SECTION A

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

$$n^5 - 6n \text{ is divisible by } 5.$$

[6 marks]

2. Find the greatest common divisor d of 2829 and 2296, and find integers s and t such that

$$d = 2829s + 2296t.$$

[6 marks]

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

(a) $6x \equiv 21 \bmod 43$;

(b) $6x \equiv 21 \bmod 44$;

(c) $6x \equiv 21 \bmod 45$. [10 marks]

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

Find $\phi(33)$ and use Euler's Theorem to show that $2^{43} + 5^{42}$ is divisible by 33.

[6 marks]

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

[8 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 5 & 4 & 1 & 2 \end{pmatrix}, \quad \rho = (3427)(1526).$$

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 $S(3)$ of permutations of $\{1, 2, 3\}$.

Find elements π, ρ of $S(3)$ such that $\pi\rho \neq \rho\pi$.

Write down the inverse of each element of $S(3)$. [11 marks]

SECTION B

8. (a) Find the inverse of 85 modulo 494. [6 marks]

(b) Find the smallest positive integer n which satisties the simultaneous congruences

$$x \equiv 2 \bmod 16, \quad x \equiv 3 \bmod 19, \quad x \equiv 7 \bmod 25.$$

Find also the next smallest integer satisfying these congruences. [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 positive integers under multiplication;

(b) the set of integers under subtraction;

(c) the set $\{2, 4, 6, 8\}$ under multiplication modulo 10. [15 marks]

10. (a) Say what it means for a group G to be *cyclic*.

Determine whether or not the group G_9 of invertible congruence classes modulo 9 is cyclic. [5 marks]

(b) 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 a line joining the mid-points of a pair of opposite sides.

Now let $H = \{e, a^2, ab, a^3b\}$. 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 $D(4)$. [10 marks]

11. A group code has generator matrix

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

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	E	N	P	G	W	T	S
000	001	010	100	011	101	110	111

correct and read the received message:

010110 011011 101100 110000 100000 010101 001011
000110 110111.

[15 marks]