MATH 120A Prep: Modular Arithmetic

Facts to Know:

Fix a positive integer n. Then $x \sim y$ if $n|(x-y)$ is an equivalence relation on $\mathbb{Z}$. The quotient set of equivalence classes is the set:

$$\mathbb{Z}_n = \{[x] : x \in \mathbb{Z}\}$$
$$= \{[0], [1], [2], \ldots, [n-1]\}$$

Operations on $\mathbb{Z}_n$:

$\mathbb{Z}_5$:

- Addition: $[a]+[b] = [a+b]$ $\quad [2]+[4] = [6] = [1]$
- Multiplication: $[a]\cdot[b] = [ab]$ $\quad [7]+[9] = [16] = [1]$

$[2]\cdot[3] = [6] = [1]$

Well-Defined Operations: Show that different choices of representative don't affect the output of the function. If $f : \mathbb{Z}_n \to X$ we want to show that

if $[a]=[b]$ then $f([a]) = f([b])$.

Examples:

1. List the elements of $\mathbb{Z}_4$ and create an addition and multiplication table.

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0] = [4]
[2]	[2]	[3]	[0]	[1] = [5]
[3]	[3]	[0]	[1]	[2] = [6]

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

2. Show that the function $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $f([a]) = [a^2]$ is well-defined. Is it a bijection?

Well-defined: Suppose $[a]=[b]$, want to show $f([a])=f([b])$ or $[a^2]=[b^2]$.

$[a]=[b]$ means $a \sim b$ so $5 \mid b-a$

$[a^2]=[b^2]$ means $a^2 \sim b^2$ so $5 \mid b^2-a^2$.

$b^2-a^2 = (b-a)(b+a)$ and $5 \mid b-a$ so $5 \mid b^2-a^2$. ✓

$f([0]) = [0^2] = [0]$ $\quad$ $f([2]) = [2^2] = [4]$ $\quad$ $f([4]) = [4^2] = [16] = [1]$

$f([1]) = [1^2] = [1]$ $\quad$ $f([3]) = [3^2] = [9] = [4]$

Not a bijection.

3. Let $[a]_n$ denote the equivalence class of a in $\mathbb{Z}_n$. Prove that the map $g : \mathbb{Z}_3 \to \mathbb{Z}_6$ defined by $g([a]_3) = [2a]_6$ is well-defined and injective but not surjective. Is $g([a]_3) = [3a]_6$ well-defined?

$[a]_3$ is equivalence class of a in $\mathbb{Z}_3$.
$[a]_6$ is equivalence class of a in $\mathbb{Z}_6$.

$g: \mathbb{Z}_3 \to \mathbb{Z}_6 \quad g([a]_3) = [2a]_6$

If $[a]_3 = [b]_3$ then need $[2a]_6 = [2b]_6$.

$[a]_3 = [b]_3$ means $a \sim b$ in $\mathbb{Z}_3$ so $3 \mid b-a$

To show $[2a]_6 = [2b]_6$ we need $6 \mid 2b-2a$

$2b-2a = 2(b-a)$ so $6 \mid 2b-2a$ so $[2a]_6 = [2b]_6$. ✓

2 · 3 divides

$g([0]_3) = [2\cdot 0]_6 = [0]_6$
$g([1]_3) = [2\cdot 1]_6 = [2]_6$
$g([2]_3) = [2\cdot 2]_6 = [4]_6$

these are all different so injective.

$[1]_6, [3]_6, [5]_6$ don't show up so not surjective.

$h([a]_3) = [3a]_6$ $\quad$ not well-defined.

$[0]_3 = [3]_3$ but $h([0]_3) = [3\cdot 0]_6 = [0]_6 \neq [3]_6 = [9]_6 = [3\cdot 3]_6 = h([3]_3)$ in $\mathbb{Z}_6$