# TD 04 – Informantique

**Exercice 1.** *Théorème de Ladner*

**Définition.** Pour toute fonction $F : \mathbb{N} \to \mathbb{N}$, on définit

$$\text{SAT}_F = \left\{ \psi 01^{n^{F(n)}} \mid \psi \in \text{SAT et } n = |\psi| \right\}$$

**Définition.** On définit la fonction $H$ ainsi : $H(0) = H(1) = 1$ et pour $n \geq 2$, $H(n)$ est le plus petit $i < \log\log n$ tel que pour tout $x \in \{0,1\}*$ avec $|x| < \log n$, la machine $M_i$ calcule $\text{SAT}_H(x)$ sur l'entrée $x$ en au plus $i|x|^i$ étapes. Si un tel $i$ n'existe pas, on pose $H(n) = \lceil \log\log n \rceil$.

1. Montrer que la fonction $H$ est bien définie.
2. Montrer que si $\text{SAT}_H \in \mathsf{P}$ alors $H(n) = O(1)$.
3. Montrer que si $\text{SAT}_H \notin \mathsf{P}$ alors $H(n) \underset{n\to\infty}{\to} \infty$.
4. Montrer que la fonction $H$ est calculable en temps polynômial en $n$.

On suppose pour les deux prochaines questions que $\mathsf{P} \neq \mathsf{NP}$.

5. Montrer que $\text{SAT}_H \notin P$.
6. Montrer que $\text{SAT}_H$ n'est pas NP-complet.
7. Conclure

**Exercice 2.** *Depuis Ératosthène...*

PRIMES est dans NP [1].

1. PRIMES est-il dans coNP ? dans P ?

On admettra [2] dans la suite qu'un entier $n$ est premier si et seulement si il existe un nombre $a$ dans $[1, n-1]$ tel que
– $a^{n-1} \equiv 1 \mod n$
– $\forall q \in \mathbb{P} : q|(n-1), a^{n-1/q} \not\equiv 1 \mod n$

2. Avec cette définition, montrer que PRIMES est dans NP.

**Exercice 3.** *Comme pour Pythagore*

On définit les deux réductions suivantes :
– *many-one* ou *Karp* : $A \leq_m^p B \iff \exists f \in \mathsf{FP}, (x \in A \iff f(x) \in B)$
– *par oracle* ou *Cook-Turing* : $A \leq_T^p B \iff A \in \mathsf{P}^B$

1. Quelle est la réduction vue en cours ?
2. Montrer que TAUTOLOGIE $\in \mathsf{P}^{\text{SAT}}$, et plus généralement que pour tout $A$, $\bar{A} \leq_T^p A$.

1. On n'utilisera pas l'algorithme AKS pour répondre aux questions suivantes...
2. Il s'agit du test de primalité de Lucas connu depuis la fin du XIX$^{\text{e}}$ siècle. (cf. wikipedia si vous voulez des détails).

**3.** Montrer que pour tout $A \in \mathsf{P}$, $\mathsf{P}^A = \mathsf{P}$.

**4.** Montrer que $\leq_T^p$ est transitive ($A \leq_T^p B$ et $B \leq_T^p C$ impliquent $A \leq_T^p C$).

**5.** Montrer que si TAUTOLOGIE $\leq_m^p$ SAT alors $\mathsf{NP} = \mathsf{coNP}$.

**6.** Montrer que $\mathsf{NP} = \mathsf{coNP}$ ssi NP est close pour $\leq_T^p$ ($A \leq_T^p B$ et $B \in \mathsf{NP} \implies A \in \mathsf{NP}$).

**7.** Quelles relations existent entre $\leq_m^p$ et $\leq_T^p$ ?