SECTION A

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

$$1.2 + 2.3 \ldots + n(n+1) = \frac{1}{3}n(n+1)(n+2).$$

[6 marks]

2. Find the greatest common divisor d of 1025 and 2542, and find integers s and t such that

$$d = 1025s + 2542t.$$

[6 marks]

3. Find the inverse of 60 modulo 257. [6 marks]

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

(a) $8x \equiv 4 \bmod 38$;

(b) $8x \equiv 4 \bmod 39$;

(c) $8x \equiv 4 \bmod 40$. [10 marks]

5. Let X be the set consisting of the three elements 1, 2 and 3, and Y the set consisting of the two elements a and b. List the eight maps $f : X \to Y$ and say which (if any) of these are injective and which (if any) are surjective.

[7 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 2 & 6 & 5 & 7 \end{pmatrix}, \ \rho = (3762)(3421).$$

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

7. List the elements of the group G_{24} of invertible congruence classes modulo 24. Construct a multiplication table for this group.

Find the orders of all elements of the group. [12 marks]

SECTION B

8. (a) Solve the simultaneous congruences

$$x \equiv 9 \bmod 25, \quad x \equiv 14 \bmod 24,$$

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

(b) State Fermat's Theorem.

Verify that 211 is a prime number. Determine the remainder when each of the following numbers is divided by 211:

$$\text{(i) } 11^{210}, \quad \text{(ii) } 11^{212} \quad \text{and (iii) } 11^{214}.$$

[9 marks]

9. (a) State the axioms for a group. [3 marks]

(b) Let $G = \{2, 4, 6, 8\}$. Write down a multiplication table for G for the operation of multiplication modulo 10. Show that G is a group under this operation. [You may assume that multiplication modulo 10 is associative.]

[6 marks]

(c) Let $G = \{x \in \mathbf{R} : x \neq -1\}$. An operator $*$ is defined on G by

$$x * y = xy + x + y.$$

Show that G is a group under the operation $*$. [You may assume that multiplication of real numbers is associative.] [6 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 anticlockwise 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 that $a^2b = ba^3$. [7 marks]

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

Now let $G = G_{20}$, the group of invertible congruence classes modulo 20, and let $H = \{[1]_{20}, [9]_{20}, [11]_{20}, [19]_{20}\}$. By constructing a multiplication table for H, or otherwise, show that H is a subgroup of G. Find also a subgroup K of G with four elements, containing the element $[3]_{20}$. [8 marks]

11. A group code has generator matrix

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

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	L	O	P	R	T	Y
001	010	100	011	101	110	111	000

correct and read the received message:

001011 001101 110001 011101 010111 011110 100110 101101.

[15 marks]