# Chapter 4

1.) Consider the following sets under addition:

1. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
   For all $a \in \mathbb{Z}_6$, there exist $n_1, n_2 \in \mathbb{Z}$ where $a = 1^{n_1} = 5^{n_2}$.
2. $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
   For all $a \in \mathbb{Z}_8$, there exist $n_1, n_2, n_3, n_4 \in \mathbb{Z}$ where $a = 1^{n_1} = 3^{n_2} = 5^{n_3} = 7^{n_4}$.
3. $\mathbb{Z}_{20} = \{0, 1, \ldots, 19, 20\}$
   For all $a \in \mathbb{Z}_{20}$, there exist $n_1, \ldots, n_8 \in \mathbb{Z}$ where $a = u_i^{n_i}$. Given $u_i \in U_{20}$.

3.) In $\mathbb{Z}_{30}$, $\langle 20\rangle = \{20, 10, 0\}$, and $\langle 10\rangle = \{10, 20, 0\}$. Suppose $a \in \mathbb{Z}_{30}$ where $|a| = 30$, thus $a^{40} = a^{30}a^{10} = a^{10}$ and $a^{60} = (a^{30})^2 = e$, thus $\langle a^{20}\rangle = \{a^{20}, a^{10}, e\}$ and $\langle a^{10}\rangle = \{a^{10}, a^{20}, e\}$.

9.) For all $k \in \mathbb{N}$ where $k \mid 20$, $\langle k\rangle$ is a subgroup of $\mathbb{Z}_{20}$ under addition, thus the subgroups of $\mathbb{Z}_{20}$ are $\langle 1\rangle$, $\langle 2\rangle$, $\langle 4\rangle$, $\langle 5\rangle$, $\langle 10\rangle$, and $\langle 20\rangle$ with generators 1, 2, 4, 5, 10, and 20 respectively. Given a group $G = \langle a\rangle$ where $|a| = 20$, the subgroups of $G$ are given by $\left\langle a^{kn}\right\rangle$ where $k \mid 20$ and $n \in \mathbb{N}$, thus there are 6 subgroups of $G$. Each of these subgroups has a generator of $a^k$.

22.) Let $G$ be a group with order 3 where $G = \{e, x, y\}$, and consider $x \in G$. If $x^2 = e$, then $x^3 = ex = x$, thus $x$ would not be a generator. If $x^2 = x$, then $x^3 = x^2 = e$, thus $x$ would not be a generator. Finally, if $x^2 = y$, then $x^3 = xy$. If $xy = x^2$, then $y = x$, thus $x^3 \neq xy$. If $x^3 = x$, then $x^2 = e$, thus $x^2 \neq e$. Thus we can conclude that $x^3 = e$, thus $x^1 = x$, $x^2 = y$, and $x^3 = e$, thus $G = \langle x\rangle$, thus $G$ is cyclic. ■

31.) Let $G$ be a finite group and $N = |G|$. Since the order of any $a \in G$ divides $N$, then given $|a| = k$, $a^N = a^{kn} = \left(a^k\right)^n = e^n = e$, thus there exists a suitable $N \in \mathbb{N}$. ■