Question 5 (Units 3 and 4) – 10 marks

This question is concerned with solutions of the congruence $x^2 \equiv 1 \pmod{pq}$, where p and q are distinct odd primes.

(i) Prove that an integer x satisfies $x^2 \equiv 1 \pmod{pq}$ if, and only if, x satisfies both

$$x^2 \equiv 1 \pmod{p} \quad \text{and} \quad x^2 \equiv 1 \pmod{q}\,. \qquad [2]$$

(ii) Explain why $x^2 \equiv 1 \pmod{p}$ has just the two solutions $x \equiv \pm 1 \pmod{p}$. [2]

(iii) From part (ii), any integer satisfying $x^2 \equiv 1 \pmod{p}$ is either of the form $x = 1 + kp$ or of the form $x = -1 + k'p$ for integers k and k'.

(a) Show that $x = 1 + kp$ also satisfies $x^2 \equiv 1 \pmod{q}$ if, and only if, either

$$k \equiv 0 \pmod{q} \quad \text{or} \quad kp + 2 \equiv 0 \pmod{q}\,. \qquad [2]$$

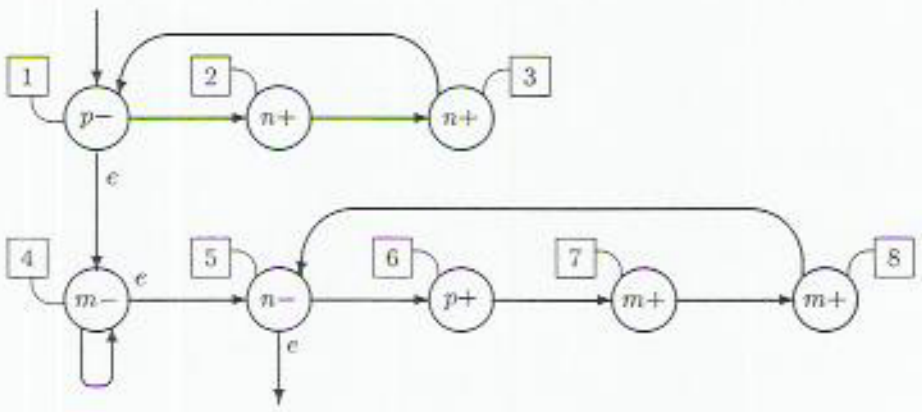
(b) What are the corresponding conditions on k' when $x = -1 + k'p$ also satisfies $x^2 \equiv 1 \pmod{q}$? [2]

(iv) Use the above results to solve the equation $x^2 \equiv 1 \pmod{7 \times 13}$. [2]

Mathematical Logic

Question 6 (Unit 2) – 10 marks

This question concerns the abacus machine whose flow chart is shown below.



(i) Write down the trace table for the computation of this machine when initially the contents of the registers are:

$$[m] = 2, \quad [n] = 1, \quad [p] = 1. \qquad [4]$$

(ii) Suppose that m, n, p initially contain respectively the first, second and third arguments of a function f and that the value of f is given by the content of register m when the computation halts.

(a) Write down a formula which describes the rule of f. [2]

(b) How are the final contents of registers n and p related to the initial contents of the three registers? [4]