CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 9 *Spring 2019*

1. Factor the integer $N = 2028455971$.

   Hint: For $s = 702505371$ and $t = 188270011$ we observe that $s^2 \equiv t^2 \pmod{N}$ holds.

2. De Bruijn's lower bound. Show that for all $x \geq 1$ and $k \in \mathbb{Z}_{\geq 1}$ we have $\Psi(x^k, x) \geq \binom{\pi(x)+k}{k} \geq \left(\frac{\pi(x)}{k}\right)^k$.

   Hints: Recall that we write $\Psi(M, B)$ for the number of B-smooth positive integers at most M and $\pi(x)$ for the number of prime numbers at most x. For the first inequality, recall that $\binom{n+k}{k}$ counts the nonnegative integer solutions $z_1, z_2, \ldots, z_n$ of the inequality $z_1 + z_2 + \ldots + z_n \leq k$. For the second inequality, recall that $\binom{m}{k} = m!/(k!(m-k)!)$.

3. Given an integer $N \in \mathbb{Z}_{\geq 2}$ as input, design an algorithm that either (i) outputs a prime p and a positive integer a such that $N = p^a$ or (ii) asserts that N is not a prime power. Your algorithm should run in time $O((\log N)^c)$ for a constant $c > 0$. Carefully justify the running time of your algorithm. You may assume that you have available a subroutine that tests whether a given $m \in \mathbb{Z}_{\geq 2}$ is prime in time $O((\log m)^d)$ for a constant $d > 0$.

   Hints: Design an algorithm for the following problem. Given integers $N, k \in \mathbb{Z}_{\geq 2}$ as input, find the largest integer b such that $b^k \leq N$. You may want to make use of binary search. Try out different values of k to work out whether N is a prime power.

4. Number of square roots and Hensel lifting. Let N be odd with r distinct prime factors and let t be an integer coprime to N. Show that the congruence $s^2 \equiv t^2 \pmod{N}$ admits exactly 2^r integer solutions $s \in \{1, 2, \ldots, N-1\}$ coprime to N.

   Hints: Let $N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the factorization of N. We have that t is coprime to N if and only if none of $p_1, p_2, \ldots, p_r$ divides t. By the Chinese Remainder Theorem, we have $s^2 \equiv t^2 \pmod{N}$ if and only if $s^2 \equiv t^2 \pmod{p_i^{a_i}}$ holds for all $i = 1, 2, \ldots, r$. Recall from previous week's problem set that modulo an odd prime p there exist exactly two distinct solutions s to $s^2 \equiv t^2 \pmod{p}$, namely $s \equiv t \pmod{p}$ and $s \equiv -t \pmod{p}$. For an odd prime p and an integer u coprime to p, show that if $x_e \in \{0, 1, \ldots, p^e - 1\}$ is a solution to the congruence $x_e^2 \equiv u \pmod{p^e}$ for a positive integer e, then there is a unique lift $x_{e+1} \in \{0, 1, \ldots, p^{e+1} - 1\}$ with $x_{e+1} \equiv x_e \pmod{p^e}$ and $x_{e+1}^2 \equiv u \pmod{p^{e+1}}$. Try $x_{e+1} = x_e + yp^e$ for $y \in \{0, 1, \ldots, p-1\}$ and solve for y.

Deadline and submission instructions. This problem set is due no later than Sunday 31 March 2019, 20:00 (8pm), Finnish time. Please submit your solutions as a single PDF file via e-mail to the lecturer (`petteri.kaski(atsymbol)aalto.fi`). Please use the precise title

```
CS-E4500 Problem Set 9: [your-student-number]
```

with "`[your-student-number]`" replaced by your student number. For example, assuming that my student number is 123456, I would carefully title my e-mail

```
CS-E4500 Problem Set 9: 123456
```

and attach to the e-mail a single PDF file containing my solutions. Please note that the submissions are automatically processed and archived, implying that failure to follow these precise instructions may result in your submission not being graded.