ÉNS de Lyon | Option C
M2 FEADéP | 2020–2021

Algorithmes élémentaires

Exercice 1 —Changement de base

Soient a et b deux entiers strictement supérieurs à 1.

1. Donner un algorithme qui prend en entrée un entier n et qui renvoie l'écriture de n en base a. Donner une majoration de sa complexité.

2. Donner un algorithme qui prend en entrée un entier n écrit en base a et qui renvoie l'écriture de n en base b, dans le cas où a est une puissance de b et dans le cas où b est une puissance de a. Donner une majoration de leurs complexités.

On admet dans les exercices 2 et 3 que le coût de l'algorithme d'Euclide étendu appliqué à deux entiers $1 \leq u, v \leq N$ est $O((\log N)^2)$.

Exercice 2 —Applications de l'algorithme d'Euclide étendu

Soient $u, v \geq 1$ des entiers premiers entre eux.

1. On se donne $a \in \mathbb{Z}/u\mathbb{Z}$ et $b \in \mathbb{Z}/v\mathbb{Z}$. Montrer qu'il existe un unique $x \in \mathbb{Z}/uv\mathbb{Z}$ tel que $x \equiv a \mod u$ et $x \equiv b \mod v$. Estimer le coût du calcul de x en fonction de la taille de u et v.
2. Montrer que toute fraction de la forme $\frac{n}{uv}$ s'écrit de manière unique $k + \frac{a}{u} + \frac{b}{v}$ avec $k \in \mathbb{Z}$, $0 \leq a < u$ et $0 \leq b < v$. Estimer le coût du calcul de k, a, b en fonction de la taille de n, u, v.

Exercice 3 —Coût de RSA

Soient p, q des nombres premiers distincts. Soit $n = pq$.

1. Déterminer $\varphi(n)$, où φ est l'indicatrice d'Euler.

Soit $e \in [\![1, \varphi(n)]\!]$ tel que $e \wedge \varphi(n) = 1$.

2. Soit $M \in [\![1, n]\!]$ tel que $M \wedge n = 1$. Soit $C = M^e$. Comment déterminer M à partir de C ?

3. Quel est le coût du calcul de M à partir de C ?