Computational Number Theory
Quiz 5

1. Suppose we are given a positive integer n with the promise that n is of the form $n = p^2q$. How efficiently can we factor n using the Pollard rho algorithm? [**3 marks**]

2. Let $n, a, B \in \mathbb{N}$, $a \leq n^2$, $b \leq n$. Let $S = \{x^2 - 2 : x \in \{a+1, a+2, \ldots, a+n\}\}$. Describe an $\tilde{O}(n)$ algorithm to factorize all the B-smooth numbers in S.

3. Let n be a product of distinct odd primes such that $(p-1)|(n-1)$ for all $p|n$. Let $r \in \mathbb{N}$ be such that $r|(p-1)$ for all $p|n$. Eg: $n = 1729 = 7 \times 13 \times 19$; $r = 3$. Show that n fails the AKS primality test if $x^r - 1$ is used as the modulus polynomial.