

Faire une multiplication ... plus vite qu'à l'école !(*)

Arno Eigenwillig et Kurt Mehlhorn(**)

Nous avons tous appris à l'école primaire à faire des multiplications, en suivant une méthode qui nous paraît familière et naturelle, mais est-elle vraiment rapide ?

1. La méthode scolaire

Pour multiplier entre eux deux nombres entiers a et b , nous multiplions a par chaque chiffre de b et nous écrivons ces produits intermédiaires en biais les uns au-dessous des autres. Ensuite, nous additionnons ces produits intermédiaires. Selon les pays, il existe quelques variantes dans la façon de poser les opérations, mais globalement, c'est ainsi que fonctionne la méthode scolaire de la multiplication.

Lorsque les nombres a et b sont grands, c'est-à-dire qu'ils comportent beaucoup de chiffres, alors cette méthode devient trop coûteuse en temps. Cela mérite réflexion :

1. Pourquoi juge-t-on cette méthode trop coûteuse en temps ?

2. Existe-t-il une autre méthode qui nous permettrait de gagner du temps ?

$$\begin{array}{r}
 5678 \\
 \times 4321 \\
 \hline
 5678 \\
 11356. \\
 17034.. \\
 22712... \\
 \hline
 24534638
 \end{array}$$

Ces questions sont intéressantes pour plusieurs raisons.

1. Du point de vue pratique : effectuer rapidement des calculs sur de grands nombres est utile dans beaucoup de domaines d'application de l'informatique, par exemple, pour manipuler l'information ou pour résoudre efficacement des problèmes géométriques et arithmétiques.

2. Du point de vue théorique : la méthode scolaire de la multiplication nous paraît si familière et naturelle que toute amélioration significative - et nous allons en découvrir une - constitue une véritable surprise.

Mais que veut-on dire par « la méthode scolaire est trop coûteuse en temps » ? Les informaticiens ne mesurent pas le temps de calcul en secondes (car l'année prochaine, de nouveaux ordinateurs plus rapides seront disponibles sur le marché), mais en nombre d'opérations de base qu'une méthode réalise. Nous pouvons ainsi comparer des algorithmes et pas les ordinateurs sous-jacents. Une opération de base est quelque chose qu'un ordinateur ou un homme peut faire en une seule étape. Les

(*) Cet article provient du site « interstices », site de culture scientifique créé par l'INRIA que l'on trouvera à l'adresse http://interstices.info/jcms/int_64256/

Une première version de ce document est parue en allemand dans la série publiée à l'occasion de l'Année de l'informatique (Informatikjahr) 2006.

Les auteurs remercient H. Alt, M. Dietzfelbinger et C. Klost pour leurs remarques utiles.

(2) Chercheur et enseignant-chercheur à l'Institut Max Planck de Sarrbrücken (Allemagne) ; arno@mpi-sb.mpg.de

opérations de base dont nous avons besoin ici sont des calculs qui font intervenir des nombres à un seul chiffre en base dix, les nombres étant donc écrits avec les chiffres 0, 1, 2, ..., 8, 9. Plus précisément, on considère :

1. Multiplication de deux nombres à un chiffre : si nous connaissons nos tables, nous pouvons pour deux nombres à un chiffre qu'on nous donne, déterminer en une seule étape les deux chiffres de leur produit. Nous appelons cette opération multiplication élémentaire.

2. Addition de trois nombres à un chiffre : pour trois nombres à un chiffre, nous pouvons trouver en une étape les deux chiffres de leur total (nous verrons juste après la raison pour laquelle nous voulons additionner ici trois nombres à un chiffre plutôt que deux).

En ne considérant que ces deux opérations de base, on va comparer des algorithmes de multiplication. Combien d'opérations de base la méthode scolaire de la multiplication nécessite-t-elle alors ? Avant de pouvoir répondre à cette question, nous devons d'abord évoquer l'addition de deux grands nombres, car nous en avons également besoin pour la multiplication.

L'addition de grands nombres

Combien d'opérations faut-il pour additionner deux nombres a et b ? Supposons que a et b comportent chacun n chiffres (si l'un des deux nombres est plus court, nous ajoutons simplement des zéros devant celui-ci, pour obtenir deux nombres de même longueur). Pour les additionner, nous les écrivons l'un au-dessous de l'autre et additionnons de droite à gauche les chiffres dans chaque colonne. À partir du résultat $10 \times u + v$, nous inscrivons le chiffre v comme chiffre du résultat dans la colonne considérée et nous ajoutons le chiffre u comme troisième chiffre (retenue) à la colonne suivante. Nous avons alors effectué au total n opérations de base, à savoir une addition de deux ou trois chiffres pour chaque colonne.

La multiplication d'un grand nombre par un nombre à un chiffre

Multiplions le nombre a à n chiffres par le nombre y à un chiffre. Nous multiplions chaque chiffre x de a par y . Nous écrivons le résultat $10 \times u + v$ sur une nouvelle ligne, de sorte que v se trouve dans la même colonne que x , et u à sa gauche. Ensuite, nous additionnons ces résultats intermédiaires à deux chiffres (nous écrivons habituellement directement le résultat sur une seule ligne en mémorisant les retenues). Cela fait au total $2n$ opérations de base : n additions et n multiplications.

Analyse de la méthode scolaire de la multiplication

Analysons à présent le nombre d'opérations de base que nécessite la méthode scolaire de la multiplication pour deux grands nombres a et b , qui comportent n chiffres. (Comme auparavant, si l'un des nombres est plus court, nous écrivons suffisamment de zéros.)

Pour chaque chiffre y de b , nous devons calculer un produit intermédiaire $a \times y$. C'est une « multiplication d'un grand nombre par un nombre à un chiffre », elle nécessite donc $2n$ opérations de base, comme on l'a expliqué ci-dessus. Comme b possède au

total n chiffres, nous devons effectuer $2n^2$ opérations de base, pour calculer tous les produits intermédiaires.

Ensuite, nous devons additionner les produits intermédiaires, placés en biais les uns au-dessous des autres. Pour nous simplifier le calcul, pensons à inscrire des zéros aux endroits vides ; nous obtenons alors n nombres de la même longueur, que nous devons tous additionner. À cette fin, nous utiliserons plusieurs fois la méthode décrite ci-dessus pour l'addition des grands nombres : nous additionnerons d'abord la première ligne avec la deuxième, puis ce sous-total avec la troisième ligne et ainsi de suite, jusqu'à ce que nous ayons finalement additionné tous les n produits intermédiaires. Nous aurons donc besoin de $n - 1$ additions de grands nombres.

Mais combien d'opérations de base cela fait-il ? Pour être en mesure de le dire, nous devons connaître la longueur de tous les sous-totaux qui apparaissent pendant cette série d'additions. Changeons de perspective : le résultat final de notre calcul, $a \times b$, peut au plus avoir $2n$ chiffres (si vous ne voyez pas pourquoi, réfléchissez-y !). Au fur et à mesure que nous additionnons les lignes les unes après les autres, les nombres deviennent toujours plus grands, ils ne redeviennent jamais plus petits. Par conséquent, tous les résultats intermédiaires ont une longueur au plus égale à $2n$ chiffres. Selon l'analyse ci-dessus relative à l'addition, cela signifie que chaque addition distincte de produits intermédiaires nécessite au plus $2n$ opérations de base. Pour nos $n - 1$ additions de ces nombres, nous avons donc besoin au plus de $(n - 1) \times (2n) = 2n^2 - 2n$ opérations de base.

En pratique, nous ne calculons pas ces additions intermédiaires, nous préférons additionner successivement tous les chiffres présents dans chaque colonne, en commençant par la colonne de droite, sans oublier de prendre en compte la retenue éventuelle. Mais cela revient au même pour le nombre global d'opérations élémentaires.

Conjointement avec les $2n^2$ opérations de base pour calculer les produits intermédiaires, cela fait donc au total au plus $4n^2 - 2n$ opérations de base, pour multiplier deux nombres de n chiffres avec la méthode scolaire ; dont n^2 sont des multiplications élémentaires. Le nombre d'additions est ici évidemment surestimé, car les premières additions sont plus petites, mais l'ordre de grandeur est respecté.

Qu'est-ce que cela signifie concrètement ? Si nous voulons effectuer des calculs sur des nombres vraiment longs, disons avec 100 000 chiffres, nous avons alors besoin de presque 40 milliards d'opérations de base pour une seule multiplication, dont 10 milliards de multiplications élémentaires. Nous avons besoin d'environ 200 000 opérations arithmétiques en moyenne pour chaque chiffre de sortie distinct d'un tel produit. C'est un rapport manifestement très défavorable, et il devient d'autant plus défavorable que les nombres deviennent plus longs : avec 1 million de chiffres, nous avons besoin de presque 4000 milliards d'opérations de base (dont mille milliards de multiplications élémentaires), cela fait en moyenne environ 2 millions d'opérations de base pour un seul chiffre du résultat.

Considérons maintenant que la multiplication est une opération plus coûteuse que l'addition, ce qui est souvent le cas en pratique, et essayons d'améliorer le coût en temps de la multiplication.

2. L'algorithme de Karatsuba

Examinons à présent une méthode qui permet de multiplier deux nombres de n chiffres avec sensiblement moins d'opérations de base. Elle porte le nom du mathématicien russe Anatolii Alexeevich Karatsuba, qui a eu l'idée centrale de cette méthode (publiée en 1962 avec Yuri Ofman). Nous décrirons cette méthode tout d'abord pour les nombres comportant un, deux ou quatre chiffres, ensuite pour les nombres de longueur n quelconque.



A. A. Karatsuba (photo Wikipédia)

Le cas le plus simple est la multiplication de deux nombres à un chiffre ($n = 1$) ; par exemple $8 \times 4 = 32$. Pour cela, on n'a besoin que d'une opération de base, à savoir une seule multiplication élémentaire qui fournit directement le résultat.

Le cas suivant que nous considérons est le cas $n = 2$, donc la multiplication de deux nombres a et b à deux chiffres : $a = 10 \times p + q$ et $b = 10 \times r + s$. Voici comment se présente le produit $a \times b$ exprimé à partir de la décomposition en chiffres de ses deux facteurs :

$$a \times b = (10 \times p + q) \times (10 \times r + s) = (p \times r) \times 100 + (p \times s + q \times r) \times 10 + q \times s.$$

Par exemple

$$78 \times 21 = (7 \times 2) \times 100 + (7 \times 1 + 8 \times 2) \times 10 + 8 \times 1 = 1400 + 230 + 8 = 1638.$$

Nous voyons directement qu'on peut calculer le produit des nombres a et b à deux chiffres en effectuant quatre multiplications de nombres à un chiffre et en additionnant les résultats (décalés les uns par rapport aux autres). C'est précisément ce que fait la méthode scolaire de la multiplication.

Nous devons à Karatsuba la découverte du fait que trois multiplications de nombres à un chiffre suffisent. Les valeurs à calculer sont les suivantes :

$$u = p \times r, v = (q - p) \times (s - r), w = q \times s.$$

En effet l'égalité suivante s'applique :

$$u + w - v = p \times r + q \times s - (q - p) \times (s - r) = p \times s + q \times r.$$

L'astuce de Karatsuba réside alors dans le fait qu'on peut exprimer le produit $a \times b$ à l'aide de cette identité, comme suit :

$$a \times b = u \times 10^2 + (u + w - v) \times 10 + w.$$

Contrairement à la méthode scolaire, le calcul de v fait intervenir des soustractions. Nous avons donc besoin de définir la soustraction de deux nombres à un chiffre comme autre opération de base similaire à l'addition, que nous devons appliquer ici deux fois. Techniquement, les résultats $(q - p)$ et $(s - r)$ n'ont certes qu'un chiffre, mais peut-être un signe négatif. Quand nous multiplions pour obtenir v , nous devons tout d'abord effectuer une multiplication élémentaire de ces deux valeurs et ensuite déterminer le signe.

Calculons le produit $a \times b$ pour notre exemple $a = 78$ et $b = 21$:

$$u = 7 \times 2 = 14, v = (8 - 7) \times (1 - 2) = -1, w = 8 \times 1 = 8.$$

Ainsi, nous trouvons :

$$78 \times 21 = 14 \times 100 + (14 + 8 - (-1)) \times 10 + 8 = 1400 + 230 + 8 = 1638.$$

Nous n'avons utilisé que trois multiplications élémentaires au lieu de quatre, auxquelles s'ajoutent plusieurs additions et soustractions pour le calcul des résultats intermédiaires.

La méthode de Karatsuba appliquée aux nombres à quatre chiffres

Après le cas $n = 2$, tournons-nous à présent vers le cas $n = 4$, c'est-à-dire la multiplication de deux nombres a et b à quatre chiffres. Exactement comme ci-dessus, nous pouvons les séparer chacun en deux moitiés p et q ou r et s ; mais ces moitiés de nombres ne sont à présent plus des nombres à un chiffre, mais des nombres à deux chiffres, de telle sorte que : $a = p \times 10^2 + q$ et $b = r \times 10^2 + s$.

À partir de ces quatre moitiés, nous calculons de nouveau les trois produits auxiliaires avec la méthode de Karatsuba, de la même façon que pour les nombres à deux chiffres :

$$u = p \times r, v = (q - p) \times (s - r), w = q \times s$$

et comme précédemment, nous obtenons le produit de a et b à partir de ces trois produits auxiliaires :

$$a \times b = u \times 10^4 + (u + w - v) \times 10^2 + w.$$

Exemple : Calculons $a \times b$ pour $a = 5678$ et $b = 4321$. Nous séparons d'abord a et b en moitiés $p = 56$ et $q = 78$ ainsi que $r = 43$ et $s = 21$. Ensuite, nous calculons les produits auxiliaires, à l'aide de la méthode de Karatsuba pour les nombres à deux chiffres :

$$u = 56 \times 43 = 2408, v = (78 - 56) \times (21 - 43) = -484, w = 78 \times 21 = 1638.$$

Il en résulte :

$$\begin{aligned} 5678 \times 4321 &= 2408 \times 10\,000 + (2408 + 1638 - (-484)) \times 100 + 1638 \\ &= 24\,080\,000 + 45\,3000 + 1638 = 24\,534\,638. \end{aligned}$$

Pour ce calcul, nous avons dû former trois produits auxiliaires de nombres à deux chiffres, et nous venons justement de voir dans la partie précédente la façon de les obtenir par la méthode de Karatsuba. Pour chaque produit auxiliaire, nous avons besoin de trois multiplications élémentaires. Pour multiplier deux nombres à quatre chiffres selon la méthode de Karatsuba, nous avons donc besoin au total de $3 \times 3 = 9$ multiplications élémentaires, ainsi que de plusieurs additions et soustractions. Avec la méthode scolaire, nous aurions eu besoin de 16 multiplications élémentaires et de plusieurs additions.

La méthode de Karatsuba pour n'importe quels grands nombres

En continuant selon le même principe, nous pouvons ramener la multiplication de nombres à 8 chiffres à trois multiplications de nombres à 4 chiffres, la multiplication de nombres à 16 chiffres à trois multiplications de nombres à 8 chiffres, et ainsi de suite. En d'autres termes, pour la méthode de Karatsuba expliquée ci-dessus, la longueur n des deux nombres a et b peut être une quelconque puissance de 2.

Nous pouvons écrire la méthode de Karatsuba sous une forme générale de la façon suivante. Nous décomposons deux nombres a et b de longueur $n = 2^k$ sous la forme :

$$a = p \times 10^{n/2} + q \text{ et } b = r \times 10^{n/2} + s$$

et calculons ensuite leur produit avec trois multiplications de nombres de longueur

$n/2 = 2^{k-1}$ du type

$$a \times b = p \times r \times 10^n + (p \times r + q \times s - (q - p) \times (s - r)) \times 10^{n/2} + q \times s.$$

Ainsi, le nombre de multiplications élémentaires nécessaires pour multiplier des nombres de longueur 2^k n'est que le triple de celui nécessaire pour multiplier des nombres de longueur 2^{k-1} (au lieu du quadruple avec la méthode scolaire). Il en résulte que la méthode de Karatsuba nécessite 3^k multiplications élémentaires, au lieu de 4^k par la méthode scolaire. Autrement dit, en notant \log le logarithme de base 2, $n^{\log(3)}$ au lieu de n^2 .

Considérons à présent la multiplication de deux nombres d'un million de chiffres. La méthode scolaire nécessite environ mille milliards de multiplications élémentaires. Pour pouvoir appliquer la méthode de Karatsuba, nous devons d'abord écrire une série de zéros devant un million de chiffres pour arriver à la puissance de 2 immédiatement supérieure, à savoir $2^{20} = 1\,048\,576$. Mais ensuite, nous n'avons besoin « que » d'environ trois milliards et demi de multiplications élémentaires, soit presque 300 fois moins : une seconde comparée à cinq minutes ...

Nous voyons donc que la méthode de Karatsuba est considérablement plus économique en temps de calcul ; du moins lorsque – comme nous le faisons – nous ne comptons que les multiplications élémentaires. Pour une analyse vraiment précise, nous devrions aussi considérer le temps engendré par l'addition et la soustraction des résultats intermédiaires. Nous préfererions alors peut-être calculer nos exemples concernant les nombres à deux et quatre chiffres selon la méthode scolaire. Mais dès que les nombres deviennent assez longs, c'est la méthode de Karatsuba qui gagne à tous les coups, parce qu'elle produit beaucoup moins de résultats intermédiaires que la méthode scolaire. La longueur exacte à partir de laquelle elle est plus rapide dépend des propriétés de l'ordinateur utilisé.

Résumons-nous pour conclure : quelle est la recette du succès de la méthode de Karatsuba ? Elle découle de deux idées cruciales.

La première idée est tout à fait générale. La tâche à accomplir « multiplier deux nombres de longueur n » est ramenée à plusieurs tâches du même type, mais de moindre dimension, à savoir : « multiplier deux nombres de longueur $n/2$ ». Ainsi, nous réduisons le problème jusqu'à ce qu'il soit devenu assez simple (« multiplier deux nombres à un chiffre »). On appelle ce principe *divide and conquer* (diviser pour régner), et nous l'avons déjà vu en action dans d'autres algorithmes (par exemple, pour un tri plus rapide). Pour les différentes dimensions du problème, nous ne programmons naturellement pas à chaque fois une nouvelle procédure, mais nous écrivons une procédure pour la longueur générale n , qui s'auto-appelle à différentes reprises pour la dimension réduite du problème $n/2$. Nous appelons cela une récursion, et c'est effectivement une des techniques les plus importantes en informatique.

La seconde idée, spécifique à la multiplication, est l'astuce de Karatsuba, grâce à laquelle nous n'avons besoin de résoudre que trois sous-problèmes au lieu de quatre lors de chaque étape intermédiaire. Cette différence en apparence minuscule fournit une énorme économie sur toute la récursion et constitue l'avantage décisif de la méthode de Karatsuba par rapport à la méthode scolaire.