# 1998 Paper 1 Question 7

## Discrete Mathematics

State and prove the Chinese Remainder Theorem concerning the simultaneous solution of a pair of congruences to co-prime moduli and the uniqueness of that solution. [10 marks]

An early form of public key encryption worked as follows. A person, $R$, wishing to receive secret messages, selected two large primes, $p$ and $q$ also co-prime to $p-1$ and $q-1$, and published their product, $n = p \times q$. Another person, $S$, wishing to send a message $m$ to $R$, encoded it as $s = m^n (\text{mod } n)$.

Show how to calculate inverses $a$ and $b$ so that $ap \equiv 1(\text{mod } q-1)$ and $bq \equiv 1(\text{mod } p-1)$. By considering $s^a(\text{mod } q)$ and $s^b(\text{mod } p)$ and recalling the Fermat–Euler theorem, show how $R$ could recover the original message, $m$. State clearly any other results that you use. [10 marks]