SECTION A

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

$$\sum_{r=1}^{n}(2r-1)=n^2.$$

[6 marks]

2. Find the greatest common divisor d of 1131 and 2418, and find integers s and t such that

$$d = 1131s + 2418t.$$

[6 marks]

3. Find the inverse of 69 modulo 260. [6 marks]

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

(a) $6x \equiv 14 \bmod 33$;

(b) $6x \equiv 14 \bmod 34$;

(c) $6x \equiv 14 \bmod 35$. [10 marks]

5. Let A be the set consisting of the two elements a and b, and B the set consisting of the three elements 0, 1 and 2. List the six injective maps $f : A \to B$.

Say why it is not possible for any map $f : A \to B$ to be surjective. [6 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 6 & 3 & 7 & 4 & 1 \end{pmatrix}, \ \rho = (1435)(267).$$

Write π, ρ, ρ^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_{15} of invertible congruence classes modulo 15. Construct a multiplication table for this group.

Find the order of each element of the group. [13 marks]

SECTION B

8. (a) Find the smallest positive integer x which satisfies the simultaneous congruences

$$x \equiv 12 \bmod 23, \quad x \equiv 9 \bmod 16.$$

Find also the next smallest positive integer that satisfies both congruences.

[8 marks]

(b) State Fermat's Theorem.

Verify that 53 is a prime number.

Use Fermat's Theorem to prove the following two assertions:

(i) $4^{26} \equiv 1 \bmod 53$;

(ii) $4^{27} + 7^{54}$ is divisible by 53. [7 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 odd integers under multiplication;

(b) the set of non-zero real numbers under multiplication;

(c) the set of non-zero congruence classes modulo 8 under multiplication modulo 8. [15 marks]

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

Determine whether or not the group G_{18} of invertible congruence classes modulo 18 is cyclic. [5 marks]

(b) Say what it means for a subset H of a group G to be a *subgroup* of G.

Now let $G = S(4)$, the group of permutations of $\{1, 2, 3, 4\}$, and let $H = \{e, (1234), (13)(24), (1432)\}$. By constructing a multiplication table for H, or otherwise, show that H is a subgroup of G.

Find the order of each element of H. [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	D	E	F	I	L	M	P
000	001	010	100	011	101	110	111

correct and read the received message:

001000 110011 110000 101111 011101 110101 011001
110110 001011.

[15 marks]