2002 Paper 9 Question 8

Advanced Algorithms

(*a*) Explain how to check a large number for primality using a probabilistic method that gives you a bound of the probability of getting an incorrect judgment. [7 marks]

(*b*) Give an asymptotic formula predicting the number of computer operations needed to verify that a number with n bits is prime, supposing that multiplication, division and remaindering are done using $O(n^2)$ methods and that you want to achieve a probability of error bounded by 1 in 2^{60}. You do not need to prove that the algorithm you describe works, but you should nevertheless explain it carefully and completely. [7 marks]

(*c*) The gap between adjacent primes near the integer N is roughly $\log(N)$. Estimate roughly the number of computer operations you would expect to be needed to find a 2000-bit prime that is just slightly larger than some given 2000-bit random number. [6 marks]