Travaux dirigés n° 11
Algorithmes calculatoires

Exercice 11.1 — Division entière

Voici un rappel de l'algorithme de *division entière* qui retourne le quotient et le reste de la division entière de deux grands entiers positifs dont le second est non nul. Cet algorithme utilise la multiplication ou division entières par 2 qui sont supposées s'effectuer en temps logarithmique.

Entrée : deux grands entiers naturels x et y de n bits chacun, y non nul
Sortie : deux grands entiers q et r tels que $x = y * q + r$ avec $r < y$

```
divisionEntière(grand entier x, grand entier y){// y non nul
1   si (x < y) {
2     retourner (0,x)
    }
3   q,r ← divisionEntière(DIV2(x),y)
4   q ← MULT2(q)
5   r ← MULT2(r)
6   si (ODD(x)){
7       r ← r + 1
    }
8   si (r ≥ y){
9     r ← r − y
10    q ← q + 1
    }
11  retourner (q,r)
}
```

1. Assurez-vous que vous avez bien compris cet algorithme en effectuant sa trace sur les valeurs $x = 123$ et $y = 21$.
2. Evaluez la complexité de cet algorithme quand on l'applique à de grands entiers.

Exercice 11.2 — Exponentielle modulaire

Cette opération est très utilisée pour chiffrer et déchiffrer des messages par exemple avec RSA.

Entrée : trois grands entiers naturels x, y et N de n bits chacun
Sortie : l'exponentielle modulaire $x^y \mod N$

1. Donnez un algorithme récursif efficace pour cette opération.
2. Evaluez sa complexité sachant que les 3 paramètres sont des grands entiers.

Exercice 11.3 — Calcul dichotomique du pgcd

Entrée : deux entiers naturels a et b de n bits chacun, avec $a \geq b \geq 0$
Sortie : le pgcd (plus grand commun diviseur) de a et b

1. Donnez un algorithme dichotomique récursif pour calculer le pgcd de 2 grands entiers.
2. Evaluez la complexité de votre algorithme et dites s'il est plus efficace ou pas que celui donné en cours.