SECTION A

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

$$\sum_{r=1}^{n} r^3 = \frac{1}{4}n^2(n+1)^2.$$

[6 marks]

2. Find the greatest common divisor d of 2323 and 1656, and find integers s and t such that

$$d = 2323s + 1656t.$$

[6 marks]

3. Find the inverse of 83 modulo 614. [6 marks]

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

(a) $9x \equiv 15 \bmod 42$;

(b) $10x \equiv 15 \bmod 42$;

(c) $11x \equiv 15 \bmod 42$. [10 marks]

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

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

(b) $f : \mathbf{Z}_6 \to \mathbf{Z}_6$ given by $f(x) = 5x$;

(c) $f : \mathbf{Z}_6 \to \mathbf{Z}_3$ given by $f(x) = [x]_3$. [Here $[x]_3$ denotes the congruence class of x modulo 3.]

[9 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 5 & 4 & 7 & 1 & 6 & 3 \end{pmatrix}, \quad \rho = (2714)(7326).$$

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 G_{24} of invertible congruence classes modulo 24.

List the elements of order 2 in this group. [10 marks]

SECTION B

8. (a) Solve the simultaneous congruences

$$x \equiv 3 \bmod 25, \quad x \equiv 11 \bmod 27,$$

expressing your answer in the form $x \equiv a \bmod n$ for suitable a and n. [6 marks]

(b) Define Euler's function $\varphi(n)$ for every integer $n > 1$. State a formula for $\varphi(pq)$, where p and q are distinct primes.

Find $\varphi(185)$.

Determine the remainder when each of the following numbers is divided by 185.

$$\text{(i) } 14^{144}; \quad \text{(ii) } 14^{146}; \quad \text{(iii) } 14^{147} + 31^{145}.$$

[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 multiplication, and multiplication modulo n, are associative.]

(a) The set of odd integers under multiplication;

(b) the set of non-zero congruence classes modulo 6 under multiplication modulo 6;

(c) the set of non-zero congruence classes modulo 7 under multiplication modulo 7. [15 marks]

10. Say what it means for a subset H of a group G to be a *subgroup* of G.

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) Describe geometrically by means of diagrams the elements a^2, ab and a^2b of $D(4)$.

(ii) Prove that

$$a^4 = e, \quad b^2 = e, \quad ba^3 = ab.$$

(iii) Let $H = \{e, a^2, b, a^2b\}$. By constructing a multiplication table for H, or otherwise, show that H is a subgroup of $D(4)$.

Determine whether or not H is a cyclic subgroup of $D(4)$. [15 marks]

11. A group code has generator matrix

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

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	B	G	N	O	R	S	W
000	001	010	100	011	101	110	111

correct and read the received message:

1100101 1101000 0010000 1001111 1110101 0110011 1001011 1101110.

[15 marks]