1 Factorization problems

Let us consider the three following problems :
— FINDSMALLESTFACTOR given $N \in \mathbb{N}^*$ find the smallest $k \in \mathbb{N}$ with $k \geq 2$ such that k divide N.
— FINDGREATESTFACTOR given $N \in \mathbb{N}^*$ find the biggest $k \in \mathbb{N}$ with $k < N$ such that k divide N.
— HASFACTOR given $(N, M) \in \mathbb{N}^{*2}$ decide whether there exists a non-trivial factor of N smaller than M.

Exercice 1. Show that, if you can solve any of these problems in polynomial time, then you can solve all of these problems in polynomial time. Beware that the time is considered in the size of the input which is logarithmic in the considered numbers.

Exercice 2. Show that these problems are $\mathcal{NP}$. *You can assume that the primality test is* $\mathcal{P}$.

Exercice 3. Show that these problems are co-$\mathcal{NP}$.

2 Closure properties

Exercice 4. Show that the set of languages decidable in polynomial time is stable by intersection, union, complementation and star (i.e. the language L^*).

3 One-way functions

Let us suppose that :
— we have f a one-to-one function over integers with n bits towards integers with n bits for all n (i.e., given an input x with n bits, $f(x)$ is an integer with n bits such that $f(x) = f(y) \Rightarrow x = y$) ;
— f can be computed in polynomial time ;
— the inverse function of f cannot be computed in polynomial time. (It is thus called a one-way function).

Exercice 5.
Show that, if such a function exists then $\mathcal{P} \neq \mathcal{NP}$
Suggestion : Show that the language $L = \{(x, f(y)) : x < y\}$ *belongs to* $\mathcal{NP} \setminus \mathcal{P}$.

Exercice 6. Such that, if such a function exists, then $\mathcal{NP} \cap \text{co-}\mathcal{NP} \neq \mathcal{P}$.

4 Quines

Given two TM A et B we note $A \cdot B$ a TM executing B after having executed A.
For each $w \in \Sigma^*$, let $P(w)$ be a TM over Σ writing w on the tape.

Exercice 7. Justify with $q : \mathbb{N} \to \mathbb{N}$ is computable ?

$$q(n) = \begin{cases} \langle P(w) \rangle & \text{s'il existe } w \in \Sigma^* \text{ tel que } n = \langle w \rangle \\ \bot & \text{sinon} \end{cases}$$

Exercice 8. Justify why $s_2(m, n) : \mathbb{N}^2 \to \mathbb{N}$ is computable

$$s_2(m, n) = \begin{cases} \langle A \cdot B \rangle & \text{s'il existe } A, B \text{ telles que } \langle A \rangle = m \wedge \langle B \rangle = n \\ \bot & \text{sinon} \end{cases}$$

Exercice 9. Deduce from the previous questions that there exists a TM M that halts by printing $\langle M \rangle$ on the tape.