QUIZ 3

CS 198-087: INTRODUCTION TO MATHEMATICAL THINKING
UC BERKELEY EECS
SPRING 2019

This quiz is due on Sunday, March 17th, at 11:59PM, on Gradescope. This quiz is open-book and open-note, but no collaboration is allowed.

Note: There are 24 possible points on the quiz, but the quiz will be scored out of 20.

---

1. *Existence of Inverses (Points: 2 + 3 = 5)*

   a. Does 5 have an inverse in mod 10? Why or why not?

   b. Determine the number of solutions to $5x \equiv 5 \pmod{10}$. *(Hint: Since we're working in mod* 10*, the maximum number of solutions is 10.)*

> **Solution:**
>
> a. $\boxed{\text{No}}$, because $\gcd(5, 10) = 2 \neq 1$, and we require $\gcd(a, m) = 1$ for an inverse to exist.
>
> b. We can represent the equivalence $5x \equiv 5 \pmod{10}$ using the equation $5x + 5 = 10k$, or $x + 1 = 2k$, for some integer k.
>
> Now, we just need all x in the set $\{0, 1, 2, ...9\}$ that satisfy $x + 1 = 2k$ — in other words, the x in this set that are odd. This is just $x = 1, x = 3, x = 5, x = 7, x = 9$, and therefore there are $\boxed{5}$ solutions. *(Note: One could also arrive at this result by directly substituting each of* $\{0, 1, 2, ...9\}$ *into the original equivalence.)*

2. *Modular Arithmetic Mechanics (Points: 5 + 5 = 10)*

   In both parts, you will need to show all of your work in order to receive credit. Solutions that just state the answer will not receive any credit.

   a. Determine $14^{93} \pmod{73}$.

   b. Determine $14^{-1} \pmod{73}$.

> **Solution:**

a. Since 73 is prime, we can use Fermat's Little Theorem to see that $14^{73} \equiv 14 \pmod{73}$. Since $93 = 73 + 20$, we have $14^{93} = 14^{73} \cdot 14^{20}$. Now, we only need to compute 14^{20}.

We can do this using repeated squaring.

$$\begin{aligned}
14^1 &\equiv 14 \pmod{73} \\
14^2 &\equiv 196 \equiv 50 \pmod{73} \\
14^4 &\equiv 50^2 \equiv 2500 \equiv 18 \pmod{73} \\
14^8 &\equiv 18^2 \equiv 324 \equiv 32 \pmod{73} \\
14^{16} &\equiv 32^2 \equiv 1024 \equiv 2 \pmod{73}
\end{aligned}$$

Then, since $20 = 16 + 4$, we have

$$\begin{aligned}
14^{93} &\equiv 14^{73} \cdot 14^{16} \cdot 14^4 \pmod{73} \\
&\equiv 14 \cdot 2 \cdot 18 \pmod{73} \\
&\equiv 504 \pmod{73} \\
&\equiv 66 \pmod{73}
\end{aligned}$$

Therefore, we have $14^{93} \equiv \boxed{66} \pmod{73}$.

b. First, we know an inverse exists since $\gcd(14, 73) = 1$.

Let's look at the calls we'd make to the Euclidean Algorithm:

$$\gcd(73, 14) = \gcd(14, 3) = \gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0)$$

Now, using the Division Algorithm, we can state

$$\begin{aligned}
73 = 14 \cdot 5 + 3 &\implies 3 = 73 - 14 \cdot 5 \\
14 = 3 \cdot 4 + 2 &\implies 2 = 14 - 3 \cdot 4 \\
3 = 2 \cdot 1 + 1 &\implies 1 = 3 - 2 \cdot 1
\end{aligned}$$

Now, substituting into the last equation:

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (14 - 3 \cdot 4) \cdot 1 = 3 \cdot 5 - 14 \\
&= (73 - 14 \cdot 5) \cdot 5 - 14 \\
&= 73 \cdot 5 - 14 \cdot 26
\end{aligned}$$

Since we can state $73 \cdot 5 + 14 \cdot (-26) = 1$, we have that -26 is the inverse of 14 in modulo 73. However, we need to re-write -26 as a number in the range $[0, 72]$: we can do so by adding 73, giving us $\boxed{47}$.

3. *Functions in Modular Arithmetic (Points: 3 + 3 + 3 = 9)*

Recall, Z_n refers to the set of integers modulo n. In each each of the following, assume that we take mod n after the operation, if Z_n is the codomain of the function.

a. Is $f(x) = 7x$ a bijection from Z_{12} to Z_{12}? Justify your answer.

b. Is $f(x) = 6x$ a bijection from Z_{12} to Z_{24}? Justify your answer.

c. Does there exist an surjection from Z_{12} to Z_{24}? If so, identify one. If not, explain why.

Solution:

a. $\boxed{\text{Yes}}$, because 7 has an inverse in modulo 12. This is important, because inverses are unique, and no two un-equal elements have the same inverse. Therefore, there is a unique solution to $7x \equiv c$ for each $c = 0, 1, ..., 11$.

However, to be sure, we can enumerate all possible values in the input (as many students did):

$$
\begin{aligned}
7 \cdot 0 &\equiv 0 \pmod{12} \\
7 \cdot 1 &\equiv 7 \pmod{12} \\
7 \cdot 2 \equiv 14 &\equiv 2 \pmod{12} \\
7 \cdot 3 \equiv 21 &\equiv 9 \pmod{12} \\
7 \cdot 4 \equiv 28 &\equiv 4 \pmod{12} \\
7 \cdot 5 \equiv 35 &\equiv 11 \pmod{12} \\
7 \cdot 6 \equiv 42 &\equiv 6 \pmod{12} \\
7 \cdot 7 \equiv 49 &\equiv 1 \pmod{12} \\
7 \cdot 8 \equiv 56 &\equiv 8 \pmod{12} \\
7 \cdot 9 \equiv 63 &\equiv 3 \pmod{12} \\
7 \cdot 10 \equiv 70 &\equiv 10 \pmod{12} \\
7 \cdot 11 \equiv 77 &\equiv 5 \pmod{12}
\end{aligned}
$$

We've seen all elements in Z_{12} as an output exactly once, and therefore this function is a bijection.

(Note: Consider $f(x) = 6x$ with the same domain and codomain. You will see that it is not a bijection, and that's because $\gcd(6, 12) \neq 1$.)

b. $\boxed{\text{No}}$. We can see this by looking at $f(4)$ and $f(8)$: both map to 0, meaning that f is not an injection (and thus can't be a bijection). In general, in order for there to be a bijection between a set with domain A and codomain B, we require $|A| = |B|$. However, $|Z_{12}| \neq |Z_{24}|$, and thus it is impossible for *any* bijection to exist between the two sets.

c. $\boxed{\text{No}}$. As we identified earlier in the course, in order for a surjection to exist, there must be a pre-image for every element in the codomain (i.e. an element in the domain for each element in the codomain). However, there are 24 elements in the codomain, and since (for a function) each element in the domain can only point to one element in the codomain, such a surjection is not possible.

Put more succinctly, for a surjection to exist $A \to B$, we must have $|A| \geq |B|$. However, $|Z_{12}| < |Z_{24}|$, and thus no surjection exists between the two sets.