TD 1 : Arithmétique naïve

Exercice 1. *Correction de l'algorithme de multiplication naïve*

1. Écrire l'algorithme d'addition avec décalage, qui prend en entrée deux nombres M et N de m et n chiffres respectivement, ainsi qu'un décalage i, et renvoie l'entier $M + \beta^i N$ où β est la base. Estimer sa complexité.
2. Montrer que dans l'algorithme de multiplication par un chiffre, les chiffres du résultats sont tous strictement inférieurs à la base β.
3. En déduire la correction de l'algorithme de multiplication par un chiffre.
   Indication. Utiliser l'invariant $\overline{m_i \cdots m_0}^\beta \times n = \overline{r s_i \cdots s_0}^\beta$.
4. En supposant la correction de l'algorithme d'addition avec décalage, montrer la correction de l'algorithme de multiplication naïve.

Exercice 2. *Division euclidienne naïve*

1. **Correction de l'algorithme.** On note Q_j et R_j les valeurs de Q et R à la *sortie* de la $j^{\text{ème}}$ itération de la boucle, avec $Q_{m+1} = 0$ et $R_{m+1} = A$.
   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. L'étape de calcul de q_j est « $q_j \leftarrow \max\{q : q_j \beta^j B \leq R\}$ ». Proposer un algorithme sous-linéaire en β pour calculer ce maximum. Que devient la complexité globale de l'algorithme ?
3. **Amélioration.** On souhaite supprimer toute dépendance en β dans la complexité.
   i. 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

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

   ii. Quelle est la complexité du calcul de $q_{\max}$? Quelle opération de base sur les chiffres est nécessaire ?
   iii. On suppose que $b_{n-1} \geq \beta/2$. Montrer que pour tout j, $q_j \geq q_{\max} - 2$.
   iv. En déduire un algorithme de complexité $O(mn)$ pour la division euclidienne.
   v. Adapter l'algorithme au cas d'entiers en base 2^{64} où les chiffres sont des mots machine.

Exercice 3. *Calculs modulaires*

On utilise les algorithmes vus précédemment 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 $\mathsf{D}(\cdot)$.