Special instructions: You may work either individually or in a group of exactly two persons. Write your solutions out on paper and deliver them (with one photocopy thereof) to SSO by 12:00 on Wednesday, 2nd December, 2015. If you are working in a group, one script should be submitted for the group, with both names at the top; both members of the group will then receive the same mark. Clearly write your name(s), student ID number(s) and the words "Comp36111 Sec. B Coursework" on the front (cover) sheet and staple all sheets together. Submitted solutions must be entirely the effort of the persons whose names appear at the top of the submission.

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Advanced Algorithms I: Coursework for Sec. B

Time: This should take you about six hours

Please answer all questions.

Marks will be awarded for clarity and succinctness as well as correctness.

The use of electronic calculators is not recommended.

Section B

In this coursework, we are going to show that the problem

PRIMES
Given: a positive integer n represented as a decimal string
Output: Y if n is a prime; N otherwise

is in NPTIME $\cap$ coNPTIME. Remember that the size of the input is the number of bits in the string representing n, and hence at least $\lfloor \log_2 n \rfloor + 1$. We rely on the following theorem (which you need not prove).

Theorem 1. *A number $p > 1$ is prime if and only if there is a number r $(1 < r < p)$ such that $r^{p-1} = 1 \mod p$ and, furthermore, $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p-1$.*

So, if p is prime, we can 'verify' this fact by taking the prime divisors $q_1, \ldots, q_m$ of $p-1$, and checking the condition given in the theorem. Of course, we also need to check that the $q_1, \ldots, q_m$ really *are* the prime divisors of $p-1$. In particular, we need to check that they are prime. So we define, recursively, a *certificate of putative primeness* (or CPP) for any prime p, as follows. If $p = 2$, then $\mathrm{CPP}(p) = \star$ (some special symbol). Else,

$$\mathrm{CPP}(p) = (r; q_1, \mathrm{CPP}(q_1), q_2, \mathrm{CPP}(q_2), \ldots, q_m, \mathrm{CPP}(q_m)), \tag{1}$$

where r, and $q_1, \ldots, q_m$ are as guaranteed by the theorem. That is: together with the number r, we list the prime divisors of $p-1$ along with certificates showing that they are prime.

1. Show that PRIMES is in coNPTIME. [*Hint*: forget the above theorem.] (2 marks)

2. Give a polynomial time algorithm for computing $a^b \mod p$, where p is a prime and a and b are positive integers less than p. [*Hint*: your algorithm must be polynomial in the number of bits in the input.] (4 marks)

3. Show informally that it is possible to verify in polynomial time that $p-1$ factorizes into $q_1, \ldots, q_m$ (where the factors may occur more than once, i.e. $p-1 = q_1^{d_1} \cdot \cdots \cdot q_m^{d_m}$ for some positive $d_1, \ldots, d_m$). (4 marks)

4. Show that, if $q_1, \ldots, q_m$ are the prime factors of $p-1$, then $m < \log_2 p$. (4 marks)

5. Denote the number of symbols in $\mathrm{CPP}(p)$ by $|\mathrm{CPP}(p)|$. Here we may assume that $\mathrm{CPP}(2) = \star$ takes 1 symbol to write. Taking $\mathrm{CPP}(p)$ to have the form (1), and noting that, without loss of generality, $q_1 = 2$, show that, for any prime $p > 2$,

$$|\mathrm{CPP}(p)| \leq 5 \log_2 p + 4 + \sum_{i=2}^{m} |\mathrm{CPP}(q_i)|. \tag{2}$$

[*Hints*: How many bits are there in the $q_1, \ldots, q_m$, taken together? And r? How many separators are in CPP(p)? And don't forget the enclosing parentheses!]

(4 marks)

6. It is possible to show by induction that $|\mathrm{CPP}(p)| \leq 5(\log p)^2$. This is true by inspection for $p = 2$ or $p = 3$. For $p \geq 5$, we apply (2). By inductive hypothesis $\sum_{i=2}^{m} |\mathrm{CPP}(q_i)| \leq 5\sum_{i=2}^{m} (\log q_i)^2$. Now $\sum_{i=2}^{m} \log q_i = \log \prod_{i=2}^{m} q_i \leq \log_2 p - 1$. Hence $5\sum_{i=2}^{m} (\log q_i)^2 \leq 5(\log_2 p - 1)^2$, whence, from (2), $|\mathrm{CPP}(p)| \leq 5\log_2 p + 4 + 5(\log_2 p)^2 - 10\log_2 p + 5 = 5(\log_2 p)^2 + [9 - 5\log_2 p] < 5(\log_2 p)^2$ when $p \geq 5$. Explain why, together with the above results, this shows that PRIMES is in NPTIME. (2 marks)

It was established by Agrawal, Kayal and Saxena in 2002 that PRIMES is in fact in PTIME.

END OF EXAMINATION