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 $\cdot$, which is a map $G \times G \mapsto G$ where

   - For all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ ($\cdot$ associative)
   - 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 $g \cdot g^{-1} = e$

   And we call a group abelian if for all $g_1, g_2 \in G$, $g_1 \cdot g_2 = g_2 \cdot g_1$. Verify that $\mathbb{Z}/n\mathbb{Z}$ forms an abelian 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? (This is called the multiplicative group of integers mod n)

4. (a) Let G be a finite set closed under an associative operation with a left identity e_L such that for all g, $g \cdot e_L$ and for all g, there exists a left inverse ${g_L}^{-1} \cdot g = e_L$. Verify that G forms a group with $e_L = e$ and ${g_L}^{-1} = g^{-1}$

   (b) Show that it is not necessarily true that if G has a left identity and every element has a right inverse $g \cdot {g_R}^{-1} = e_L$ that G forms a group.

   (c) Let G be a finite set closed under an associative operation such that for all $a, b, c \in G$, $a \cdot b = a \cdot c \implies b = c$ and $b \cdot a = c \cdot a \implies b = c$. Show that G is a group.

   (d) Hence show that the multiplicative group of integers mod n, call it U_n, is a group.

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

   (b) 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.

   (c) Let G, H be groups with the operations $\cdot, \diamond$ respectively, and we define an (external) direct product $G \times H$ with the operation $*$ where $(g, h') * (g, h) = (g \cdot g', h \diamond h')$. Use the Chinese remainder theorem to show that if m, n are coprime, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

6. 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. Show that for $\prod_i^r \mathbb{Z}/n_i\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$, we have that $\#(g_1, g_2, \ldots, g_r) = \operatorname{lcm}(\#g_1, \#g_2, \ldots, \#g_r)$.

   (c) We say the order of a group G, denoted $\#G$, is the cardinality of G. Let H be a subgroup of G where G is a finite group. Prove that $\#H \mid \#G$.

   (d) Every subgroup H induces a partition on G under the relation $g \sim g'$ if and only if there exists $h \in H$ such that $g = g'h$. Show that every equivalence class, call it gH (also known as a coset of H), has the same number of elements as H, and hence conclude that $\#G = \#H[G : H]$ where $[G : H]$ is called the index of H and represents the number of distinct cosets of H.

   (e) Show that if $\#g = k$ then $\#\langle g^d \rangle = \frac{d}{\gcd(d,k)}$.

   (f) Show that every group of prime order is cyclic.

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

   (h) 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.

7. 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 $n = \sum_{d:d|n} \varphi(d)$.

8. 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 $A_d = \{x \in G : x^d = e, \#x = d\}$. Prove that G is cyclic. (Hint: Use a counting argument involving the result from 6d and show that $A_n \neq \varnothing$ for all $n \in \mathbb{N}$, so $A_{\#G} \neq \varnothing$ and thus we have an element of order $\#G$).

9. Let P be a maximal subgroup in a finite group G (so a subgroup that is only contained by G) such that its order is p^k where p is prime, so P is called a Sylow $p-$subgroup. Sylow's theorems state that

- For every $p \mid \#G$, there exists a Sylow $p-$subgroup of order p^k (Corollary: For every $p^r \mid \#G$, there exists a group of order p^r)
- If P_1, P_2 are Sylow $p-$subgroups, there exists g such that $P_1 = gP_2g^{-1}$
- Let n_p be the number of distinct Sylow $p-$subgroups. Then, n_p divides the index of the Sylow $p-$subgroups, $n_p \equiv 1 \mod p$, and $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup, $N_G(P) = \{g \in G : gPg^{-1} = P\}$
- If H is a group of order p^r where $r \leq k$ then H is contained in a Sylow $p-$subgroup.

(a) Show that $N_G(P)$ is a subgroup of G

(b) We say H is normal in G, denoted $H \trianglelefteq G$, if for all $g \in G$, $gHg^{-1} = H$

(c) Show that if P is a unique Sylow $p-$subgroup of G, then $P \trianglelefteq G$.

(d) Show that $N_G(N_G(P)) = N_G(P)$

(e) Let $K \trianglelefteq G$. Show that if P is a Sylow $p-$subgroup such that $P \trianglelefteq K$, then $P \trianglelefteq G$.

(f) A group G is called simple if $\{e\}, G$ are the only normal subgroups of G. Show that if $\#G = 8896$ then G is not simple.

(g) Show that if $\#G = 56$ then G is not simple.

(h) Let p, q be primes with $p < q$. Show that if $\#G = pq$ then G is not simple.

(i) Let p, q be primes and assume $p \nmid q - 1$, $p < q$. Show that if $\#G = pq$, then G is cyclic.

(j) Let p, q be primes and assume $p \mid q - 1$, $p < q$. Show that if $\#G = pq$, then G has a unique non-abelian group of order pq.

10. We say $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{r+1} = \{1\}$ is a composition series if at every stage, G_{i+1} is maximal in G_i. Using normal groups $K \trianglelefteq G$, we can form quotient groups G/K where its order is $[G : K]$ and its elements are cosets of K with multiplication being defined as $g_1K * g_2K = (g_1 \cdot g_2)K$ where $\cdot$ is the multiplication in G.

    (a) Show that if G is abelian, G is finite if and only if it has a composition series.

    (b) Show that if G is a finite cyclic group, G has a composition series $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{r+1} = \{1\}$ where $\#G_i/\#G_{i+1}$ is prime.

    (c) Show that if $n = n_1, n_2, \ldots, n_{r+1} = 1$ is a sequence of integers such that n_i/n_{i+1} is prime, then G has a composition series $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{r+1} = \{1\}$.

11. We say G is supersolvable if G has a composition series $G = G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_{r+1} = \{1\}$ where at every stage, the quotient group G_i/G_{i+1} is cyclic and $G_i \trianglelefteq G$.

    (a) Show that every group of square free order is supersolvable.

    (b) Show that every group with cyclic Sylow $p-$subgroups is supersolvable.

    (c) Show that if G is finite and supersolvable then every maximal subgroup has a prime index.