1 Complexity Theory (tg508)

Let Factor be the *decision* problem where given a pair of integers (x, k), the goal is to decide whether x has a factor smaller than k. Let Factoring be the *search* problem, where given an integer x, the goal is to output a prime factorisation of x. (In the following, carefully note the distinction between Factor and Factoring.)

(*a*) Prove that $\mathsf{Factor} \in \mathsf{NP} \cap \mathsf{coNP}$. [5 marks]

(*b*) Prove that if $\mathsf{P} = \mathsf{NP} \cap \mathsf{coNP}$, then there exists a polynomial-time algorithm for Factoring. [7 marks]

(*c*) Define the class BQP. Is $\mathsf{Factoring} \in \mathsf{BQP}$? [4 marks]

(*d*) Show that a quantum (BQP) algorithm for a problem P, which is correct with probability $2/3$ over the measurement, can be amplified into a quantum algorithm for P, which is correct with probability $1 - o(1)$ over the measurement. [4 marks]