## SECTION A

**1.** (a) Find the greatest common divisor $d$ of 1529 and 1641 and express $d$ in the form $1529a + 1641b$ for integers $a$ and $b$. [11 marks]

(b) Find the inverse of 47 mod 153.

**2.** Solve the following systems of equations if solutions exist

(i)
$$\begin{aligned} 4x + y + z &= 3 \\ 2x + y + z &= 2 \\ 3x + y + z &= 2 \end{aligned}$$

(ii)
$$\begin{aligned} 4x + y + z &= 4 \\ 2x + y + z &= 2 \\ 3x + y + z &= 3. \end{aligned}$$

[11 marks]

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

(i) $4x \equiv 3 \bmod 22$.

(ii) $8x \equiv 4 \bmod 28$.

(iii) $8x \equiv 4 \bmod 23$.

[11 marks]

**4.** Suppose the elements $\pi$ and $\rho$ of $S(6)$ are defined by

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}, \text{ and } \rho = (261)(34)(5).$$

Calculate $\pi\rho, \pi^{-1}\rho$ and $\rho^{-1}$. Express each of these permuations as a product of disjoint cycles and determine its order and sign. [11 marks]

**5.** Let $G_n$ denote the set of invertible elements among the set of residues mod $n$. Calculate the elements of $G_{14}$ and construct their multiplication table. [11 marks]

## SECTION B

**6.** (a) Find the eigenvalues and corresponding eigenvectors of the matrix

$$A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix}.$$

[15 marks]

**7.** (a) A public key code has base 143 and encoding exponent 11. Find the decoding exponent. Using the letter to number equivalents

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| *Z* | *C* | *L* | *A* | *U* | *S* | *E* | *R* | *T* | *Blank* |

a message has been converted into numbers and broken into blocks. When coded using the above base and exponent it reads 12/02. Decode the message.

(b) Using the Fermat-Euler theorem or otherwise, show that $5^{400} + 15$ is divisible by 16. [15 marks]

**8.** State the Chinese Remainder Theorem concerning simultaneous solution of congruences

$$x \equiv a \bmod n \text{ and } x \equiv b \bmod n.$$

Find the smallest positive integer with last digit 5, whose remainder when divided by 27 is 9 and which is divisible by 7. [15 marks]

**9.** A group code has generator matrix

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

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

Write down the parity check matrix and table of syndromes for this code for all possible single digit errors in transmission. A message is encoded with number-letter equivalents

000 = A, 100 = B, 010 = C, 001 = E,
110 = G, 101 = H, 011 = R, 111 = S.

Decode the message

0101011 1111010 0011101 0011001 0110110 1110001.

[15 marks]