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 2944 and 1403, and find integers s and t such that

$$d=2944s+1403t.$$

[6 marks]

3. Find the inverse of 67 modulo 128. [6 marks]

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

(a) $9x \equiv 3 \bmod 18$;

(b) $9x \equiv 3 \bmod 20$;

(c) $9x \equiv 3 \bmod 21$. [10 marks]

5. Let X be the set consisting of the two elements 1 and 2, and Y the set consisting of the three elements a, b and c. List the nine maps $f : X \to Y$ and say which (if any) of these are injective, and which (if any) are surjective.

[7 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 7 & 1 & 6 & 4 \end{pmatrix}, \ \rho = (54721)(3167).$$

Write π, ρ, $\pi\rho$ 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 the class $[3]_{16}$. Hence, or otherwise, find $[3]_{16}^{-1}$. [12 marks]

SECTION B

8. (i) Find the smallest positive integer x which satisfies both the following congruences:

$$x \equiv 15 \bmod 22, \quad x \equiv 10 \bmod 23.$$

Find also the next smallest positive integer which satisfies both these congruences. [6 marks]

(ii) State Fermat's Theorem.

Verify that 149 is a prime number and show that

$$7^{150} + 10^{150} \text{ is divisible by } 149.$$

Find the smallest positive integer b such that $b \equiv 7^{151} \bmod 149$. [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 are associative.]

(a) The set of odd integers under addition;

(b) the set of integers under subtraction;

(c) the set of non-zero real numbers under multiplication.

[15 marks]

10. (i) Write down (in disjoint cycle notation) an element π of the group $S(7)$ such that π has order 12.

Write down all the integers which can occur as orders of elements of $S(6)$, and justify your answer. [6 marks]

(ii) State Lagrange's Theorem.

Let A and B be subgroups of a group G. Prove that $A \cap B$ is a subgroup of G.

Suppose now that A has 77 elements and B has 132 elements. Write down the possible orders of $A \cap B$. Deduce that $A \cap B$ is cyclic. [9 marks]

11. A group code has generator matrix

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

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	B	E	M	N	R	S	U
000	001	010	100	011	101	110	111

correct and read the received message:

0110101 1101000 1001101 0001011 0111110 1010110 1100011.

[15 marks]