Homework #2

Problems to hand in on Thursday, January 31, in the beginning of class. Write your answers out carefully, staple pages, and write your name and section number on each page.

1) 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
   $$\begin{aligned} \mathbb{Z}_3 &\longrightarrow \mathbb{Z}_6 \\ [a]_3 &\longmapsto [a]_6 \end{aligned}$$
   a well-defined function?

   (b) Is the assignment
   $$\begin{aligned} \mathbb{Z}_6 &\longrightarrow \mathbb{Z}_3 \\ [a]_6 &\longmapsto [a]_3 \end{aligned}$$
   a well-defined function?

   (c) Show that if $n|m$ then the rule
   $$\begin{aligned} \mathbb{Z}_m &\longrightarrow \mathbb{Z}_n \\ [a]_m &\longmapsto [a]_n \end{aligned}$$
   is a well-defined function.

   (d) Show that if $n \nmid m$ then the rule
   $$\begin{aligned} \mathbb{Z}_m &\longrightarrow \mathbb{Z}_n \\ [a]_m &\longmapsto [a]_n \end{aligned}$$
   is *not* a well-defined function.

2) Fix two positive integers m, n where m and n are relatively prime (meaning $\gcd(m, n) = 1$). Consider the system of congruences
   $$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \qquad (\clubsuit)$$
   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 $\{x \equiv 7 \pmod{20},\quad x \equiv 11 \pmod{97}.\}$

3) 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?