Practice questions:

1. Let $\mathbb{Z}/n\mathbb{Z}$ be defined as the equivalence classes on $\mathbb{Z}$ where $x \sim y$ if and only if $n \mid x-y$. Verify that $\sim$ is an equivalence relation.

2. We say G is a group if G is closed under an operation $\cdot : G \times G \mapsto G$ where

   - For all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$
   - There exists $e \in G$ (called the identity) such that for all $g \in G$, $g \cdot e == g$
   - For all $g \in G$, there exists $g^{-1} \in G$ (called g inverse) such that $g \cdot g^{-1} = e$

   Verify that $\mathbb{Z}/n\mathbb{Z}$ forms a group under addition mod n.

3. Consider $\mathbb{Z}/n\mathbb{Z} - [0]_n$.

   (a) When does this set form a group under multiplication mod n?

   (b) What is the biggest subset $U_n \subseteq \mathbb{Z}/n\mathbb{Z}$ such that U_n is a group under multiplication with $[1]_n$ as the identity?

4. We say G is a cyclic group if $G = \left\{g^k : k \in \mathbb{Z}\right\}$ for some $g \in G$. Then, we call g a generator of G.

   (a) We say G is isomorphic to H, written $G \cong H$, where G, H are groups under the operations $\cdot, \diamond$ respectively, if there exists a bijection $\phi : G \mapsto H$ such that for all $g_1, g_2 \in G$, $\phi(g_1 \cdot g_2) = \phi(g_1) \diamond \phi(g_2)$. Show that if G is cyclic, then G is isomorphic to $\mathbb{Z}$ under addition or $\mathbb{Z}/n\mathbb{Z}$ under addition mod n.

   (b) Verify that $\mathbb{Z}/n\mathbb{Z}$ under addition mod n is a cyclic group.

5. We say H is a subgroup of G if H is a group contained in G with the same operation as G.

   (a) Show that every subgroup of a cyclic group is also cyclic.

   (b) We say the order of an element g, written $\#g$, is the smallest natural number n such that $g^n = e$ where g^n denotes g multiplied by itself n times.

   (c) We say the order of a group G, denoted $\#G$, is the cardinality of G. Show that if $\#g = k$ then $\#\langle g^d \rangle = \frac{d}{\gcd(d,k)}$.

   (d) Show that if $g_1, g_2 \in G$ have the same order, then $\langle g_1 \rangle = \langle g_2 \rangle$.

   (e) Show that the generators of $\mathbb{Z}/n\mathbb{Z}$ under addition mod n are $[d]_n$ such that d is coprime to n and that there are $\varphi(n)$ generators of $\mathbb{Z}/n\mathbb{Z}$ under addition mod n where φ denotes the Euler totient function

6. Let R be a relation on $\mathbb{Z}/n\mathbb{Z}$ where $[x]_n R [y]_n$ if and only if there exists an invertible $[u]_n$ (under multiplication mod n) such that $[x]_n \cdot [u]_n = [y]_n$ where $\cdot$ is the usual multiplication mod n.

(a) Show that for every divisor d of n, there exists a unique subgroup of order d contained in $\mathbb{Z}/n\mathbb{Z}$.

(b) Show that xRy if and only if x and y have the same order in $\mathbb{Z}/n\mathbb{Z}$ under addition mod n.

(c) Hence show that distinct equivalence classes of R are precisely the set of generators for distinct subgroups of $\mathbb{Z}/n\mathbb{Z}$

(d) Using this, prove that $n = \sum_{d:d|n} \varphi(d)$.

7. Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n. For every $d \in \mathbb{N}$, define a set $A_d = \left\{x \in G : x^d = e, \#x = d\right\}$. Prove that G is cyclic. (Hint: Use a counting argument involving the result from 6d and show that $A_n \neq \varnothing$ for all $n \in \mathbb{N}$).