SECTION A

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

$$1^3 + 2^3 + \ldots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

[6 marks]

2. Find the greatest common divisor d of 1092 and 1430, and find integers s and t such that

$$d = 1092s + 1430t.$$

[6 marks]

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

(a) $7x \equiv 13 \bmod 24$;

(b) $8x \equiv 14 \bmod 24$;

(c) $9x \equiv 15 \bmod 24$. [10 marks]

4. Verify that 193 is a prime number.

Using Fermat's Theorem, or otherwise, show that

$$7^{194} + 12^{194} \text{ is divisible by } 193.$$

[6 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) $f : \mathbf{Z}_5 \to \mathbf{Z}_5$ given by $f(x) = 4x$;

(b) $f : \mathbf{Z}_{10} \to \mathbf{Z}_{10}$ given by $f(x) = 4x$;

(c) $f : \mathbf{Z}_{10} \to \mathbf{Z}_5$ given by $f(x) = 4x$. [8 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 2 & 7 & 6 & 5 \end{pmatrix}, \quad \rho = (127463)(1856).$$

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_{20} of invertible congruence classes modulo 20. 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 51 mod 529. [6 marks]

(b) Find the smallest positive integer x which is congruent to 5 mod 22, is divisible by 7 and leaves remainder 11 when divided by 25.

Find also the next smallest positive integer with these properties. [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 even integers under addition;

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

(c) the set $\{1, 7, 11, 13\}$ under multiplication modulo 30. [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 $S(4)$ denote the group of permutations of $\{1, 2, 3, 4\}$. Subsets H and K of $S(4)$ are defined by

$$H = \{e, (1234), (13)(24), (1432)\}$$

and

$$K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

By constructing multiplication tables for H and K, or otherwise, show that H and K are both subgroups of $S(4)$.

For each of H and K, determine whether or not it is a cyclic subgroup of $S(4)$. [15 marks]

11. A group code has generator matrix

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

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:

A	D	E	P	R	S	T	U
000	001	010	100	011	101	110	111

correct and read the received message:

1011101 0110100 1001110 0111101 0111010 1011011 1000011
0100000 0111010.

[15 marks]