Sélection Internationale **Session 2007**
Ecole Normale Supérieure
Epreuve de culture scientifique - **Informatique** Durée : 4 heures

Premier Exercice : Combinaisons linéaires

On note $\mathbb{Z}$ l'ensemble des entiers relatifs. Pour tout couple $(a, b) \in \mathbb{Z}^2$, on note $L(a, b)$ l'ensemble $\{ax + by \text{ où } (x, y) \in \mathbb{Z}^2\}$ des combinaisons linéaires de a et b.

Question-1. Montrer qu'il existe un unique entier $\pi(a, b) \geq 0$ tel que $L(a, b)$ soit l'ensemble des multiples de $\pi(a, b)$, c'est-à-dire :

$$L(a, b) = \pi(a, b)\mathbb{Z}.$$

Pour tout $(a, b) \in \mathbb{Z}^2$ où $b \neq 0$, on note $a \bmod b$ le reste de a modulo b, c'est-à-dire l'unique entier $r \in \mathbb{Z}$ tel que $0 \leq r < |b|$ et que b divise l'entier $a - r$. On considère l'algorithme suivant :

Algorithme 1 Calcul de $\pi(a, b)$

Entrée : Deux entiers a et b positifs.
1: **si** $a \leq b$ **alors**
2: échanger a et b.
3: **fin si**
4: **Tant que** $b \neq 0$ **faire**
5: $r \longleftarrow a \bmod b$.
6: $a \longleftarrow b$.
7: $b \longleftarrow r$.
8: **fin Tant que**
9: renvoyer a.

Question-2. Montrer que l'algorithme 1 termine en un nombre fini d'étapes.

Question-3. Montrer que l'algorithme 1 renvoie $\pi(a, b)$.

Question-4. Montrer que le nombre d'itérations de la boucle (étapes 4 à 8) de l'algorithme 1 est au plus linéaire en n, où n est un majorant du nombre de bits des entiers a et b : $0 \leq a, b < 2^n$.

Question-5. Modifier l'algorithme 1 de façon à ce qu'il renvoie en plus deux entiers x et y tels que $ax + by = \pi(a, b)$.

Question-6. En déduire un algorithme qui, étant donné un quadruplet d'entiers $(a, b, n, m) \in \mathbb{Z}^4$ tel que $\pi(a, b) = 1$, renvoie un entier α tel que $\alpha - n$ soit divisible par a, et que $\alpha - m$ soit divisible par b.

Deuxième Exercice : Sommes partielles

Le problème des sommes partielles est le suivant : étant donnés un entier s d'au plus ℓ bits, et n entiers $a_1, \ldots, a_n$ d'au plus ℓ bits, décider s'il existe $(x_1, \ldots, x_n) \in \{0,1\}^n$ tels que $s = \sum_{i=1}^{n} x_i a_i$, et si la réponse est affirmative, exhiber un tel $(x_1, \ldots, x_n) \in \{0,1\}^n$.

On évaluera le coût des algorithmes de façon usuelle : le temps de calcul sera mesuré en nombre d'opérations élémentaires sur des bits, et l'espace mémoire sera mesuré en bits. On admettra qu'une liste de m entiers d'au plus ℓ bits puisse être triée en temps $O(m\ell \log m)$. Pour simplifier les analyses, on notera $\mathsf{poly}(n, \ell)$ toute fonction de n et ℓ qui soit au plus polynomiale en n et ℓ, c'est-à-dire qu'il existe des entiers c_1, c_2 et c_3 tels que la fonction soit inférieure à $c_1 \times n^{c_2} \ell^{c_3}$. Par exemple, multiplier n entiers de ℓ bits coûte $\mathsf{poly}(n, \ell)$.

Question-1. Montrer que l'on peut résoudre le problème des sommes partielles en temps $2^n \mathsf{poly}(n, \ell)$.

Question-2. On suppose ici que n est pair. Montrer que l'on peut résoudre le problème des sommes partielles en temps $2^{n/2} \mathsf{poly}(n, \ell)$ et espace $2^{n/2} \mathsf{poly}(n, \ell)$.

Question-3. On suppose ici que n est un multiple de quatre. Montrer que l'on peut résoudre le problème des sommes partielles en temps $2^{n/2} \mathsf{poly}(n, \ell)$ et espace $2^{n/4} \mathsf{poly}(n, \ell)$.

Sélection Internationale **Session 2007**
Ecole Normale Supérieure
Scientific Background Assessment - **Computer Science** Duration : 4 hours

First Exercise: Linear combinations

Denote by $\mathbb{Z}$ the set of integers. For any $(a, b) \in \mathbb{Z}^2$, denote by $L(a, b)$ the set $\{ax + by$ where $(x, y) \in \mathbb{Z}^2\}$ of all integral linear combinations of a and b.

Question-1. Show that there exists a unique integer $\pi(a, b) \geq 0$ such that $L(a, b)$ is the set of all multiples of $\pi(a, b)$, that is to say :

$$L(a, b) = \pi(a, b)\mathbb{Z}.$$

For any $(a, b) \in \mathbb{Z}^2$ such that $b \neq 0$, denote by $a \bmod b$ the remainder of a modulo b, that is the unique integer $r \in \mathbb{Z}$ such that $0 \leq r < |b|$ and b divides the integer $a - r$. Consider the following algorithm :

Algorithm 1 Computing $\pi(a, b)$

Input: Two non-negative integers a et b.
1: **if** $a \leq b$ **then**
2: swap a and b.
3: **end if**
4: **while** $b \neq 0$ **do**
5: $r \longleftarrow a \bmod b$.
6: $a \longleftarrow b$.
7: $b \longleftarrow r$.
8: **end while**
9: output a.

Question-2. Show that Algorithm 1 terminates within a finite number of steps.

Question-3. Show that Algorithm 1 outputs $\pi(a, b)$.

Question-4. Show that the number of loop iterations (steps 4 to 8) of Algorithm 1 is at most linear in n, where n is an upper bound on the number of bits of a and b : $0 \leq a, b < 2^n$.

Question-5. Modify Algorithm 1 so that it further outputs two integers x and y such that $ax + by = \pi(a, b)$.

Question-6. Deduce an algorithm which, given as input $(a, b, n, m) \in \mathbb{Z}^4$ such that $\pi(a, b) = 1$, outputs an integer α such that $\alpha - n$ is divisible by a, and $\alpha - m$ is divisible by b.

Second Exercise: Subset sums

The subset sum problem is the following : given an integer s of at most ℓ bits, and n integers $a_1, \ldots, a_n$ of at most ℓ bits, decide if there exists $(x_1, \ldots, x_n) \in \{0,1\}^n$ such that $s = \sum_{i=1}^{n} x_i a_i$, and if the answer is yes, output one such $(x_1, \ldots, x_n) \in \{0,1\}^n$.

We will assess the cost of algorithms in the usual way : the running time will be measured in elementary bit operations, and space will be measured in bits. We will assume that a list of m integers of at most ℓ bits can be sorted in time $O(m\ell \log m)$. To simplify analyses, we will denote by $\mathsf{poly}(n, \ell)$ any function of n and ℓ which is at most polynomial in n and ℓ, that is, there exist integers c_1, c_2 et c_3 such that the function is less than $c_1 \times n^{c_2} \ell^{c_3}$. For instance, multiplying n integers of ℓ bits costs $\mathsf{poly}(n, \ell)$.

Question-1. Show that the subset sum problem can be solved within time $2^n \mathsf{poly}(n, \ell)$.

Question-2. Assume that n is even. Show that the subset sum problem can be solved within time $2^{n/2} \mathsf{poly}(n, \ell)$ and space $2^{n/2} \mathsf{poly}(n, \ell)$.

Question-3. Assume that n is a multiple of four. Show that the subset sum problem can be solved within time $2^{n/2} \mathsf{poly}(n, \ell)$ and space $2^{n/4} \mathsf{poly}(n, \ell)$.