MHF3202
Challenge Problem

Oliver Deng

April 8, 2025

Lemma 0.0.1 Given a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$, it is injective if and only if it is surjective.

Let f be a function that maps from $\mathbb{Z}_n$ to $\mathbb{Z}_n$.

First we prove that if f is injective, then it is surjective.
To that end, assume by way of contradiction that f is injective and not surjective.
Observe that since f is injective and our domain is $\mathbb{Z}_n$, f maps $|\mathbb{Z}_n|$ distinct elements to $|\mathbb{Z}_n|$ distinct elements.
Thus, its domain is of the same cardinality as its codomain, i.e. $|\mathbb{Z}_n| = |\mathbb{Z}_n|$.
However, since f is not surjective, $|\mathbb{Z}_n| < |\mathbb{Z}_n|$ by the pigeonhole principle, which is a contradiction.

Now we prove that if f is surjective, then it is injective.
To that end, assume by way of contradiction that f is surjective and not injective.
Observe that since f is surjective and our domain is $\mathbb{Z}_n$, f maps $|\mathbb{Z}_n|$ distinct elements to $|\mathbb{Z}_n|$ distinct elements.
Thus, its domain is of the same cardinality as its codomain, i.e. $|\mathbb{Z}_n| = |\mathbb{Z}_n|$.
However, since f is not injective, $|\mathbb{Z}_n| > |\mathbb{Z}_n|$ by the pigeonhole principle, which is a contradiction.

So a function f is injective if and only if it is surjective.

Theorem 0.0.1 Given the function $f([x]) = 3[x]$, $f : \mathbb{Z}_n \to \mathbb{Z}_n$, if $3 \mid n$, then f is neither injective nor surjective.

Proof: Let f be the function as given and let $3 \mid n$.
We want to show that f is not injective.
Observe that $f([0]) = 3[0] = [3 \cdot 0] = [0]$.
Also, $n = 3k$ for some $k \in \mathbb{Z}$ by definition of divisibility.
Observe that $f([k]) = 3[k] = [3k] = [n] = [0]$ under $\mathbb{Z}_n$.
Note that $k \neq 0$ since $n > 0$.
Thus, we can observe that $0 < k < n$, so $[0] \neq [k]$ under $\mathbb{Z}_n$ since k cannot be a representative of $[0]$
Since $[0] \neq [k]$ and we have that $f([0]) = f([k])$, f is not injective, and by lemma 0.0.1, f is also not surjective. 😊

Theorem 0.0.2 Given the function $f([x]) = 3[x]$, $f : \mathbb{Z}_n \to \mathbb{Z}_n$, if $3 \nmid n$, then f is both injective and surjective, i.e. bijective.

Let f be the function as given and let $3 \nmid n$.
To show that f is surjective, let $[y] \in \mathbb{Z}_n$ be given.
We need to show that there is some $[x] \in \mathbb{Z}_n$ for which $3[x] = [3x] = [x]$.
If $3 \mid y$, then $y = 3m$ for some $m \in \mathbb{Z}$ and $f([m]) = 3[m] = [3m] = [y]$.
Since $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$, then $m \in \mathbb{Z}_n$.
However, if $3 \nmid y$, then we can observe that y is either in the form $3m + 1$ or $3m + 2$ for some $m \in \mathbb{Z}$ by the division algorithm.
Also, n can similarly either be in the form $3k + 1$ or $3k + 2$ for some $k \in \mathbb{Z}$ by the division algorithm.

Case 1: $n = 3k + 1$

In the case where $n = 3k + 1$, we have two options.

If $y = 3m + 1$, we observe, by the equivalence classes under $\mathbb{Z}_n$, that $[y] = [y + 2n] = [3m + 1 + 6k + 2] = [6k + 3m + 3] = [3(2k + m + 1)] = [3l]$ where $l = 2k + m + 1 \in \mathbb{Z}$.

Since $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$, $l \in \mathbb{Z}_n$, and we have $f([l]) = 3[l] = [3l] = [y]$.

Similarly for the case where $y = 3m + 2$, by replacing $2n$ with n and therefore l with $k + m + 1$, we have $l \in \mathbb{Z}_n$ such that $f([l]) = [y]$.

Case 2: $n = 3k + 2$

In the case where $n = 3k + 2$, we have two options.

If $y = 3m + 1$, we observe, by the equivalence classes under $\mathbb{Z}_n$, that $[y] = [y + n] = [3m + 1 + 3k + 2] = [3k + 3m + 3] = [3(k + m + 1)] = [3j]$ where $j = k + m + 1 \in \mathbb{Z}$.

Since $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$, $j \in \mathbb{Z}_n$, and we have $f([j]) = 3[j] = [3j] = [y]$.

Similarly for the case where $y = 3m + 2$, by replacing n with $2n$ and therefore j with $2k + m + 2$, we have $j \in \mathbb{Z}_n$ such that $f([j]) = [y]$.

Since cases 1 and 2 are exhaustive for the rest of the cases, we have $[x] \in \mathbb{Z}_n$ in all cases such that $f([x]) = [y]$, and so f is surjective.
Also, f is surjective by lemma 0.0.1.
Hence, f is bijective.