

# D34: Méthodes de calcul efficaces

## TD n 1: arithmétique multiprécision

### 1 Exercices

#### Exercice 1. Utilisations des algorithmes multiprécision

1. Faire la somme et le produit des entiers suivants en base 16:  $a = 56FA2$  et  $b = 35CD1$ .
2. Appliquer, de façon détaillée, l'algorithme de Karatsuba pour calculer le produit des polynômes  $X^3 + 2X^2 - 3X + 1$  et  $4X^3 + X^2 - X - 1$ .
3. Appliquer, de façon détaillée, l'algorithme Toom-3 pour calculer le produit des polynômes  $X^2 + 3X + 2$  et  $2X^2 - 3X + 1$ .

#### Exercice 2. Algorithme de Karatsuba

On considère des polynômes de degré 2:  $A[X] = A_2X^2 + A_1X + A_0$  et  $B[X] = B_2X^2 + B_1X + B_0$ :

1. Calculer les coefficients  $C_0, \dots, C_4$  du produit  $C[X] = A[X]B[X]$ . Combien de multiplications sont nécessaires?
2. En utilisant une approche similaire à celle de Karatsuba, montrer qu'il est possible d'effectuer ce calcul en seulement 6 multiplications.
3. En déduire un algorithme de multiplication des polynômes de degré  $3^t - 1$ . Quelle est sa complexité?

#### Exercice 3. Variation autour de Karatsuba

On se propose d'étudier une variante de l'algorithme de Karatsuba dans le cadre des polynômes de degré  $3^t - 1$ .

1. Soit  $P$  le polynôme  $P[X] = a_2X^2 + a_1X + a_0$ . On considère le découpage suivant:  $P[X] = A_1X^2 + A_0$  ( $A_1$  est donc un polynôme de degré 1). Décrire une méthode de multiplication de polynômes, type Karatsuba, utilisant ce découpage.
2. Calculer, de manière détaillée, le produit de polynômes  $(X^2 + 3X + 1)(2X^2 - 4X + 3)$  en utilisant le découpage précédent et en appliquant récursivement la méthode précédente.
3. On considère maintenant des polynômes de degré  $3^t - 1$ . Écrire un algorithme de multiplication utilisant ce qui précède.
4. Montrer que la complexité de l'algorithme vérifie la formule de récurrence  $T(n) = 7T(\frac{n}{3})$ . En déduire la complexité de l'algorithme.

**Exercice 4.** Algorithme de Toom-Cook22

1. Décrire l'algorithme de Toom-Cook dans le cas  $k = 2$  (découpage en 2). En quels points peut-on évaluer les polynômes pour simplifier les calculs?
2. Donner les formules permettant de calculer les valeurs du polynôme produit en ces points.
3. En déduire la matrice d'interpolation TC2 permettant d'obtenir les coefficients du polynôme produit.
4. Quelle est la complexité de cette méthode?

## 2 Programmation

### Exercice 1. Seuils d'efficacité

Le but de cet exercice de réaliser une implantation de différents algorithmes de multiplications afin dans comparer les performances. L'étude devra notamment mettre en évidence les différents seuils d'efficacité des algorithmes. Pour cela, vous utiliserez le type `bignum` dont les fonctions élémentaires sont fournies dans le fichier `bignum.c`. Le fichier header correspondant contient les informations nécessaires pour manipuler les grands nombres.

1. Écrire le fichier `bn_arith.c` correspondant au fichier d'entete `bn_arith.h`. Le but est d'implanter l'algorithme de multiplication multi-précision des livres d'écoles. Pensez à utiliser la bibliothèque `gmp` pour vérifier la validité de votre implantation.
2. Implanter l'algorithme de Karatsuba puis . Effectuer une expérience numérique afin de mettre en évidence le seuil d'efficacité de chaque algorithme.