Implementation Project

Johan-Luca ROSSI, Baptiste CHEVALIER

December 2021

1 Structure du programme

Le code est découpé en six fichiers et est structuré de la façon suivante :

- arit.c contient les opérations de bases relatives à l'arithmétique modulaire.
- poly.c contient la définition du type polynôme et les opérations relatives à ces dernières pour des coefficients dans Z/NZ.
- karatsuba.c contient l'algorithme de karatsuba ainsi que des fonctions auxiliaires.
- toom.c contient l'implémentation de toom-cook (toom3) ainsi que des fonctions auxiliaires
- expe.c contient les fonctions relatives aux tests des performances des differents algorithmes
- main.c est le fichier permetant de lancer les tests.

Pour tester le code

- Compiler avec la commande make
- Exécuter le fichier "main" (**penser a mettre en paramètre un nombre premier pour définir le corps**)

2 Valeurs de seuil

Pour trouver la valeur de seuil T pour laquelle il est plus intéressant d'appeler un autre algorithme plutôt qu'un appel récursif, nous avons suivi le protocole expérimental suivant : Pour un polynôme de taille t_{poly} nous avons calculé le temps d'exécution de l'algorithme récursif (Toom-3 ou Karatsuba) pour différentes valeur de $T \in [1; t_{poly}]$, et cela répété pour plusieurs t_{poly}. Et enfin il suffit de trouvé pour quel T la valeur du temps d'exécution minimale de l'algorithme est atteinte (les courbes représentés ci-dessous ne représentes pas l'intervalle $[1; t_{poly}]$ en entier pour des raison de lisibilité mais le minima est bien atteint sur la partie de courbe affichée).

Karatsuba: Pour Karatsuba, c'est l'algorithme naif qui sera appelé pour des degrés inférieurs a T_k. Comme on l'observer sur les deux figures ci-dessous, le minima du temps d'exécution se trouve au alentour de 50, on posera donc $T_k = 50$.

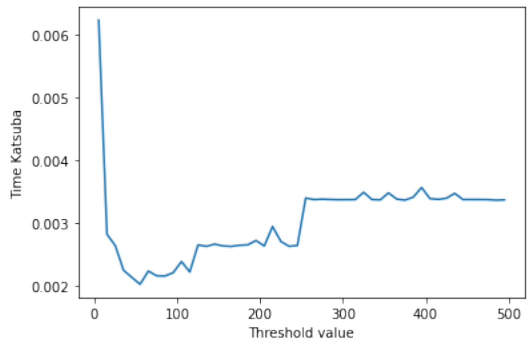

Figure 1: Temps d'exécution de Karatsuba en fonction de T pour un polynôme de taille 500

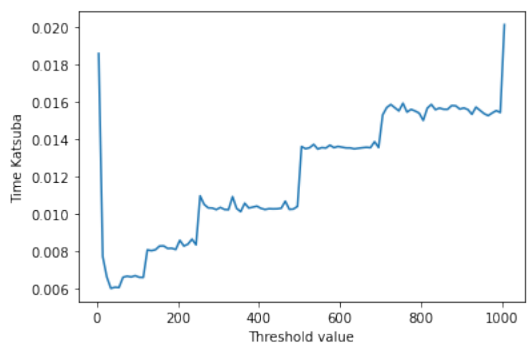

Figure 2: Temps d'exécution de Karatsuba en fonction de T pour un polynôme de taille 1000

Toom-Cook (Toom3): Pour Toom-3, c'est l'algorithme de karatsuba qui sera appelé pour des degrés inférieurs a T_{tc}. D'après l'analyse des temps exécutions (cf. Figure ci-dessous) les valeurs de temps d'exécution les plus faibles se trouvent au alentour de T=250, on posera donc $T_{tc} = 250$.

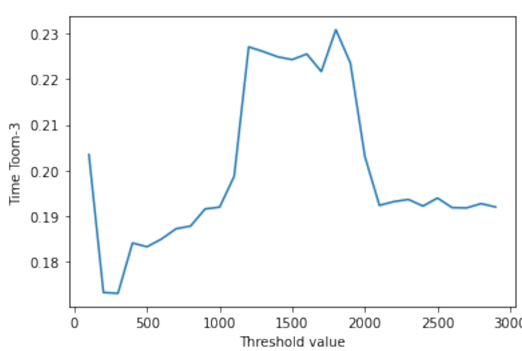

Figure 3: Temps d'exécution de Toom-3 en fonction de T pour un polynôme de taille 10000

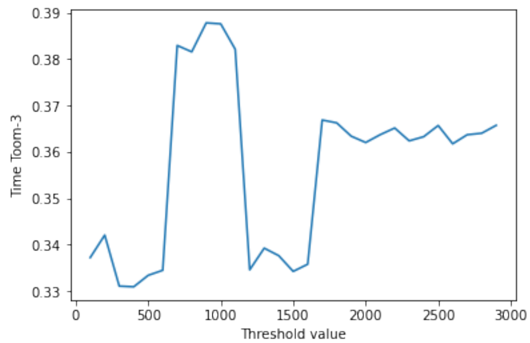

Figure 4: Temps d'exécution de Toom-3 en fonction de T pour un polynôme de taille 15000

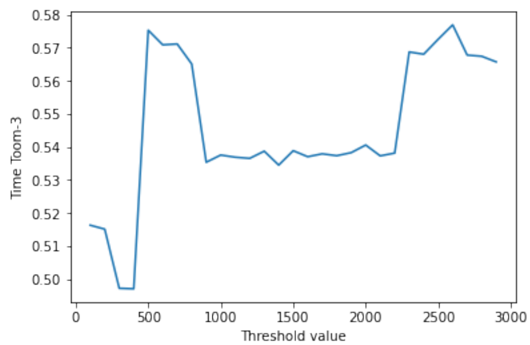

Figure 5: Temps d'exécution de Toom-3 en fonction de T pour un polynôme de taille 20000

3 Comparaison

Maintenant que les valeurs de seuil on été définies il est intéressant de comparer l'évolution des temps d'exécutions de nos algorithmes.

Karatsuba et algorithme naif:

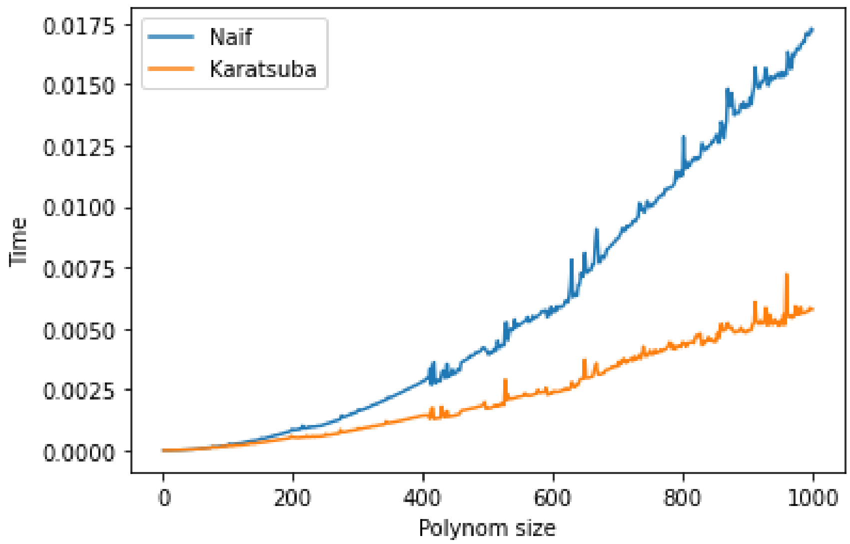

Figure 6: Temps d'exécution de Karatsuba et de l'algorithme naif en fonction de la taille des polynômes

La valeur de seuil étant pout $T_k = 50$ on observe bien que les courbe sont confondues avant cette valeur, les courbes se séparent ensuite, on observe un écart effectif au alentour de $t_{poly} = 200$.

Toom-3 et Karatsuba:

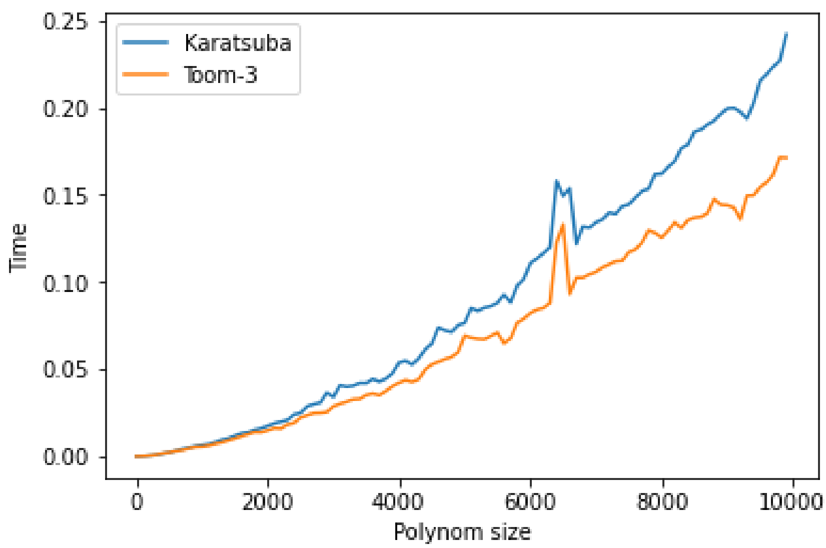

Figure 7: Temps d'exécution de Toom-3 et de Karatsuba en fonction de la taille des polynômes $t_{poly} \in [1, 10000]$

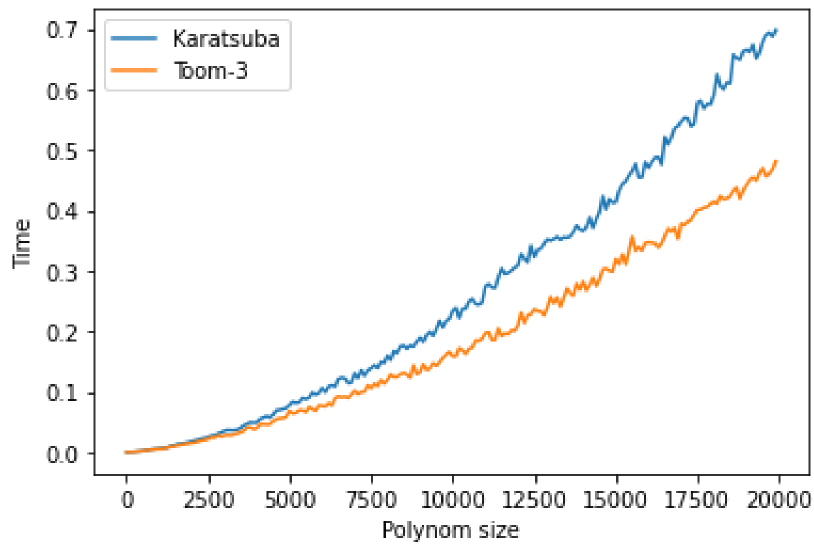

Figure 8: Temps d'exécution de Toom-3 et de Karatsuba en fonction de la taille des polynômes $t_{poly} \in [1, 20000]$

De la même manière pour Toom-3, les courbes sont confondue sous le seuil $T_{tc} = 250$, et on observe un écart conséquent qu'a partir de $t_{poly} = 2000$ (cf. Figure 7), l'écart s'intensifie avec la taille des polynome (cf. Figure 8), on observe donc concrètement l'intérêt de Toom-Cook pour les polynôme de haut degré.

4 Conclusion:

A travers ce projet nous avons pu mettre en évidence l'intérêt des méthodes "diviser pour régner", de l'interpolation pour la multiplication de polynôme et de définir le domaine d'utilisation des algorithmes présentés en fonction de la taille des polynômes. Un entier pouvant être représenté comme un polynôme en base 2, on peux définir l'entier m a partir duquel il est plus intéressant d'utiliser Karatsuba que l'algorithme naif, le degré de seuil étant à 50, on pose $n = 2^{50}$, de la même manière pour Toom-3 et Karatsuba, on pose $m = 2^{250}$.