SECTION A

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

$$\sum_{r=1}^{n} r^2 = \frac{1}{6}n(n+1)(2n+1).$$

[6 marks]

2. Find the greatest common divisor d of 4171 and 1806, and find integers s and t such that

$$d = 4171s + 1806t.$$

[6 marks]

3. Find the inverse of 102 modulo 337. [6 marks]

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

(a) $15x \equiv 10 \bmod 33$;

(b) $15x \equiv 10 \bmod 35$;

(c) $15x \equiv 10 \bmod 37$. [10 marks]

5. Let A be the set consisting of the two elements a and b, and B the set consisting of the three elements 0, 1 and 2. List all the maps $f : A \to B$ and say which (if any) of these are injective.

Say why it is not possible for any map $f : A \to B$ to be surjective. [8 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 7 & 6 & 1 & 3 \end{pmatrix}, \quad \rho = (3572)(861).$$

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

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

Find the order of each element of the group. [11 marks]

SECTION B

8. (a) Solve the simultaneous congruences

$$x \equiv 11 \bmod 24, \quad x \equiv 7 \bmod 23,$$

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

(b) State Fermat's Theorem.

Find

(i) the smallest positive integer k such that $2^k \equiv 1 \bmod 11$ (the *order* of 2 modulo 11);

(ii) the order of 3 modulo 11;

(iii) the remainder when 5^{22} is divided by 11. [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 negative integers under multiplication;

(b) the set of integers under division;

(c) the set $\{1, 3, 7, 9\}$ under multiplication modulo 10. [15 marks]

10. (a) Let $D(5)$ denote the group of symmetries of a regular pentagon. The element a of $D(5)$ is defined as the anti-clockwise rotation through $2\pi/5$ and b as reflection in one of the lines joining a vertex to the mid-point of the opposite side. Show that $ab = ba^{-1}$ and $a^2b = ba^3$. [7 marks]

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

Let $S(4)$ denote the group of permutations of $\{1, 2, 3, 4\}$, and let

$$H = \{e, (12)(34), (13)(24), (14)(23)\}.$$

By constructing a multiplication table for H, or otherwise, show that H is a subgroup of $S(4)$. [8 marks]

11. A group code has generator matrix

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

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:

U	L	A	T	R	C	E	X
000	001	010	100	011	101	110	111

correct and read the received message:

0110111 1110110 1011100 1001011 1000000 0101010 1100110
0111110.

[15 marks]