SECTION A

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

$$5^{2n} - 1 \text{ is divisible by } 24.$$

[6 marks]

2. Find the greatest common divisor d of 1080 and 1665, and find integers s and t such that

$$d = 1080s + 1665t.$$

[6 marks]

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

(i) $10x \equiv 25 \bmod 45$;

(ii) $11x \equiv 25 \bmod 45$;

(iii) $12x \equiv 25 \bmod 45$. [10 marks]

4. State Fermat's Theorem.

Show that

$$4^{42} + 5^{42} \text{ is divisible by } 41.$$

[7 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.

(i) $f : \mathbf{Z}_5 \to \mathbf{Z}_5$ given by $f(x) = 3x$;

(ii) $f : \mathbf{Z}_6 \to \mathbf{Z}_6$ given by $f(x) = 3x$;

(iii) $f : \mathbf{Z}_2 \to \mathbf{Z}_6$ given by $f(x) = 3x$.

[9 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 3 & 1 & 7 & 6 \end{pmatrix}, \quad \rho = (3124)(1567).$$

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

7. Construct a multiplication table for the group G_{18} of invertible congruence classes modulo 18.

Find the order of each element of this group. [9 marks]

SECTION B

8. (a) Find the inverse of 61 modulo 312. [6 marks]

(b) Solve the simultaneous congruences

$$x \equiv 4 \bmod 17, \quad x \equiv 5 \bmod 19, \quad x \equiv 6 \bmod 21,$$

expressing your answer in the form $x \equiv a \bmod n$ for suitable a and n.

[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, and multiplication modulo 4, are associative.]

(i) The set of even integers under addition;

(ii) the set of integers under subtraction;

(iii) the set of non-zero congruence classes modulo 4 under multiplication modulo 4. [15 marks]

10. 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.

(i) Draw a picture of the square showing the effects of a and b.

[2 marks]

(ii) Show that

$$a^4 = e, \quad b^2 = e \quad \text{and} \quad ba^3 = ab.$$

[4 marks]

(iii) Let $H = \{e, a, a^2, a^3\}$ and $K = \{e, a^2, ab, a^3b\}$. Show that H and K are subgroups of $D(4)$. [You may find it useful to construct multiplication tables for H and K.] [9 marks]

11. A group code has generator matrix

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

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	L	Z	M	E	B	S	Y
000	001	010	100	011	101	110	111

correct and read the received message:

010000 110011 100011 011111 100110 111101 001011 011000.

[15 marks]