SECTION A

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

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

[6 marks]

2. Find the greatest common divisor d of 1802 and 1224, and find integers s and t such that

$$d = 1802s + 1224t.$$

[6 marks]

3. Find the inverse of 114 modulo 277. [6 marks]

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

(i) $12x \equiv 9 \bmod 45$;

(ii) $12x \equiv 9 \bmod 46$;

(iii) $12x \equiv 9 \bmod 47$. [10 marks]

5. Let X be the set consisting of the two elements a and b. List the four maps $f : X \to X$ and say which of these are bijective and which are not.

Write down the 4×4 table showing all possible compositions of these 4 maps. [7 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 8 & 7 & 6 & 1 & 4 \end{pmatrix}, \quad \rho = (12564)(1438).$$

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

7. List the elements of the group G_{30} of invertible congruence classes modulo 30. Construct a multiplication table for this group.

Find the order of each element of this group. [12 marks]

SECTION B

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

$$x \equiv 6 \bmod 23, \quad x \equiv 5 \bmod 31.$$

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

[6 marks]

(b) Define Euler's function $\phi(n)$ for every integer $n > 1$ and state rules by which $\phi(n)$ may be determined.

Use these rules to show that $\phi(63) = 36$ and find $\phi(64)$.

Determine the remainder when

(i) 11^{290} is divided by 63;

(ii) 11^{290} is divided by 64. [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 multiplication modulo n is associative.]

(i) The set of non-zero integers under division;

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

(iii) the set of non-zero congruence classes modulo 6 under multiplication modulo 6. [15 marks]

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

Determine whether or not the group G_{14} of invertible congruence classes modulo 14 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 $H = \{e, (12)(34), (13)(24), (14)(23)\}$. By constructing a multiplication table for H, or otherwise, show that H is a subgroup of G. Find also a subgroup K of G with four elements, containing the element (1342). [10 marks]

11. A group code has generator matrix

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

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:

I	P	T	M	N	G	R	O
000	001	010	100	011	101	110	111

correct and read the received message:

1011011 1101010 1100001 1000111 1110001 0111101 0000100
0110001 0110110.

[15 marks]