1. Write out the definitions of the following concepts:
   (a) group
   (b) cyclic group
   (c) one-to-one function; onto function
   (d) greatest common divisor of two integers.

2. Write out the statements of the following theorems:
   (a) The Division Algorithm
   (b) Lagrange’s Theorem (on the order of a subgroup of a finite group)
   (c) The proposition which gives Euler’s function \( \varphi(n) \) in terms of the prime factorization of \( n \).

3. Let \( \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 3 & 1 & 4 & 7 & 2 \end{pmatrix} \) and \( \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 6 & 5 & 4 & 3 \end{pmatrix} \).
   (a) Write \( \sigma, \tau, \sigma\tau, \) and \( \tau\sigma \) as products of disjoint cycles.
   (b) Find the order of each of \( \sigma, \tau, \sigma\tau, \) and \( \tau\sigma \).

4. Write out the proof of the theorem which states that every subgroup of a cyclic group is cyclic.

5. Write out a proof of the theorem which states that if \( G \) is any cyclic group, then \( G \) is isomorphic to either \( \mathbb{Z} \) or \( \mathbb{Z}_n \) (for some positive integer \( n \)).

6. Show that the three groups \( \mathbb{Z}_6, \mathbb{Z}_9^\times, \) and \( \mathbb{Z}_{18}^\times \) are isomorphic to each other. In each case, write down the function that gives the isomorphism. (You can quote theorems which prove that the function is in fact an isomorphism.)

7. Let \( p = 2k + 1 \) be a prime number. Prove that if \( a \) is an integer such that \( p \nmid a \), then either \( a^k \equiv 1 \pmod{p} \) or \( a^k \equiv -1 \pmod{p} \).

8. Let \( n \) be a positive integer. For \( \alpha, \beta \in S_n \), define \( \alpha \sim \beta \) if there exists \( \sigma \in S_n \) such that \( \sigma\alpha\sigma^{-1} = \beta \).
   (a) Prove that \( \sim \) is an equivalence relation on \( S_n \).
   (b) For \( S_3 \), find the equivalence classes of the relation \( \sim \).