Theory of Computation

Solutions to Homework 5

Problem 1. Let p, q be two distinct primes. Recall that the RSA function, shown on pages 551–558 in the slides, is $x^e \bmod pq$ for an odd e relatively prime to $\phi(pq)$. Show that the RSA function is not secure when q is restricted to be $p+2$. That is, given the binary representations of pq, e and $x^e \bmod pq$ as inputs, show how to compute $x \bmod pq$ in time polynomial in the input length, provided the following conditions hold:

1. $q = p + 2$.
2. p and q are distinct primes.
3. e is odd and relatively prime to $\phi(pq)$.

Problem 2. Show that if SAT has no polynomial circuits, then coNP $\neq$ BPP. (Hint: Adleman's theorem states that all languages in BPP have polynomial circuits.)