Complexité

1 Somme des sous-ensembles

Le *problème de la somme des sous-ensembles* consiste, étant donné un ensemble fini d'entiers, à déterminer s'il existe un sous-ensemble non-vide dont la somme des éléments est nulle.

Question 1.1. *Montrer que ce problème est dans NP.*

2 Étoiles

Étant donné un langage $A \subseteq \Sigma^*$, on note A^* le langage formé des mots de la forme $\omega_1 \cdots \omega_n$ où pour tout i, $\omega_i \in A$, y compris le mot vide.

Question 2.1. *Soit A un langage dans NP. Montrez que A^* est dans NP.*

Question 2.2. *Soit A un langage dans P. Montrez que A^* est dans P.*

3 Primalité

Soit PRIMES l'ensemble des entiers naturels premiers, écrits en *binaire*.

Question 3.1. *Donnez un algorithme « simple » de test de primalité (appartenance à PRIMES). Quelle est sa complexité ?*

Question 3.2. *Montrez que PRIMES est dans co-NP (c'est-à-dire que son complémentaire est dans NP).*

Question 3.3. *Peut-on déduire de la question précédente que PRIMES est dans NP ?*

On admet le résultat suivant, appelé *théorème de Lehmer* : un nombre $n > 2$ est premier si et seulement s'il existe $1 < a < n$ tel que $a^{n-1} \equiv 1 \pmod{n}$ et pour tout facteur premier q de $n-1$, $a^{(n-1)/q} \not\equiv 1 \pmod{n}$.

Question 3.4. *Montrez que PRIMES est dans NP.*

Note culturelle

On sait depuis 2002 que PRIMES est en fait dans P, mais la preuve est trop compliquée pour être donnée en PC... En pratique, on n'utilise de toute façon pas le test déterministe en temps polynomial, mais un test probabiliste beaucoup plus rapide, dont on peut rendre aussi petite que l'on veut la probabilité de pouvoir se tromper en déclarant qu'un nombre est premier alors qu'il ne l'est pas.