SECTION A

1. Solve the following systems of equations if solutions exist

(i)
$$\begin{aligned} x - 2y + 5z &= 1 \\ 2x - 4y + 8z &= 2 \\ -3x + 6y + 7z &= 1 \end{aligned}$$

(ii)
$$\begin{aligned} x - 2y + 5z &= 1 \\ 2x - 4y + 8z &= 2 \\ -3x + 6y + 7z &= -3. \end{aligned}$$

[11 marks]

2. (a) Find the greatest common divisor d of the numbers $a = 51$ and $b = 152$. Find also integers r and s such that $ra + sb = d$.

(b) Find the inverse of 43 mod 123.

[11 marks]

3. Find solutions (if any) of each of the following congruences

(i) $4x \equiv 3 \bmod 13$.

(ii) $24x \equiv 10 \bmod 34$.

(iii) $3x \equiv 2 \bmod 9$.

[11 marks]

4. Find the eigenvalues and corresponding eigenvectors of the following matrix

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

[11 marks]

5. Permutations π and ρ are defined by

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 3 & 2 & 7 & 5 \end{pmatrix}, \text{ and } \rho = (125)(34).$$

Express π^{-1}, $\pi\rho$ and ρ^{-2} as a product of disjoint cycles and find the orders and signs of these permutations. [11 marks]

SECTION B

6. (a) Let G be a group. Say what it means for G to be cyclic. Show that the group G_{20} of invertible congruence classes mod 20 is not cyclic.

(b) Say what it means for two groups to be isomorphic. Decide with reasons, which pairs of groups in the following list are isomorphic, where C_n denotes a cyclic group of order n.

(i) C_8. (ii) $C_2 \times C_4$. (iii) G_{18}. (iv) G_{20}.

If you believe two groups in this list are isomorphic it is not necessary to prove they are isomorphic. Just describe a map between them that defines an isomorphism. [15 marks]

7. (a) A public key code has base 123 and encoding exponent 27. Find the decoding exponent. Using the letter to number equivalents

R	I	E	Q	D	T	A	B	X	Z
0	1	2	3	4	5	6	7	8	9

a message has been converted into numbers and broken into blocks. When coded using the above base and exponent it reads 05/04. Decode the message.

(ii) Say whether the function $f : G_5 \to G_5$ defined by $f(x) = 2x$ is a one to one correspondence. Justify your answer.

[Here G_n denotes the set of invertible residue classes mod n]. [15 marks]

8. (a) Assuming that multiplication of 2×2 matrices is associative, show that the set of matrices of the form

$$M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbf{R}, ab \neq 0 \right\}$$

forms a group under multiplication. Show that the set of matrices M_1 of the form

$$M_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} ; a, b \in \mathbf{R}, ab = 1 \right\}$$

forms a subgroup of M under the same operation.

(b) Suppose $\mathbf{Z}_n$ denotes the set of residue classes $\bmod n$ viewed as a group under addition. Work out the orders of all the elements in both $\mathbf{Z}_2 \times \mathbf{Z}_2$ and $\mathbf{Z}_4$ and hence decide if the two groups are isomorphic or not. Justify your conclusion. [15 marks]

9. A group code has generator matrix

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

List the codewords and state how many errors are detected and how many are corrected by this code.

Write down the parity check matrix for this code and a table of syndromes and coset leaders.

A letter is encoded with number equivalents

000 = Blank, 001 = H, 010 = E, 011 = S,
100 = F, 101 = T, 110 = R, 111 = L.

Decode the message

100110 110010 110101 010001.

[15 marks]