

Question 4 (Unit 4) - 12 marks

(i) Applying Wilson's Theorem for the prime 11, deduce that:

$$\begin{aligned} 9! &\equiv 1 \pmod{11} \\ 2! \times 8! &\equiv -1 \pmod{11} \\ 3! \times 7! &\equiv 1 \pmod{11} \\ 4! \times 6! &\equiv -1 \pmod{11} \\ 5! \times 5! &\equiv 1 \pmod{11} \end{aligned}$$

Prove the general result which this illustrates, namely

$$(n-1)! \times (p-n)! \equiv (-1)^n \pmod{p}$$

for p prime and n integer with $1 \leq n \leq p$.

[5]

(ii) (a) Prove that an integer $m = 4k + 3$ is prime if and only if

$$((2k+1)!)^2 \equiv +1 \pmod{m}.$$

[Note that this result is illustrated in part (i) for the case $k = 2$.]

[5]

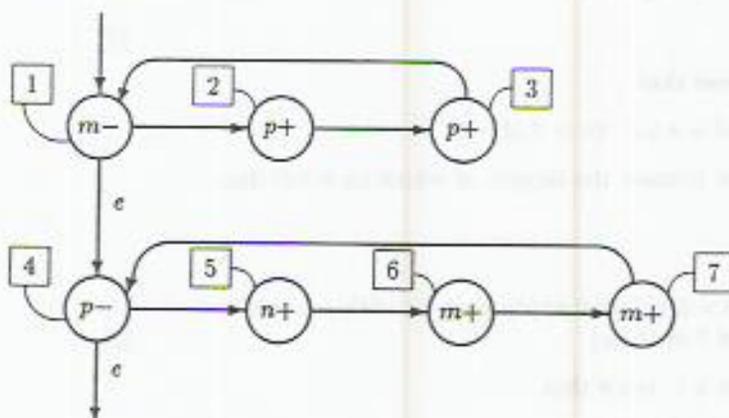
(b) Write down the corresponding result for an integer $m = 4k + 1$.

[2]

Mathematical Logic

Question 5 (Unit 2) - 10 marks

Let A be the abacus machine whose flow chart is as follows.



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

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

[4]

(ii) Suppose that m , n and 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 n when the computation halts.

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

(b) How are the final contents of registers m and p related to the initial contents of the three registers?

[6]