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.

Solution.

(a) No! $[0]_3 = [3]_3$, but the rule maps these to $[0]_6 \neq [3]_6$.

(b) Yes! If $[a]_6 = [b]_6$, then $6|(a-b)$. Consequently, $3|(a-b)$, and $[a]_3 = [b]_3$, as required.

(c) If $[a]_m = [b]_m$, then $m|(a-b)$. Consequently, $n|(a-b)$, since $n|m$. We then have $[a]_n = [b]_n$, as required.

(d) Consider $[0]_m = [m]_m$. By hypothesis, $n \nmid m = (m-0)$, so $[0]_n \neq [m]_n$. This means that the map is not well-defined.

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

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

where a and b are arbitrary integers.

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

(b) Prove that ♣ has a solution for all choices of a and b.

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

(d) Fix a solution x_1 to system ♣. Show the set of all solutions to ♣ 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 $\{x \equiv 7 \pmod{20},\quad x \equiv 11 \pmod{97}.\}$

Solution.

(a) We just need to check $asn + brm \mod m = asn \mod m = a(1 - rm) \mod m = a \mod m$. Similarly, $asn + brm \mod n = b \mod n$.

(b) This follows from 1, since if m and n are relatively prime, then we can write 1 as a $\mathbb{Z}$-linear combination.

(c) Any arbitrary element of $[x_1]_{mn}$ can be written $x_1 + mnk$. Note that $x_1 + mnk \mod m = x_1 \mod m$ for any $k \in \mathbb{Z}$; also $x_1 + mnk \mod n = x_1 \mod n$ for any $k \in \mathbb{Z}$. So every element in $[x_1]_{mn}$ is a solution if x_1 is.

(d) Since x_1 is a solution, we can write $x_1 = a + mk_1 = b + nk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Suppose that y is a solution. So $y = a + mr_1$ and $y = b + nr_2$ for some $r_1, r_2 \in \mathbb{Z}$. This means that $x_1 - y = m(k_1 - r_1) = n(k_2 - r_2)$. So $x_1 - y$ is divisible by both m and n. So all the primes appearing in a prime factorization of m must appear in $x_1 - y$ and likewise all the primes appearing in a prime factorization of n must appear in $x_1 - y$; since m and n have no primes in common, we have all primes of both m and n appear in the prime factorization of $x_1 - y$, so that mn divides $x_1 - y$.

(e) We first use the reverse-engineered Euclidean algorithm to write $1 = -7 \cdot 97 + 34 \cdot 20$. So one solution is $x = 7 \cdot -7 \cdot 97 + 11 \cdot 34 \cdot 20$. So the set of all solutions is $[7 \cdot -7 \cdot 97 + 11 \cdot 34 \cdot 20]_{97\times 20}$, or $[2727]_{1940}$.

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?

Solution.

(a) We need to show this is reflexive, symmetric, and transitive.

$\sim$ is reflexive: $f(x) = f(x)$, so $x \sim x$.

$\sim$ is symmetric: If $x \sim y$, then $f(x) = f(y)$. Then $f(xy) = f(x)$, so $y \sim x$.

$\sim$ is transitive: If $x \sim y$ and $y \sim z$, then $f(x) = f(y)$ and $f(y) = f(z)$. Then $f(x) = f(z)$, so $x \sim z$.

(b) We claim that the map $\bar{f}$ sending $[x] \mapsto f(x)$ gives a bijection between the equivalence classes of $\sim$ and the image of f. First, this is a well-defined function from $\{\text{equivalence classes of } \sim\}$ to image(f), since if $[x] = [x']$, then $f(x) = f(x')$, so they map to the same thing.

To see this is bijective, we construct an inverse, which we will call g. For $y \in \text{image}(f) \subseteq Y$, write $y = f(x)$ for some $x \in X$, which we can do since $z \in \text{image}(f)$, and define $g(y) = [x]$. This depended on the *choice* of some x such that $y = f(x)$, so we need to show that if we choose two different such x's, we get the same value. Suppose that $f(x) = f(x') = y$. Then, by definition, $x \sim x'$, so $[x] = [x']$. Thus, $g(y)$ returns the same class $[x] = [x']$, no matter which preimage of y we chose. That is, g is a function from image(f) to $\{\text{equivalence classes of } \sim\}$.

Now, $\bar{f}$ and g are inverse functions. Indeed, given $[x]$, let $f(x) = y$. We have $g(\bar{f}([x])) = g(y) = [x]$. Given y in the image of f, write $y = f(x)$, and then $\bar{f}(g(y)) = \bar{f}([x]) = y$.

(c) Let f be the function sending an integer to its remainder when you divide by n: this is the function we seek. The equivalence classes are just congruence classes modulo n.