SECTION A

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

$$4^{2n} - 1 \text{ is divisible by } 15.$$

[6 marks]

2. Find the greatest common divisor d of 7614 and 3713, and find integers s and t such that

$$d = 7614s + 3713t.$$

[6 marks]

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

(a) $10x \equiv 14 \bmod 35$;
(b) $10x \equiv 14 \bmod 36$;
(c) $10x \equiv 14 \bmod 37$. [10 marks]

4. State Fermat's Theorem.

Show that $4^{91} + 5^{90}$ is divisible by 89. [6 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 0 and 1. List all the maps $f : A \to B$ and say which (if any) of these are surjective.

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

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 2 & 6 & 8 & 5 \end{pmatrix}, \quad \rho = (1684)(6245).$$

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

7. List the elements of the group G_{16} of invertible congruence classes modulo 16. Construct a multiplication table for this group.

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

SECTION B

8. (a) Find the inverse of 65 modulo 412. [6 marks]

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

$$x \equiv 21 \bmod 31, \quad x \equiv 3 \bmod 15, \quad x \equiv 4 \bmod 26.$$

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 addition and multiplication, and multiplication modulo n, are associative.]

(a) The set of odd integers under addition;

(b) the set $\{1, 3, 7, 9\}$ under multiplication modulo 20;

(c) the set of rational numbers under multiplication. [15 marks]

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

List the elements of the group G_9 of invertible congruence classes modulo 9. Determine whether or not G_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 $\pi/2$.

Let $H = \{e, a, a^2, a^3\}$. By constructing a multiplication table for H, or otherwise, show that H is a subgroup of $D(4)$. Show further that H is cyclic and determine the orders of all elements of H. [10 marks]

11. A group code has generator matrix

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

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:

X	W	R	L	F	E	D	A
000	001	010	100	011	101	110	111

correct and read the received message:

0111110 1110001 0111011 1011010 1010111 1001010 1011101 1001101.

[15 marks]