THE UNIVERSITY
of LIVERPOOL

SECTION A

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

$$\sum_{k=1}^{n} \frac{k}{2^{k-1}} = 4 - \frac{n+2}{2^{n-1}}.$$

[6 marks]

2. Find the greatest common divisor d of 3961 and 2091, and find integers s and t such that

$$d = 3961s + 2091t.$$

[6 marks]

3. Find the inverse of 179 modulo 507. [6 marks]

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

(a) $25x \equiv 10 \pmod{30}$;

(b) $25x \equiv 11 \pmod{30}$;

(c) $11x \equiv 25 \pmod{30}$. [10 marks]

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

(a) $f : \mathbf{Z}_5 \to \mathbf{Z}_5$ given by $f(x) = 2x$;

(b) $f : \mathbf{Z}_5 \to \mathbf{Z}_5$ given by $f(x) = x^2$;

(c) $f : \mathbf{Z}_2 \to \mathbf{Z}_4$ given by $f([x]_2) = [2x]_4$. [Here $[x]_n$ denotes the congruence class of x modulo n.]

[9 marks]

6. Let π, ρ be the permutations

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 2 & 3 & 7 & 4 \end{pmatrix}, \quad \rho = (237)(5471).$$

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

7. Construct a multiplication table for the group G_{18} of invertible congruence classes modulo 18.

List the elements of order 3 in this group. [10 marks]

SECTION B

8. (a) Solve the simultaneous congruences

$$x \equiv 9 \pmod{13}, \quad x \equiv 5 \pmod{17},$$

expressing your answer in the form $x \equiv a \pmod{n}$ for suitable a and n.

[6 marks]

(b) Define Euler's function $\varphi(n)$ for every integer $n > 1$. State a formula for $\varphi(pq)$, where p and q are distinct primes.

Find $\varphi(161)$.

Determine the remainder when each of the following numbers is divided by 161.

$$\text{(i) } 10^{133}; \quad \text{(ii) } 10^{265}; \quad \text{(iii) } 10^{134} + 2^{138}.$$

[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 modulo n, are associative.]

(a) The set of nonnegative integers under addition;

(b) the set of non-zero congruence classes modulo 13 under multiplication modulo 13;

(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*.

List the elements of the group G_{14} of invertible congruence classes modulo 14. Determine whether or not G_{14} is cyclic.

[5 marks]

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

Let $H = \{1, 9, 11\}$. By constructing a multiplication table for H or otherwise, show that H is a subgroup of G_{14}.

[7 marks]

(c) Find a subgroup of G_{14} which has order 2.

[3 marks]

11. A group code has generator matrix

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

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	D	G	K	L	M	O	U
000	001	010	011	100	101	110	111

correct and read the received message:

0100110 1001101 1101001 0011100 1001111 1100001 0010000 0111010

[15 marks]