1996 Paper 9 Question 6

Advanced Algorithms

Explain the steps involved in using the Miller–Rabin test to check whether a number N is composite. This will involve computing $a^{N-1} \bmod N$ for some value of a.

[10 marks]

Carry out the steps for $N = 65$ and $a = 1, 2, 8$ and 12. Comment on what (if anything) each partial result tells you about N and which cases (if any) help you to decide whether N is prime or what its factors might be.

Pretend throughout the calculation that you do not know that $65 = 5 \times 13$. Proceed as though 65 were a huge number, imagining that you do not know at the outset whether it is prime or composite and that you are certainly unable to spot any factors.

[10 marks]