Multiplication rapide d'entiers utilisant des nombres de Fermat généralisés premiers

Svyatoslav Covanov
Université de Lorraine, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506
Inria, Villers-lès-Nancy, F-54600
CNRS, LORIA, UMR 7503, Vandoeuvre-lès-Nancy, F-54506
svyatoslav.covanov@inria.fr

La multiplication d'entiers a et b de n bits est un problème d'algorithmique pour lequel la meilleure complexité connue a été obtenue à travers un effort de 50 ans, passant d'une complexité naïve en $O(n^2)$ à $O(n \log n \cdot 4^{\log^* n})$ [6]. Puisqu'on connaît des algorithmes pour accélerer le produit de polynômes, une première approche pour améliorer la complexité de l'algorithme naïf consiste à transformer a et b en des polynômes A et B tels que $a = A(2^k)$ et $b = B(2^k)$ pour un certain k divisant n.

Il se trouve qu'on peut accélerer le produit de 2 polynômes d'un certain degré N, en évaluant ces polynômes en N points bien choisis, et en multipliant point à point ces N évaluations. Cette observation aboutit à l'exploitation de racines primitives de l'unité comme $e^{\frac{i\pi k}{n}}$ dans $\mathbb{C}$ et de la transformée de Fourier, car on dispose d'un algorithme rapide pour évaluer un polynôme en des racines primitives de l'unité, appelé Fast Fourier Transform (FFT) et dont la forme la plus connue est celle de Cooley-Tukey [1].

Ainsi, en transformant les entiers a et b en des polynômes à coefficients dans $\mathbf{R} = \mathbb{Z}/(2^N + 1)\mathbb{Z}$, dans lequel 2 est une racine primitive $2N$-ème de l'unité, on obtient l'algorithme de Schönhage-Strassen [7], qui fut pendant près de 35 ans l'algorithme de multiplication d'entiers avec la meilleure la complexité connue, dont l'estimation est $O(n \cdot \log n \cdot \log\log n)$.

En 1989 [4], M. Fürer émet l'idée qu'en utilisant des nombres premiers de Fermat $F_m = 2^{2^m} + 1$, on bénéficie d'un anneau $\mathbf{R}$ dans lequel la multiplication par les racines 2^m-èmes primitives de l'unité sont des multiplications par des puissances de 2, ce qui s'effectue via un décalage de bits. Bien que peu probable, si on émet l'hypothèse qu'il existe une infinité de nombres premiers de Fermat, on aboutit à une complexité en $O(n \cdot \log n \cdot 2^{O(\log^* n)})$, $\log^* n$ étant le nombre de fois où il faut composer le logarithme avec n pour avoir un nombre plus petit que 1.

En 2007 [5], M. Fürer propose d'utiliser l'anneau $\mathbb{C}[X]/(X^P + 1)$, dans lequel X

a des propriétés similaires à 2 dans $\mathbb{Z}/(F_m)\mathbb{Z}$. Cet anneau permet d'aboutir à une complexité en $O(n \cdot \log n \cdot 2^{O(\log^* n)})$, sans dépendre d'une conjecture sur la répartition des nombres premiers de Fermat. Mais on peine à réaliser une implémentation efficace de cet algorithme, c'est-à-dire effectuer de meilleures performances que les implémentations actuelles de l'algorithme de Schönhage-Strassen.

Peu après, Harvey, Van Der Hoeven, and Lecerf publient un rapport [6] dans lequel ils proposent une analyse plus fine de l'algorithme de M. Fürer et obtiennent une estimation en $O(n \cdot \log n \cdot 16^{\log^* n})$ pour une version optimisée de l'algorithme original. Ils proposent par ailleurs d'autres algorithmes dont un en $O(n \cdot \log n \cdot 4^{\log^* n})$, reposant sur une conjecture sur la répartition des nombres premiers de Mersenne.

Cet exposé présentera les travaux réalisés dans [2], proposant un algorithme conjecturel alternatif à celui proposé par Harvey, Van Der Hoeven, and Lecerf, et bénéficiant d'une complexité en $O(n \cdot \log n \cdot 4^{\log^* n})$. On reprend l'idée de Fürer exploitant les nombres premiers de Fermat, mais en utilisant plutôt des nombres généralisés de Fermat, pour lesquels les travaux de Gallot et Dubner [3] permettent de conjecturer qu'on peut en trouver suffisamment pour effectuer une analyse de complexité satisfaisante. L'avantage principal de cet algorithme est sa simplicité en terme d'implémentation, que des travaux futurs vont chercher à mettre en œuvre.

Bibliographie

[1] J. W. Cooley and J. W. Tukey. An algorithm for the machine calculation of complex fourier series. *Math. Comput.*, 19:297–301, 1965.

[2] S. Covanov and E. Thomé. Fast arithmetic for faster integer multiplication. Jan. 2015.

[3] H. Dubner and Y. Gallot. Distribution of generalized fermat prime numbers. Technical report, Math. Comp, 1999.

[4] M. Fürer. On the complexity of integer multiplication (extended abstract). Technical Report CS-89-17, Pennsylvania State University, 1989.

[5] M. Fürer. Faster integer multiplication. In D. S. Johnson and U. Feige, editors, *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 57–66. ACM, 2007.

[6] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. *CoRR*, abs/1407.3360, 2014.

[7] A. Schönhage and V. Strassen. Schnelle Multiplikation großer Zahlen. *Computing*, 7(3-4):281–292, 1971.