TD 1 : Arithmétique entière

Exercice 1. *Calculs modulaires*

On utilise les algorithmes vus en cours pour calculer *modulo* un entier N. On note $\mathsf{A}(n)$ le coût d'une addition de deux entiers de n chiffres, $\mathsf{M}(n)$ le coût de la multiplication et $\mathsf{D}(n)$ celui de la division euclidienne d'un entier de $2n$ chiffres par un entier de n chiffres.

✎ Exprimer le coût d'une addition et le coût d'une multiplication, *modulo* N, à l'aide des fonctions $\mathsf{A}(\cdot)$, $\mathsf{M}(\cdot)$ et $\mathsf{D}(\cdot)$.

Exercice 2. *Division euclidienne naïve*

On rappelle l'algorithme de division euclidienne naïve, où $A = \sum_{i=0}^{n+m-1} a_i\beta^i$ et $B = \sum_{j=0}^{n-1} b_i\beta^i$ (et on pose $a_{n+m} = 0$).

Division(A, B):
  $Q \leftarrow 0$
  $R \leftarrow A$
  Pour $j = m$ **à** 0:
    $q_j \leftarrow \max\{q : q_j\beta^j B \leq R\}$
    $R \leftarrow R - \beta^j q_j B$
  Renvoyer $Q = \sum_j q_j\beta^j$ et R

1. **Correction de l'algorithme.** On note Q_j et R_j les valeurs de Q et R à la *sortie* de l'itération j de la boucle, avec $Q_{m+1} = 0$ et $R_{m+1} = A$. En particulier, $Q_j = \sum_{i\geq j} q_i\beta^i$.
   - **i.** Montrer que pour tout j, $A = BQ_j + R_j$.
   - **ii.** Montrer que pour tout j, $R_j < \beta^j B$.
   - **iii.** En déduire que l'algorithme est correct.
2. Proposer un algorithme rapide pour calculer q_j. Que devient la complexité de l'algorithme ?

Exercice 3. *Amélioration de l'algorithme de division euclidienne*

On souhaite supprimer toute dépendance en β dans la complexité.

1. Montrer que $q_j b_{n-1} \leq \lfloor R_{j+1}/\beta^{j+n-1}\rfloor < \beta^2$.

La question précédente montre qu'on peut calculer une borne sur q_j en posant

$$q_{\max} = \left\lfloor \frac{\lfloor R_{j+1}/\beta^{j+n-1}\rfloor}{b_{n-1}} \right\rfloor.$$

2. Quelle est la complexité du calcul de $q_{\max}$? Quelle opération de base est nécessaire ?
3. On suppose que $b_{n-1} \geq \beta/2$. Montrer que pour tout j, $q_j \geq q_{\max} - 2$.
4. En déduire un algorithme de complexité $O(mn)$ pour la division euclidienne, lorsque $b_{n-1} \geq \beta/2$.
5. Donner un algorithme de même complexité dans le cas général, en se ramenant au cas précédent.
6. Adapter l'algorithme au cas d'entiers en base 2^{64} où les chiffres sont des mots machine.