

1. (a) State the division algorithm.
- (b) State the Chinese remainder theorem.
- (c) Solve the following system of congruences:

$$x \equiv 13 \pmod{25} \quad x \equiv 9 \pmod{18}$$

2. (a) Use the Euclidean algorithm to find $[8]_{27}^{-1}$ (in \mathbf{Z}_{27}^\times).
 - (b) Find $\varphi(27)$ and list all of its positive divisors.
 - (c) Find the order of $[8]_{27}$ in the group \mathbf{Z}_{27}^\times .
3. Let $\sigma = (3, 6, 8)(1, 9, 4, 3, 2, 7, 6, 8, 5)(2, 3, 9, 7) \in S_9$.
 - (a) Write σ as a product of disjoint cycles.
 - (b) Is σ an even permutation or an odd permutation?
 - (c) What is the order of σ in S_9 ?
 - (d) Compute σ^{-1} in S_9 .
4. (a) State the definition of an equivalence relation.
 - (b) State the definition of a subgroup of a group.
 - (c) Let G be a group, and let H be a subgroup of G . For $x, y \in G$, define $x \sim y$ if $x^{-1}y \in H$. Prove that \sim defines an equivalence relation on G .
5. (a) State the definition of a one-to-one function.
 - (b) State the definition of an onto function.
 - (c) State the definition of an isomorphism of groups.
 - (d) Let G_1, G_2 be groups and let H_2 be a subgroup of G_2 . Prove that if $\phi : G_1 \rightarrow G_2$ is an isomorphism, then $H_1 = \{g \in G_1 \mid \phi(g) \in H_2\}$ is a subgroup of G_1 .
6. (a) Let H and K be subgroups of the group G . Prove that HK is a subgroup of G if and only if $KH \subseteq HK$.
 - (b) Let $G = \mathbf{Z}_{10}^\times \times \mathbf{Z}_{10}^\times$, let $H = \langle(3, 3)\rangle$ and let $K = \langle(3, 7)\rangle$. List the elements of HK .
7. (a) State the definition of a cyclic group.
 - (b) Write out ONE of the following proofs from the text:
 - I. Any subgroup of a cyclic group is cyclic.
 - II. If G is a cyclic group of order n , then G is isomorphic to \mathbf{Z}_n .

8. (a) State the definition of the order of an element.

(b) Prove or disprove: If a, b are elements of the group G with $o(a) = m$ and $o(b) = n$, where m, n are positive integers, then $o(ab) \leq \text{lcm}[m, n]$.

If you are unable to answer the general question, you can get partial credit for answering the question in the special case that $ab = ba$.