SOLUTION NOTES

Advanced Algorithms 2002 Paper 9 Question 8 (ACN)

Syllabus section 3 on Probabilistic algorithms, with some reference to this as a practical application coming from both the "big arithmetic" bit in the syllabus and from Part Ia discrete maths where RSA is described and justified.

(a) Usual "strong" test as per notes

(b) For a b-bit number we need around b multiplications/squarings, each of which costs b^2, so I see b^3 per trial. We need 60 trials - whether you then show that factor here is not terribly important (it will show up in the final part anyway!)

(c) get between primes is around 2000 (supposing wrongly we use logs base 2! Maybe a bonus point for people who are careful with log bases!). From random number to next prime is thus around 1000. Only need to check odd numbers so 500. For each of these usually the first Rabin trial will show composite, so we need say 499+60 exponentiations (499 composite, one prime). Each costs $(2000/32)^3$ say times 10 computer ops because of 32 bit word. I end up 60*60*60*10*600 $= 6 * 6 * 6 * 6 * 10^6$ $= 36 * 36 * 10^6 = 10^3 * 10^6 = 10^9$ but the numeric result will be viewed as much less important than a proper consideration of where it comes from, including the fact that most non-primes are detected rapidly but the final prime needs full checking.