SECTION A

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

$$3^{2n} - 1 \text{ is divisible by } 8.$$

[6 marks]

2. Find the greatest common divisor d of 3774 and 1184, and find integers s and t such that

$$d = 3774s + 1184t.$$

[6 marks]

3. Find the inverse of 77 modulo 263. [6 marks]

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

(a) $4x \equiv 10 \bmod 34$;
(b) $4x \equiv 10 \bmod 35$;
(c) $4x \equiv 10 \bmod 36$. [10 marks]

5. Draw diagrams of each of the following maps and say which (if any) of them are injective, and which (if any) are surjective.

(a) $f : \mathbf{Z}_2 \to \mathbf{Z}_2$ given by $f(x) = x^2$;
(b) $f : \mathbf{Z}_4 \to \mathbf{Z}_4$ given by $f(x) = x^2$;
(c) $f : \mathbf{Z}_4 \to \mathbf{Z}_2$ given by $f(x) = [x^2]_2$.

[In (c), $[x^2]_2$ means the remainder when x^2 is divided by 2.]

[8 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 7 & 8 & 4 & 6 & 5 \end{pmatrix}, \quad \rho = (3516)(427).$$

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_9 of invertible congruence classes modulo 9. 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

$$x \equiv 19 \bmod 28, \quad x \equiv 1 \bmod 11,$$

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 $\phi(111)$.

Determine the remainder when each of the following numbers is divided by 111:

$$\text{(i) } 13^{72}; \quad \text{(ii) } 13^{74}; \quad \text{(iii) } 13^{74} + 53^{73}.$$

[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 of integers under multiplication;

(c) the set $\{1, 2, 4, 8\}$ under multiplication modulo 15. [15 marks]

10. Say what it means for a subset H of a group G to be a *subgroup* of G. Say also what it means for H to be a *cyclic subgroup*.

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. Show that

$$a^4 = e; \quad b^2 = e; \quad ab = ba^3.$$

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 $D(4)$. [15 marks]

11. A group code has generator matrix

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

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:

C	E	G	I	K	L	N	X
000	001	010	100	011	101	110	111

correct and read the received message:

0011110 1101000 0000100 1011110 1010101 1110101 1011011
1100110 0111101.

[15 marks]