Theory of Computation

Final-Term Examination on January 10, 2012

Fall Semester, 2011

Note: You may use any results proved in class.

Problem 1 (25 points)**.** Prove that L is **NP**-complete if and only if its complement $\bar{L}$ is **coNP**-complete.

Problem 2 (25 points)**.** The Jacobi symbol $(a \mid m)$ is the extension of the Legendre symbol $(a \mid p)$, where p is an odd prime, and

$$(a \mid p) = \begin{cases} 0 & \text{if } (p \mid a)\,, \\ 1 & \text{if } a \text{ is a quadratic residue module } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue module } p. \end{cases}$$

Recall that when $m > 1$ is odd and $\gcd(a, m) = 1$, then $(a \mid m) = \prod_{i=1}^{k} (a \mid p_i)$. Please calculate $(1234 \mid 99)$. Please write down the steps leading to your answer.

Problem 3 (25 points)**.** Let $\mu \equiv E[X]$ and $\sigma^2 \equiv E[(X-\mu)^2]$ be finite. Show that

$$\text{prob}[|X - \mu| \geq k\sigma] \leq 1/k^2$$

for $k \geq 0$.
(Hints: The Markov inequality says: $\text{prob}[Y \geq m] \leq E[Y]/m$ if random variable Y takes on only nonnegative values and $m \geq 0$. Try $Y = (X - \mu)^2$.)

Problem 4 (25 points)**.** Please define RP and prove that RP $\subseteq$ NP.