Theory of Computation

Homework 4

Due: 2014/12/9

Problem 1 Show that VALIDITY is coNP-complete.

Problem 2 Recall that the Jacobi symbol is given by $(a|m) = \prod_i^k (a|p_i)$ for any odd integer $m = p_1 p_2 \dots p_k$, $m > 1$, and $\gcd(a, m) = 1$. Show that $(-1|m) = (-1)^{(m-1)/2}$ for any odd integer m. (You may use the Legendre symbol $(a|p) = a^{\frac{p-1}{2}}$ for any odd prime p and $a \neq 0 \mod p$.)