(RÉ)APPRENDRE À M

AVEC LA MÉTHODE D

On a tous appris à multiplier ensemble deux nombres entiers. Une partie de la communauté mathématique a même cru, au XX^e siècle, que la méthode enseignée dans nos écoles était la meilleure méthode qui puisse exister pour ce faire. Et s'il en était autrement ?

Nadia Lafrenière
Université Dartmouth College

Si on vous demande de multiplier

45 758 780 × 96 803 528

sans calculatrice, comment feriez-vous ? Il y a fort à parier que vous écririez les nombres un au-dessus de l'autre, puis multiplieriez le nombre du haut par la dernière décimale du nombre du bas (les unités), un chiffre à la fois et à partir de la droite.

Multiplication

45 758 780
× 96 803 528
366 070 240
915 175 600
22 879 390 000
137 276 340 000
0
36 607 024 000 000
274 552 680 000 000
4 118 290 200 000 000
4 429 611 340 975 840

Après avoir obtenu le produit du nombre du haut par l'unité du bas, vous feriez des calculs similaires avec les dizaines du bas, avant de procéder avec les centaines, etc. Vous vous rendriez facilement compte que le processus est bien long…

Avec cette méthode, on doit multiplier chaque chiffre du premier nombre avec chaque chiffre du deuxième nombre. En cours de route, si on multiplie deux nombres de n chiffres ensemble, ça revient à faire n^2 multiplications élémentaires – c'est-à-dire des multiplications de nombres entiers entre 0 et 9.

Ainsi, si on veut multiplier deux nombres de 4 chiffres chacun, ça fait 16 multiplications élémentaires. Si on désire multiplier deux nombres de 8 chiffres chacun, on doit exécuter 64 multiplications élémentaires, ce qui est beaucoup !

Bien que l'on ait souhaité faire une seule multiplication, on finit par faire n^2 multiplications élémentaires, ainsi que quelques additions. On verra plus tard que les additions sont beaucoup plus faciles que les multiplications.

Peut-on faire mieux ?

Pourrait-on faire moins de multiplications élémentaires ? Pourrait-on même imaginer en faire significativement moins ?

Ce sont des questions que posa, en 1960, le mathématicien Andreï Kolmogorov à ses étudiants. Kolmogorov croyait profondément que c'était impossible, notamment parce qu'une façon aussi efficace de multiplier n'avait toujours pas été développée, même après des milliers d'années à multiplier. Il en était si persuadé qu'il organisa un séminaire afin de prouver sa conjecture. Après exactement une semaine, Anatoli Karatsuba, âgé de seulement 23 ans, décrivit un algorithme qui requiert beaucoup moins de multiplications élémentaires que l'algorithme qu'on a tous appris à l'école. C'était suffisant pour que Kolmogorov partage la bonne nouvelle et décide que le séminaire était terminé.

Alors, comment fait-on des multiplications plus efficacement ?

Le principe de l'algorithme de Karatsuba s'appelle « diviser pour régner ». Ça veut dire qu'on divise le problème initial (la multiplication de deux grands nombres), en plusieurs petits problèmes. Par exemple, au lieu de mul-

ULTIPLIER DE KARATSUBA

tiplier deux nombres à n chiffres ensemble, on pourrait faire quelques multiplications de nombres à $n/2$ chiffres. Pour obtenir un gain d'efficacité, il y a deux conditions :

- Le problème original est un processus relativement long. Mathématiquement, on dira que « sa complexité n'est pas linéaire ». C'est le cas de la multiplication, étant donné que faire deux multiplications de deux nombres de $n/2$ chiffres requiert moins de multiplications élémentaires que de faire une seule multiplication de nombres de n chiffres.
- Le nombre de petits problèmes doit être petit. Créer trop de petits problèmes pourrait même nous faire perdre de l'efficacité par rapport au problème original.

Dans le cas de la méthode de Karatsuba, on divise la multiplication de deux nombres de n chiffres en trois multiplications de $n/2$ chiffres. On doit aussi faire des additions et des soustractions pour recombiner les résultats, mais celles-ci nécessitent peu d'opérations en comparaison (voir encadré).

Par exemple, pour multiplier ensemble deux nombres de huit chiffres, on doit les séparer en nombres de quatre chiffres. Pour chaque nombre de huit chiffres, on crée deux nombres de quatre chiffres: celui de gauche et celui de droite. Ensuite, on multiplie ensemble les nombres de gauche et ceux de droite. Ainsi, au lieu de faire 45 758 780 × 96 803 528, on fait 4 575 x 9 680 et 8 780 x 3 528. On doit faire une multiplication supplémentaire pour combiner les deux. En multipliant ensemble des nombres de quatre chiffres, même trois fois, on sauve du temps. Là où le gain de temps est considérable, c'est qu'on applique aussi la même méthode pour faire les « plus petites » multiplications, c'est-à-dire celles avec moins de décimales.

Ceci permet un gain de temps considérable, comme expliqué plus bas.

Comment ça marche ?

Disons que l'on souhaite multiplier deux nombres, a et b, qui ont chacun un nombre pair de chiffres, par exemple $2k$ chiffres[1]. On peut réécrire les nombres a et b comme

$$a = a_1 \times 10^k + a_2 \text{ et } b = b_1 \times 10^k + b_2,$$

dans lesquels a_1, a_2, b_1 et b_2 sont des nombres à k chiffres. Utiliser la distributivité pour obtenir le produit $a \times b$ nous donne

$$(a_1 \times 10^k + a_2) \times (b_1 \times 10^k + b_2) = a_1 \times b_1 \times 10^{2k} + (a_1 \times b_2 + b_1 \times a_2) \times 10^k + a_2 \times b_2.$$

Même si les multiplications par des puissances de 10 sont en quelque sorte gratuites (on « ajoute des 0 »), on n'atteint pas le gain d'efficacité promis. Outre les multiplications par des puissances de 10, on fait quatre multiplications de nombre à k chiffres... comme dans la méthode initiale !

1. *L'algorithme peut facilement être adapté à la multiplication de deux nombres ayant un nombre impair de chiffres.*

Anatoli Karatsuba (1937-2008)

Anatoli Alekseïevitch Karatsuba est un mathématicien russe né le 31 janvier 1937 à Grozny et mort le 28 septembre 2008 à Moscou. Il est notamment connu pour son algorithme de multiplication, qui est la première méthode de multiplication rapide : l'algorithme de Karatsuba.

En 1966, il a soutenu sa thèse *The method of trigonometric sums and intermediate value theorem.*

En 1975, il a publié *Foundations of Analytic Number Theory* qui fut réédité en 1983.

Il a été directeur du département de théorie des nombres à l'Institut de mathématiques Steklov de l'Académie des sciences de Russie.

Il a notamment travaillé sur les séries de Fourier et le théorème de Moore.

L'addition, bien plus simple que la multiplication!

Puisqu'on apprend à additionner deux grands nombres ensemble deux ans avant d'apprendre à les multiplier, l'addition doit être bien plus simple que la multiplication, n'est-ce pas? Certes, le résultat de la somme de deux entiers positifs est généralement beaucoup plus petit que celui du produit. Mais la simplicité peut aussi s'exprimer par le nombre d'opérations à faire pour obtenir le résultat désiré.

Même pour un ordinateur, l'addition est plus simple. Qu'est-ce que ça veut dire ? Que beaucoup moins d'opérations sont nécessaires. En effet, lorsqu'on additionne deux nombres à n chiffres, le résultat a au plus $n + 1$ chiffres. Et pour y arriver, on ne fait qu'additionner les chiffres qui sont à la même position. Contrairement à la multiplication, le nombre d'opérations élémentaires correspond donc au nombre de chiffres de chacun des nombres. On dira alors que d'additionner deux nombres prend sensiblement le même temps que de lire ces nombres. On ne pourrait pas faire plus vite !

Exemple

Multiplier 2457 par 6819

1. Séparer les produits à effectuer

$$\begin{array}{r} 2457 \\ \times\ 6819 \end{array} \longrightarrow \begin{array}{r} 24\,|\,57 \\ 68\,|\,19 \end{array} \longrightarrow \begin{array}{r} 24 \\ \times\ 68 \end{array} \qquad \begin{array}{r} 57 \\ \times\ 19 \end{array}$$

2. Multiplier les chiffres significatifs*

$$\begin{array}{r} 24 \\ \times\ 68 \\ \hline 1632 \end{array}$$

3. Multiplier les chiffres les moins significatifs*

$$\begin{array}{r} 57 \\ \times\ 19 \\ \hline 1083 \end{array}$$

4. Étapes de reconstitution du produit

4a. Pour chaque nombre, additionner les deux parties

$$\begin{array}{r} 24\,|\,57 \\ 68\,|\,19 \end{array} \longrightarrow \begin{array}{l} 24 + 57 = 81 \\ 68 + 19 = 87 \end{array}$$

4b. Effectuer le produit des résultats de la partie 4a*

$$\begin{array}{r} 81 \\ \times\ 87 \\ \hline 7047 \end{array}$$

4c Soustraire les résultats des parties 2 et 3

$$\begin{array}{r} 7047 \\ -1632 \\ -\ 1083 \\ \hline 4332 \end{array}$$

5. Additionner les résultats des étapes 2, 3 et 4c pour obtenir le produit recherché

$$\begin{array}{r} 1632 \\ 4332 \\ 1083 \\ \hline 16754283 \end{array} \longrightarrow \begin{array}{r} 2\,457 \\ \times\ 6\,819 \\ \hline 16\,754\,283 \end{array}$$

* Les « petites multiplications » sont aussi effectuées avec la méthode de Karatsuba.

En fait, l'algorithme de Karatsuba utilise un truc supplémentaire : Il suffit de remarquer qu'on peut, au lieu de faire $(a_1 \times b_2 + b_1 \times a_2)$ dans l'exemple ci-dessus, écrire

$$(a_1 + a_2) \times (b_1 + b_2) - a_1 \times b_1 - a_2 \times b_2$$

Si cela semble encore plus compliqué qu'au départ, on réduit en fait le nombre de multiplications à faire, puisque

$$a_1 \times b_1 \text{ et } a_2 \times b_2$$

sont des expressions qu'on doit déjà calculer. Ainsi, le nombre de multiplications de nombres à k chiffres passe de quatre à trois. Certes, on doit faire des additions, mais celles-ci sont beaucoup moins coûteuses (voir encadré).

Pour multiplier deux nombres de $2k$ chiffres chacun, on devait faire $4k^2$ multiplications élémentaires avec la méthode apprise à l'école. Maintenant, on doit faire trois fois plus de multiplications élémentaires qu'il en faut pour multiplier des nombres à k chiffres. Si T est une fonction qui compte le nombre de multiplications élémentaires effectuées pour multiplier deux nombres à n chiffres[2], on a alors la récurrence

$$T(n) = 3T(n/2), \text{ quand } n > 1, \text{ et } T(1) = 1.$$

Celle-ci se résout par l'expression

$$T(n) = n^{\log_2(3)} \approx n^{1{,}58}.$$

2. *Après avoir additionné les nombres de n/2 chiffres, il est possible qu'une des multiplications se fasse avec des nombres de n/2 + 1 chiffres. Ceci n'a pas d'impact sur l'exposant de la solution à la récurrence, donc on se permet d'omettre ce détail.*

Une belle amélioration sur la méthode apprise à l'école, qui nous faisait faire n^2 multiplications élémentaires.

Pour avoir une idée du gain d'efficacité, on peut regarder le tableau ci-contre.

Y a-t-il plus efficace ?

Il y a une soixantaine d'années, la découverte de la méthode de Karatsuba a permis l'ouverture d'un tout nouveau champ de recherche. Depuis, d'autres méthodes encore plus efficaces ont été mises au jour. Certes, plusieurs d'entre elles sont difficiles à mémoriser, ce qui les rend peu réalistes pour un algorithme qui serait enseigné à l'école. En revanche, elles s'avèrent de formidables outils pour les ordinateurs qui doivent accomplir de nombreuses multiplications, ne serait-ce que pour crypter vos informations sensibles. Cela dit, si je vous demande de multiplier de grands nombres, peut-être gagneriez-vous à aller chercher la calculatrice !

Gain d'efficacité en utilisant la méthode de Karatsuba

n	n^2	$n^{1,58}$	Gain d'efficacité $n^2/n^{1,58}$
4	16	8,94	1,79
10	100	38,02	2,63
300*	90 000	8 200,71	10,97

* 300 correspond environ au nombre de chiffres des nombres utilisés dans les systèmes de cryptographie. La multiplication est au coeur de certains algorithmes de cryptographie.

La façon parfaite de multiplier ?

Avec la découverte de son algorithme, Karatsuba a créé un nouveau domaine de recherche. Il était désormais possible de se demander quelle est la meilleure méthode pour multiplier, puisque ce n'est pas celle apprise à l'école. En 1971, Arnold Schönhage et Volker Strassen ont développé un algorithme de multiplication beaucoup plus rapide que la méthode de Karatsuba en utilisant la transformée de Fourier rapide. Cette approche a permis de réduire le nombre de multiplications élémentaires nécessaires pour multiplier deux nombres de n chiffres à, asymptotiquement, $n\log(n)\log(\log(n))$, ce qui est très significatif pour des grandes valeurs de n. Ils ont alors émis la conjecture que la parfaite façon de multiplier devrait nécessiter, asymptotiquement, $n\log(n)$ multiplications élémentaires. La justification derrière cette hypothèse ? Le nombre d'opérations nécessaires pour exécuter une opération aussi fondamentale que la multiplication devait être simple à exprimer.

Bien que plusieurs améliorations importantes aient eu lieu à travers les époques, ce n'est qu'en 2019 que David Harvey et Joris van der Hoeven ont trouvé un algorithme de multiplication avec le nombre désiré d'opérations élémentaires, c'est-à-dire $n\log(n)$. Pourrait-on encore trouver une méthode significativement plus rapide ? Ce n'est pas impossible, puisque démontrer qu'on ne pourrait trouver de meilleures méthodes est extrêmement difficile. Toutefois, une grande partie de la communauté mathématique voit dans les travaux d'Harvey et van der Hoeven la méthode parfaite pour multiplier… en théorie !

En pratique, un ordinateur choisira la méthode de Karatsuba pour multiplier de petits nombres, l'algorithme de Toom et Cook pour multiplier des nombres de taille intermédiaire et l'algorithme de Schönhage et Strassen pour les grands nombres.

Développement d'algorithmes de multiplication, avec le nombre de multiplications élémentaires nécessaires