SECTION A

1. Prove by induction that, for every positive integer n,

$$n^5 - n \text{ is divisible by } 10.$$

[6 marks]

2. Find the greatest common divisor d of 6391 and 5159, and find integers s and t such that

$$d = 6391s + 5159t.$$

[6 marks]

3. In each of the following cases find the solutions (if any) of the given linear congruence:

(a) $12x \equiv 6 \bmod 21$;

(b) $13x \equiv 7 \bmod 21$;

(c) $14x \equiv 8 \bmod 21$. [10 marks]

4. Define Euler's function $\phi(n)$ for every integer $n > 1$.

Find $\phi(22)$ and use Euler's Theorem to show that

$$5^{11} + 17^{11} \text{ is divisible by } 22.$$

[8 marks]

5. Draw diagrams of each of the following maps and say which (if any) of them are injective, and which (if any) are surjective.

(a) $f : \mathbf{Z}_7 \to \mathbf{Z}_7$ given by $f(x) = 2x$;

(b) $f : \mathbf{Z}_8 \to \mathbf{Z}_8$ given by $f(x) = 2x$;

(c) $f : \mathbf{Z}_3 \to \mathbf{Z}_6$ given by $f(x) = 2x$;

[9 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 4 & 7 & 8 & 6 & 3 \end{pmatrix}, \quad \rho = (341)(1538).$$

Write π, ρ, π^2 and $\pi\rho$ as products of disjoint cycles and determine their orders and signs. [8 marks]

7. Construct a multiplication table for the group $S(3)$ of permutations of $\{1, 2, 3\}$.

Find the order of each element of this group. [8 marks]

SECTION B

8. (a) Find the inverse of 159 modulo 527. [6 marks]

(b) Find the smallest positive integer x which leaves remainder 6 when divided by 11, is divisible by 13 and is congruent to 5 modulo 14.

Find also the next smallest positive integer with these properties. [9 marks]

9. State the axioms for a group.

In each of the following, determine which of the group axioms are satisfied. [You may assume that ordinary addition and multiplication are associative.]

(a) The set of odd integers under multiplication;

(b) the set of non-zero real numbers under division;

(c) the set of real numbers under the operation $*$ defined by

$$a * b = a + b + 1.$$

[15 marks]

10. (a) Let G be a group. Say what it means for G to be *cyclic*.

Find the order of each element of the group G_{20}. Hence determine whether or not this group is cyclic. [7 marks]

(b) Let $D(4)$ denote the group of symmetries of a square. The element a of $D(4)$ is defined as the anticlockwise rotation through $\pi/2$ and b as reflection in one of the diagonals. Show that

$$H = \{e, a^2, ab, a^3b\}$$

is a subgroup of $D(4)$. [You may find it useful to construct a multiplication table for H.] [8 marks]

11. A group code has generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

List the codewords and state how many errors are detected and how many are corrected by this code, giving reasons for your answers.

Write down the parity check matrix and a table of syndromes for this code for all possible single digit errors in transmission.

Using the following letter to number equivalents:

A	E	I	O	N	S	T	X
000	001	010	100	011	101	110	111

correct and read the received message:

0011101 0111000 1100101 0011111 1110110 1010011 0101011
1101110 0110110.

[15 marks]