w \in \mathbb{Z}$, $(u, v) = 1$, and $u|vw$, then $u|w$.

   (c) Assume d divides b. Write $ra + sn = d$ for some integers $r, s \in \mathbb{Z}$. (Why is this possible?) Show that $\left[r\frac{b}{d}\right]_n$ is a solution to $\star$.

   (d) Assume d divides b. By (c) we can fix a solution $y_1 \in \mathbb{Z}_n$ to $\star$. Show that $y \in \mathbb{Z}_n$ is a solution to $\star$ if and only if $z = y - y_1 \in \mathbb{Z}_n$ is a solution to the equation

$$[a]_n z = 0.$$

   Conclude that the number of solutions to $\star$ is the same as the number of solutions to $[a]_n z = 0$, and hence by (b) there are exactly d solutions to $\star$.

4. Recall the notion of *equivalence relation* from the worksheet on Congruence in $\mathbb{Z}$, or look it up in Appendix B of the text.

   Consider a function $f : X \longrightarrow Y$ between two sets X and Y. We define a relation $\sim$ on X by saying $x \sim x'$ if $f(x) = f(x')$.

   (a) Show that $\sim$ is an equivalence relation.

   (b) Find a bijection between the equivalence classes on X and the image of f. Notice that this gives a partition of X.

   (c) Prove that the equivalence relation on $\mathbb{Z}$ given by congruences modulo a fixed n is a particular case of the equivalence $\sim$ above: i.e., find a function f. This gives a partition of $\mathbb{Z}$; what are the equivalence classes?