SECTION A

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

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

[8 marks]

2. Find the greatest common divisor d of 2665 and 861, and find integers s and t such that

$$d = 2665s + 861t.$$

[6 marks]

3. Find the inverse of 85 modulo 167. [6 marks]

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

(a) $10x \equiv 5 \bmod 15$;

(b) $11x \equiv 6 \bmod 15$;

(c) $12x \equiv 7 \bmod 15$. [10 marks]

5. Let A be the set consisting of the two elements 1 and 2. List the four maps $f : A \to A$ and say which of these are injective and which are surjective.

[5 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}, \quad \rho = (156)(31425).$$

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_{20} of invertible congruence classes modulo 20. Construct a multiplication table for this group.

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

SECTION B

8. (i) 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]

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

Write down a formula for $\phi(pq)$, where p and q are distinct prime numbers. Hence find $\phi(115)$.

Use Euler's Theorem to determine

$$\text{(a) } 11^{88} \bmod 115, \quad \text{(b) } 11^{89} \bmod 115 \quad \text{and (c) } 11^{90} \bmod 115.$$

[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 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $X^2 = I$. Show further that the set of matrices $\{\pm I, \pm X\}$ forms a group under matrix multiplication. [You may assume that matrix multiplication is associative.] [6 marks]

10. (a) 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

$$a^4 = 1, \quad b^2 = 1 \quad ba = a^3 b \quad \text{and} \quad ba^2 = a^2 b.$$

[7 marks]

(b) Let $H = \{e, a, a^2, a^3\}$ and $K = \{e, a^2, b, a^2 b\}$. Show that H and K are subgroups of $D(4)$. [You may find it useful to construct multiplication tables for H and K.] [8 marks]

11. A group code has generator matrix

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

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:

A	B	E	F	I	L	T	U
000	001	010	100	011	101	110	111

correct and read the received message:

000111 110101 000000 111001 110010 001010 100011 111001 111100.

[15 marks]