Discrete Mathematics I

(a) State and prove the Chinese Remainder Theorem concerning the simultaneous solution of two congruences to co-prime moduli and the uniqueness of that solution. [8 marks]

(b) Consider an extension to solve a set of \( r \) simultaneous congruences:

\[
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\vdots \\
x \equiv a_r \pmod{m_r}
\]

where \( i \neq j \Rightarrow (m_i, m_j) = 1 \) and \( M = m_1m_2\ldots m_r \).

(i) Prove that \( (m_i, M/m_i) = 1 \) for \( 1 \leq i \leq r \). [3 marks]

(ii) Explain briefly how to find \( s_i \) and \( t_i \) so that \( m_is_i + M/t_i/m_i = 1 \) for \( 1 \leq i \leq r \). It is not necessary to give a detailed algorithm. [2 marks]

(iii) Let \( c = a_1t_1m_2m_3\ldots m_r + m_1a_2t_2m_3\ldots m_r + m_1m_2a_3t_3\ldots m_r + \cdots + m_1m_2m_3\ldots a_rt_r \). Show that \( c \equiv a_i \pmod{m_i} \) for \( 1 \leq i \leq r \). [4 marks]

(iv) Show further that the solution is unique modulo \( M \). [3 marks]