

BROUILLON - DES OPÉRATIONS (PAS SI) SIMPLES

CHRISTOPHE BAL

*Document, avec son source L^AT_EX, disponible sur la page
<https://github.com/bc-writing/drafts>.*

Mentions « légales »

Ce document est mis à disposition selon les termes de la licence Creative Commons “Attribution – Pas d’utilisation commerciale – Partage dans les mêmes conditions 4.0 International”.



TABLE DES MATIÈRES

1.	Multiplication efficace avec Alexevich Karatsuba	2
1.1.	Une petite histoire dans la grande	2
1.2.	Multiplier efficacement deux grands nombres	2
1.3.	Un petit détour du côté du produit de deux entiers à deux chiffres	3

1. MULTIPLICATION EFFICACE AVEC ALEXEVICH KARATSUBA

1.1. Une petite histoire dans la grande. À l'automne 1960, lors d'un séminaire organisé par Kolmogorov, ce dernier parla de la conjecture suivante : « *Une multiplication de deux nombres de n chiffres ne peut être réalisée en moins de $\mathcal{O}(n^2)$ opérations élémentaires* ».

Karatsuba, qui avait assisté au séminaire, mit une semaine pour proposer une méthode en $\mathcal{O}(n^{\lg 3})$ opérations élémentaires¹, contredisant ainsi le grand Kolmogorov². Nous allons présenter cet algorithme en le redécouvrant de façon très « naturelle ».

1.2. Multiplier efficacement deux grands nombres. Comment calculer efficacement le produit $p = 12\,345\,678 \cdot 87\,654\,321$, c'est à dire en faisant le moins de multiplications possibles ?

La 1^{re} idée de la méthode de Karatsuba est de procéder comme suit.

- (1) $p = (1\,234 \cdot 10^4 + 5\,678)(8\,765 \cdot 10^4 + 4\,321)$
 $= 1\,234 \cdot 8\,765 \cdot 10^8 + (1\,234 \cdot 4\,321 + 5\,678 \cdot 8\,765) \cdot 10^4 + 5\,678 \cdot 4\,321$
- (2) On procède alors de façon analogue pour chaque nouveau produit (*nous allons voir que Karatsuba a été très malin pour gérer cette étape*). Concentrons-nous juste sur $q = 1\,234 \cdot 8\,765$ par exemple.
 $q = (12 \cdot 10^2 + 34)(87 \cdot 10^2 + 65)$
 $= 12 \cdot 87 \cdot 10^4 + (12 \cdot 65 + 34 \cdot 87) \cdot 10^2 + 34 \cdot 65$
- (3) Il reste alors des « dernières » étapes du type suivant en considérant $r = 12 \cdot 65$.
 $r = (1 \cdot 10 + 2)(6 \cdot 10 + 5)$
 $= 1 \cdot 2 \cdot 10^2 + (1 \cdot 6 + 2 \cdot 6) \cdot 10 + 2 \cdot 5$

Les habitués de l'algorithmique reconnaissent ici une approche de type « diviser pour mieux régner ». Pour simplifier nous allons considérer des nombres à $n = 2^k$ chiffres quitte à rajouter des zéros inutiles à gauche. La 1^{re} idée consiste donc à considérer $(a \cdot 10^{n/2} + b)(A \cdot 10^{n/2} + B)$ via $a \cdot A \cdot 10^n + (a \cdot B + A \cdot b) \cdot 10^{n/2} + b \cdot B$ où $(a; b; c; d) \in \llbracket 0; 10^{n/2} - 1 \rrbracket$.

Essayons de voir si l'on peut éviter de faire le calcul de tous les 4 produits $a \cdot A$, $a \cdot B$, $b \cdot B$ et $b \cdot A$. Pour cela nous allons prendre un peu de recul³ en considérant le polynôme $P(X) = (a \cdot X + b)(A \cdot X + B)$ et posons $P(X) = c_2 \cdot X^2 + c_1 \cdot X + c_0$. Projetons-nous alors un peu plus loin pour avancer...

- (1) $c_0 = P(0)$ c'est à dire $c_0 = b \cdot B$.
- (2) $c_2 = a \cdot A$ peut être vue comme la valeur à l'infini du polynôme P . Si l'on reste dans le cadre réel, on peut penser à un équivalent en $+\infty$. On peut en fait donner une définition très algébrique en considérant l'homogénéisé⁴ de P qui est par définition le polynôme $P_h(X; T) = c_2 \cdot X^2 + c_1 \cdot X \cdot T + c_0 \cdot T^2$. Dès lors, nous avons : $P_h(1; 0) = c_2$.
- (3) $P(1) = c_2 + c_1 + c_0 \iff c_1 = P(1) - c_2 - c_0$
 $\iff c_1 = (a + b)(A + B) - c_2 - c_0$

1. La fonction \lg désigne le logarithme binaire c'est à dire celui en base 2.

2. Il semblerait que Kolmogorov ait été très secoué par cette découverte, voire vexé. En effet, en 1962 Kolmogorov écrivit un article, sans doute avec Yuri Ofman l'un de ses élèves, sans en informer Karatsuba qui n'apprit l'existence de l'article que plus tard, lors de sa réédition.

3. L'auteur de ces notes ne sait pas ce qui a réellement guidé Karatsuba dans sa découverte.

4. Ce genre de considération est naturelle quand l'on fait de la géométrie projective. Le point $(1; 0)$ est un point à l'infini du plan projectif.

- (4) En résumé, $c_0 = b \cdot B$, $c_2 = a \cdot A$ et surtout $c_1 = (a + b)(A + B) - c_2 - c_0$. Donc il suffit de calculer les trois produits $c_0 = b \cdot B$, $c_2 = a \cdot A$ et $(a + b)(A + B)$, pour avoir au passage c_1 , puis d'utiliser $(a \cdot X + b)(A \cdot X + B) = c_2 \cdot 10^n + c_1 \cdot 10^{n/2} + c_0$. Joli ! Non ?

1.3. **Un petit détour du côté du produit de deux entiers à deux chiffres.** Avec $n = 2$, nous avons une façon originale de faire le produit de deux entiers à deux chiffres. Considérons par exemple le produit $56 \cdot 78$. Voici ce que donne la méthode de Karatsuba dans ce cas.

- (1) Ici $a = 5$, $b = 6$, $A = 7$ et $B = 8$.
- (2) $c_2 = 5 \cdot 7 = 35$.
- (3) $c_0 = 6 \cdot 8 = 48$.
- (4) $c_1 = (5 + 6)(7 + 8) - 35 - 48 = 165 - 35 - 48 = 82$.
- (5) $56 \cdot 78 = c_2 \cdot 10^2 + c_1 \cdot 10^1 + c_0 = 3500 + 820 + 48 = 4368$.

Visuellement nous avons fait les calculs suivants où c_0 et c_2 sont des multiplications « verticales » et c_1 s'obtient en soustrayant ces deux multiplications au produit des « additions horizontales ».

$$\begin{array}{r}
 \begin{array}{cc} 5 & + & 6 \\ \hline 7 & + & 8 \end{array} & \begin{array}{l} \text{orange} \downarrow \quad \text{green} \downarrow \\ \text{red} \rightarrow \end{array} & \begin{array}{l} 165 = 11 \cdot 15 \\ 83 = 35 + 48 \end{array} \\
 \hline
 \begin{array}{cccc} 3 & 5 & 4 & 8 \\ & 8 & 2 & \\ \hline 4 & 3 & 6 & 8 \end{array}
 \end{array}$$

Notons que le calcul directement via $a \cdot A \cdot 10^2 + (a \cdot B + A \cdot b) \cdot 10 + b \cdot B$ donne une méthode plus utile pour un calcul mental sans crayon ni papier car les calculs se font au fil de l'eau de la droite vers la gauche avec peu de calculs intermédiaires à retenir.

$$\begin{array}{r}
 \begin{array}{cc} 5 & 6 \\ \hline 7 & 8 \end{array} & \begin{array}{l} \text{orange} \downarrow \quad \text{purple} \downarrow \\ \text{green} \downarrow \quad \text{red} \downarrow \end{array} \\
 \hline
 \begin{array}{cc} 4 & 8 \\ \hline 4 & 0 \\ \hline 4 & 4 & 8 \\ \hline 4 & 2 \\ \hline 8 & 6 & 8 \\ \hline 3 & 5 \\ \hline 4 & 3 & 6 & 8 \end{array}
 \end{array}$$