SECTION A

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

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

[6 marks]

2. Find the greatest common divisor d of 1071 and 2583, and find integers s and t such that

$$d = 1071s + 2583t.$$

[6 marks]

3. Find the inverse of 27 modulo 340. [6 marks]

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

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

(b) $10x \equiv 15 \bmod 34$;

(c) $10x \equiv 15 \bmod 35$. [10 marks]

5. Let A be the set consisting of the three elements a, b and c, and B the set consisting of the two elements 1 and 2. List the six surjective maps $f : A \to B$.

Say why it is not possible for any map $f : A \to B$ to be injective.

Give an example of an injective map $g : B \to A$. [8 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 3 & 1 & 7 & 8 & 6 \end{pmatrix}, \ \rho = (1372)(4216).$$

Write π, ρ, π^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

$$x \equiv 14 \bmod 25, \quad x \equiv 11 \bmod 23,$$

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

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

Find $\phi(91)$.

Determine the remainder when each of the following numbers is divided by 91:

$$\text{(i) } 15^{72}; \quad \text{(ii) } 15^{73}; \quad \text{(iii) } 15^{74}.$$

[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 integers under subtraction;

(b) the set of real numbers under multiplication;

(c) the set $\{1, 7, 13, 19\}$ under multiplication modulo 30. [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) Express a and b as permutations of the vertices. [2 marks]

(iii) Express ab, ba and a^3 as permutations. Hence show that $ba \neq ab$ and $ba = a^3b$. [5 marks]

(iv) Let $H = \{e, a^2, ab, a^3b\}$. Show that H is a subgroup of $D(4)$. [You may find it useful to construct a multiplication table for H.] [6 marks]

11. A group code has generator matrix

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

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	D	E	O	R	V	Y
000	001	010	100	011	101	110	111

correct and read the received message:

101101 110111 100101 101010 110000 011110 011101
110011 111000.

[15 marks]