# QUANT DE TEMPS CAL PER FER UNA MULTIPLICACIÓ ?

V. Strassen
Seminar für Angewandte Mathematik
Universitat de Zürich

Mentre que el sumar o restar dos nombres enters de n xifres requereix dur a terme un càlcul el temany del qual és proporcional a n, el mètode que correntment s'utilitza per a multiplicar demana fer més de $n^2$ operacions elementals (és a dir, sumes o multiplicacions d'una sola xifra). A primera vista podria semblar que tot mètode de multiplicar que pugui imaginar-se requereix càlculs de tamany proporcional, com a mínim, a $n^2$, degut a que cal multiplicar cada xifra d'un dels nombres amb cada xifra de l'altre. El raonament que veurem a continuació mostra que aquesta afirmació no és correcta.

Siguin a i b els nombres naturals de n xifres que volem multiplicar. Suposem que n sigui parell, posem $n = 2m$ i escrivim

$$a = a_1\ 10^m + a_o$$
$$b = b_1\ 10^m + b_o$$

on $a_1, a_o, b_1, b_o$ són nombres de n xifres. ($a_1$ consta de les xifres de l'esquerra de a i $a_o$ de les xifres de la dreta.) El producte que obtenim és:

(1) $$ab = a_1b_1 10^{2m} + (a_1b_o + a_ob_1)\ 10^m + a_ob_o$$

Podem calcular tot seguit els coeficients que aquí apareixen

$$a_1b_1\ ,\ a_ob_o\ ,\ a_1b_o + a_ob_1$$

i a partir d'ells, i amb l'ajuda de (1), obtenim el producte buscat. Ara bé: en lloc de realitzar el càlcul dels coeficients anteriors mitjançant 4 multiplicacions i una suma, podem aplicar per al darrer coeficient la identitat

(2) $$a_1b_o + a_ob_1 = a_1b_1 + a_ob_o - (a_1 - a_o)(b_1 - b_o)$$

D'aquesta manera ens estalviarem una multiplicació "difícil" a canvi de fer 3 sumes o restes "fàcils". Això ens proporciona un mètode que redueix una multiplicació de nombres de 2m xifres a 3 multiplicacions de nombres de m xifres junt amb algunes sumes i restes. Per a nombres de 8 xifres, per exemple, s'obté un lleuger estalvi respecte al mètode corrent. El que és, però, decisiu, és que el mètode anterior es pot iterar, és a dir les multiplicacions de nombres de m xifres que apareixen poden tornar a reduir-se de la mateixa manera (si m és també parell) i això pot fer-se un cop darrera l'altre, successivament. La reducció del temps de càlcul s'acumula de tal manera que per a la multiplicació de nombres de n xifres calen només càlculs de tamany proporcional a

$$n^{\log_2 3} = n^{1,5849...}$$

(si n és una potència de 2, cosa que, afegint zeros a a i b, pot aconseguir-se fàcilment).

El mètode que acabem de descriure va ésser descobert per primer cop pel matemàtic rus Kavatschuba al 1962. Posteriorment s'han desenvolupat algorismes de multiplicació encara molt més eficients, els més ràpids dels quals requereixen un temps proporcional a

$$n.\log n.\log\log n.$$

Tanmateix, haurem de prescindir de donar aquí una descripció d'aquest mètode (transformació de Fourier a anells de Fermat).

És clar que l'estalvi de temps dels nous mètodes respecte als clàssics és més considerable com més grans són els nombres que cal multiplicar. Hom calcula en menys de $10^{80}$ el nombre de protons de què consta l'univers; per tant, és poc probable que apareixin nombres de més de 80 xifres que representin dades concretes de la natura. Nogensmenys, el fet de calcular amb nombres com aquests no és pas cap raresa en camps com, per exemple, la teoria experimental de nombres o la criptologia. En aquests casos els nombres no tenen cap relació amb dades físiques, sinó que es tracta de portadors d'informació matemàtica o extramatemàtica.

*Considerem breument la multiplicació de nombres reals i complexos. La primera es redueix, amb precisió finita, a la multiplicació d'enters. La segona equival, en base a la definició*

$$(a_o+ia_1)(b_o-ib_1) = (a_ob_o+a_1b_1) + i\ (a_ob_1+a_1b_o)$$

*a 4 multiplicacions reals (si prescindim de les sumes i restes, que requereixen menys temps de càlcul). Sorprenentment, podem tornar a aplicar aquí la identitat (2) i estalviar-nos una multiplicació. No és difícil veure que ja no és possible cap nova millora.*

*Fem esment, finalment, de la multiplicació de matrius, que juga un paper central a l'àlgebra lineal i a les seves àrees d'aplicació i que, malgrat la seva aparent simplicitat, amaga un bon nombre de sorpreses algorísmiques. Igual que en el cas dels nombres enters, l'objectiu de les recerques actuals, trobar un algorisme optimal, junt amb la demostració de la seva optimalitat, es creu encara llunyà.*

*Bibliografia:*

*Aho-Kopcroft-Ullman: "The Design and Analysis of Computer Algorithmus", Addison-Wesley 1974.*

*Kunth: "The Art of Computer Programming" Volume 2, Addison-Wesley 1969/81.*