HW #3

§1.4 #4 (a) $[a]_n = [b]_n$ iff $a \equiv b\ (n)$

Proof: If $[a]_n = [b]_n$ then $a \in [a]_n = [b]_n$, so $a \equiv b\ (n)$. Conversely if $a \equiv b\ (n)$ and $x \in [a]_n$ then $x \equiv a\ (n)$ and $a \equiv b\ (n)$, so $x \equiv b\ (n)$ and hence $x \in [b]_n$. Thus $[a]_n \subseteq [b]_n$. Now $a \equiv b\ (n)$ implies $b \equiv a\ (n)$ so by symmetry $[b]_n \subseteq [a]_n$. Hence $[a]_n = [b]_n$. //

1.4 #4 (b) Either $[a]_n = [b]_n$ or $[a]_n \cap [b]_n = \phi$.

Proof: As a matter of logic, either $[a]_n \cap [b]_n = \phi$ or $[a]_n = [b]_n \neq \phi$, so it suffices to show $[a]_n \cap [b]_n \neq \phi$ implies $[a]_n = [b]_n$. So, suppose $x \in [a]_n \cap [b]_n$. Then $x \equiv a\ (n)$ and $x \equiv b\ (n)$. Hence $a \equiv x \equiv b\ (n)$. By part (a), $[a]_n = [b]_n$. //

1.4 #10 Suppose $(a,n) = 1$. If $[a]_n$ has multiplicative order k then $k \mid \phi(n)$.

Proof: Write $\phi(n) = kq + r$, $0 \leq r < k$. Then $[a]^{\phi(n)} \equiv [1]$ by Fermat's Theorem and $[a]^k = [1]$ by definition of multiplicative order. Then

$$[1] = [a]^{\phi(n)} = [a]^{kq}[a]^r = [1]^q [a]^r = [a]^r.$$

Since k is the smallest positive integer solving $[a]^k = [1]$, r must not be positive. Hence $r = 0$ and $k \mid \phi(n)$. //

1.4 #11: In $\mathbb{Z}_9^\times$ show that each element is a power of $[2]$. Is there such an element in $\mathbb{Z}_8^\times$? Same question for $\mathbb{Z}_7^\times$.

Solution: $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [8]$, $[2]^4 = [7]$, $[2]^5 = [5]$ and $[2]^6 = [1]$, exhausting the elements of $\mathbb{Z}_9^\times$.

Since $\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$ and each of these has square $[1]$, no element of $\mathbb{Z}_8^\times$ generates $\mathbb{Z}_8^\times$ by taking powers.

In $\mathbb{Z}_7^\times$, $[3]$ has multiplicative order $k \mid \phi(7) = 6$, i.e. $k = 1, 2, 3$ or 6. Since $[3] \neq [1]$, $[3]^2 = [2] \neq [1]$, $[3]^3 = [6] \neq [1]$, $[3]$ must have order 6, so every element of $\mathbb{Z}_7^\times$ is a power of $[3]$. //

§2.1 #9 Show that each of the following defines a function.

(a) $f: \mathbb{Z}_8 \to \mathbb{Z}_8$ by $f[x] = [mx]$, $m \in \mathbb{Z}$. If $[x] = [y]$ then $x \equiv y$ (8) so $mx \equiv my$ (8) and hence $[mx] \equiv [my]$. //

(b) $g: \mathbb{Z}_8 \to \mathbb{Z}_{12}$ by $g[x]_8 = [6x]_{12}$. If $x \equiv y$ (8) then $x = y + 8k$ for some k. Then $6x = 6y + 48k \equiv 6y$ (12) so $[6x]_{12} = [6y]_{12}$. //

2.1 #10 Give an example to show this does not define a function.

(a) $f: \mathbb{Z}_8 \to \mathbb{Z}_{10}$ by $f[x]_8 = [6x]_{10}$

In $\mathbb{Z}_8$, $[0]_8 = [8]_8$ but $[6 \cdot 0]_{10} = [0]_{10} \neq [6 \cdot 8]_{10} = [8]_{10}$. //

(b) $g: \mathbb{Z}_2 \to \mathbb{Z}_5$ by $g[x]_2 = [x]_5$

In $\mathbb{Z}_2$, $[0]_2 = [2]_2$ but $g[0]_2 = [0]_5 \neq [2]_5 = g[2]_2$. //

2.1 #15 If $A \xrightarrow{f} B \xrightarrow{g} C$ then gf 1-1 implies f 1-1 and gf onto implies g onto.

Proof: Suppose gf is 1-1. If $f(x_1) = f(x_2)$ then $gf(x_1) = gf(x_2)$ and hence $x_1 = x_2$. Thus f is 1-1.

Suppose gf is onto. For $c \in C$ there exists $a \in A$ such that $(gf)(a) = c$. Thus $g(f(a)) = c$, showing g is onto. //