Mod numbers are actually sets of integers, In order to be a function on mod numbers, every number in the equivalence class set of a mod number has to be mapped to the same place.


The strategy for showing a function is 1-to-1 is very similar to the strategy for showing that a potential function is a function:

To show 1-to-1
suppose $a, b \in$ domain
s.t $f(a)=f(b)$


So $f$ is $1-t_{0}-1$
to show it's a function:
Suppose $a, b \in$ domain
so $f$ is a function

Here we used that strategy to prove that our first example potential function is really a function.

This is how we show $f$ is a function.
Suppose $[a], b] \in \mathbb{Z}_{4}$ Such that $[a]=[b]$

$$
[a]_{4}=[b]_{4}
$$

so $a=[n+\pi \cdot 4$ and $b=[n][k, 4$ where $n, 1, k \in \mathbb{Z}$

$$
\begin{aligned}
& \text { so } a=n(a)=[2(n+4 j)]_{8}=[2 n+8 y]_{8}=[2 n]_{8}+[88]_{8}=[2 n]_{8}+[0]_{8} \\
& f(b)=[2(n+4 k)]_{8}=[2 n+8 k]_{8}=[2 n]_{8}+[8 k]_{8}=[2 n]_{8}+[0]_{8}
\end{aligned}
$$

So $f(a)=f(b)$
so $f$ is a function.

If it's not a function, this is what happens:

try $f\left([n+4 j]=[2 n+8 j]_{10}=\right.$

$$
f([n+4 k])=[2 n+8 k]_{10}=[2 n]_{10}+[8 k]_{10}+\left(\begin{array}{l}
1 \\
j
\end{array}\right]_{10}^{\prime}
$$

for example $[0]_{4}=[4]_{4}$

$$
\begin{aligned}
& f\left([0]_{4}\right)=[0]_{10} \\
& f\left([4]_{4}\right)=[8]_{10}
\end{aligned}
$$

not equal
not a function

Here's most of a proof that something is an isomorphism:
This is the definition of the relation we will prove is a function:


Recall from earlier that $7^{2} \equiv 9(\bmod 20), \quad 7^{3} \equiv 3(\bmod 20), \quad 7^{4} \equiv 1 \quad(\bmod 20)$

Here we prove it's a function:


Here we prove this function is 1-to-1


Here we prove it is a homomorphism:


To prove it is onto, we would say:
Let $[a]_{20} \in<7>\subseteq U_{20}$
So [a]=[7] for some $n \in \mathbb{Z}$
Then $[n]_{4} \in \mathbb{Z}_{4}$ and $f\left([n]_{4}\right\}=[7]_{20}^{n}=[a]$
so $f$ is onto, and hence $f$ is an isomorphism of groups.

The homework is:
WW
due Weds

$$
7.4 * 5,6,11,13
$$

and problem:

$$
\begin{gathered}
\text { Prove } f: \mathbb{Z}_{q} \rightarrow \mathbb{Z}_{10} \text { define } a \text { by } \\
\{(x)=2 x \\
\text { is not a function }
\end{gathered}
$$

