Theory of Computation

Final Examination on January 7, 2014
Fall Semester, 2013

Problem 1 (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 all the steps leading to your answer.

Ans: $(1234 \mid 99) = (46 \mid 99) = (46 \mid 9)\,(46 \mid 11) = (1 \mid 9)\,(2 \mid 11) = 1 \cdot (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$. ■

Problem 2 (25 points) 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.)

Ans: Assume that SAT has no polynomial circuits. As all languages in BPP have polynomial circuits by Adleman's theorem, NP $\neq$ BPP. Hence coNP $\neq$ coBPP $=$ BPP. ■

Problem 3 (25 points) Consider the sequence $a_1, a_2, \ldots$ defined by

$$a_n = 2^n + 3^n + 6^n - 1 \ (n = 1, 2, \ldots)$$

Determine all positive integers that are relatively prime to every term of the sequence. (Hint: Fermat's little theorem says that for all $0 < a < p, a^{p-1} \equiv 1 \mod p$.)

Ans: If $p > 3$ is a prime, then $a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod p$. To see this, multiply both sides by 6 to get

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 6 \,(\mathrm{mod}\ p)$$

which is a consequence of Fermat's little theorem. Therefore p divides a_{p-2}. Also 2 divides a_1 and 3 divides a_2. So there is no number other than 1 that is relatively prime to all the terms in the sequence. ■

Problem 4 (25 points) Let $G = (V, E)$ be an undirected graph in which every node has a degree of at most k. Let I be a nonempty set. I is said to be independent if there is no edge between any two nodes in I. k-DEGREE INDEPENDENT SET asks if there is an independent set of size k. Consider the following algorithm for k-DEGREE INDEPENDENT SET:

$I := \emptyset$;
while $\exists v \in G$ **do**
    Add v to I;
    Delete v and all of its adjacent nodes from G;
end while;
return I;

Show that this algorithm for k-DEGREE INDEPENDENT SET is a $\frac{k}{k+1}$-approximation algorithm. Recall that an ϵ-approximation algorithm returns a solution that is at least $(1 - \epsilon)$ times the optimum for maximization problems.

Ans: Since each stage of the algorithm adds a node to I and deletes at most $k + 1$ nodes from G, I has at least $\frac{|V|}{k+1}$ nodes, which is at least $\frac{1}{k+1}$ times the size of the optimum independent set because the size of the optimum independent set is trivially at most $|V|$. Thus this algorithm returns solutions that are never smaller than $1 - \frac{1}{k+1} = \frac{k}{k+1}$ times the optimum. ■