ABC, 28 de Octubre de 2019
CIENCIA - El ABCdario de las matemáticas
Alfonso Jesús Población Sáez

Hace unos meses dos investigadores dijeron haber encontrado un nuevo algoritmo para reducir el número de operaciones necesarias para manejar grandes números

Suele ser habitual que lo que aprendemos de pequeños nos parezca incuestionable, fuera de toda duda, algo así como una verdad universal. Y nos cuesta cambiar al ir creciendo, aunque con la adolescencia las cosas van cambiando, los profesores, los padres, los adultos, ya no nos parecen esos gurús protectores que nos parecieron siendo niños. Precisamente, **una de las bondades de las matemáticas**
, uno de sus pilares fundamentales,
es que nada debe darse por supuesto
, ni antes, ni después, lo diga quien lo diga. Nos debería enseñar a ser críticos. Lo malo es que para serlo hay que tener cierto dominio, hay que estar seguro de las cosas, y eso es lo que nos falla. Y además ser consciente de que no hay nada cerrado por completo, que es una materia en constante proceso de investigación, de renovación, por tanto, y de posibles cambios.

Cuando digo de todo, es de todo. Por ejemplo, ¿**Quién va a cuestionar** a estas alturas **la forma en que hacemos las multiplicaciones**
? Lo tenemos bien aprendido, sabemos que funciona, parece que no tiene ningún sentido cambiar a estas alturas. Para empezar, ni siquiera muchos seamos conscientes de que existen varios algoritmos, varios procedimientos para hacer multiplicaciones. Nos enseñaron uno, y ya está, no nos importa más. Quizá en algún momento, aparezca por nuestras vidas algún otro método (
las denominadas exóticamente multiplicaciones egipcias, hindúes, árabes
, etc.), pero lo consideramos sencillamente una curiosidad, algo propio de matemáticas recreativas, en suma, que no vamos a cambiar de procedimiento. Pero, ¿conocemos las limitaciones de nuestro «maravilloso» método?

Hace unos meses apareció en diferentes medios la noticia de «**matemáticos descubren la manera perfecta de multiplicar**
». El noventa por ciento de los lectores, a lo de siempre, a quedarse en el titular y a pensar «¿no tendrán otra cosa en que investigar?» o «pues vaya tonterías que hacen», y lindezas semejantes. No hay más que ver los comentarios que suelen aparecer a noticias similares. En fin, veamos a qué nos referimos con eso de las limitaciones del algoritmo.

Si tenemos que hacer una multiplicación, **no nos cuesta nada hacerla, siempre que no sean números de muchos dígitos** . Si pasan de tres en el

multiplicando, nos vamos a la calculadora o al ordenador (conste que no lo critico, que es lo razonable e inteligente). Pero, ¿qué pasa cuando tenemos que hacer multiplicaciones de números de muchas cifras? H

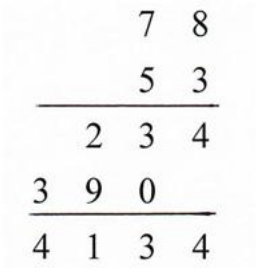
ablo de multiplicar números de miles de cifras

, por ejemplo. No me argumenten que eso no va a pasar nunca, porque se equivocan. Hay circunstancias en que hay que hacer productos de ese calibre. Les recuerdo que la invención de los

logaritmos

fue precisamente para eso, para efectuar operaciones con cifras muy grandes (sí, sirven para algo, y la raíz cuadrada también; si algo somos los matemáticos es que somos prácticos, no perdemos el tiempo en hacer entelequias que no tengan alguna utilidad, aunque a veces parezca lo contrario). Echemos unas cuentas (sencillas).

Para multiplicar un número de una cifra por otro similar, necesitamos hacer una única multiplicación. Si fueran dos números de dos cifras, ¿qué operaciones tenemos que hacer? Pongamos un ejemplo:



En la multiplicación de la imagen se realizan 4 productos (3 x 8, 3 x 7, 5 x 8 y 5 x 7: cada cifra del multiplicador, por cada cifra del multiplicando). Generalizando a números de

n

cifras, es claro por tanto que el número de multiplicaciones es proporcional a

n

^2. Respecto a las sumas (pensemos en términos del ordenador; por muy fáciles que sean, contemos todas), cuando hacemos (3 x 7) tenemos que hacer una suma porque del anterior producto (3 x 8) nos llevamos dos unidades. Por tanto, en la primera fila de la multiplicación hacemos una suma. Lo mismo en la segunda fila (la de 390), y finalmente tenemos otras tres sumas (el 3 + 0, 2 + 9 y 3 + la que nos llevamos de la suma anterior, aunque ésta en muchos casos no la tenemos). Luego en total en este ejemplo, hacemos 5 sumas, aunque pueden llegar a ser 6, si nos hubiéramos llevado alguna en la primera suma final (la del 3 + 0).

Seguramente conocemos otros algoritmos, más por curiosidad que por otra circunstancia (las llamadas multiplicaciones china, egipcia, india, etc.). También es típico ***el método de la caja***: descomponemos los números en potencias de 10 (70 + 8 y 50 + 3), multiplicamos todos por todos (como vemos en la tabla) y luego sumamos todos los productos que nos han dado: 3500 + 400 + 210 + 24 = 4134

	70	8
50	3500	400
3	210	24

Aunque parezca que hay menos sumas (en realidad son las mismas suponiendo que no contamos el sumar los ceros, porque estamos contando las sumas de digito a digito, no de números completos), seguimos teniendo 4 multiplicaciones (es decir del orden de *n*^2, siendo *n*
el número de dígitos de los números). El problema es cuando queremos multiplicar números de gran tamaño, por ejemplo, de
n
= 10^9 dígitos. Según lo anterior, habría que hacer un número de multiplicaciones proporcional a
n
^2, es decir, 10^18.
Y eso a un ordenador, por muy potente que sea, le lleva meses
(sí, no exagero; está comprobado). De modo que los matemáticos (y los informáticos, por supuesto, aunque en menor medida; su tarea es otra) han venido pensando otros algoritmos que faciliten a los ordenadores esos cálculos (o sea que precisen hacer menos operaciones). El prestigioso matemático
Andrei Kolmogorov
conjeturó que cualquier algoritmo que surja para multiplicar dos números de n cifras requerirá siempre un número de operaciones proporcional a
n
^2.

El algoritmo de Karatsuba

Sin embargo, en 1960, uno de sus alumnos, **Anatoly Karatsuba** encontró un algoritmo en el que sólo se empleaban *n*^(lo

g23) operaciones (aproximando el valor de ese logaritmo,
n
^1.58 operaciones)
. Bajar de exponente 2 a exponente 1.58 puede parecer poca cosa
, pero luego hacemos una tabla comparativa para que vean en realidad el «ahorro». El algoritmo se publicó finalmente en 1962. Al parecer, aquello sentó tan mal a su profesor, Kolmogorov, que convocó una reunión del grupo de investigación que dirigía, expuso el método de su brillante alumno Karatsuba, y se despidió sin volver a aparecer en más seminarios.

La idea del nuevo algoritmo parte de una **estrategia tipo «divide y vencerás»**: efectuamos la multiplicación de dos números
x
,
y
, a partir de otros más pequeños, con la mitad de dígitos. Para ello, elegimos una base de potencias
B
escribiendo
x e y
del siguiente modo:

$$x = x_1 B^m + x_0$$

$$y = y_1 B^m + y_0$$

donde *m < n, x0, y0 < B^m* *(0 es el subdíndice de x, y)*

Entonces:

$$xy = (x_1 B^m + x_0)\,(y_1 B^m + y_0) = x_1 y_1 B^{2m} + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0$$

Observemos que en la expresión anterior hay tres expresiones con multiplicaciones, las señaladas en color rojo. Además, la segunda de ellas puede escribirse así:

$$x_1y_0 + x_0y_1 = (x_1 + x_0)\,(y_1 + y_0) - x_1y_1 - x_0y_0$$

y en ella sólo hay una multiplicación, ya que los dos últimos valores que aparecen restando ya se han calculado (son los otros dos señalados en rojo en la igualdad previa). Es decir, **sólo hacemos tres multiplicaciones**
a costa de hacer más sumas y restas (estas operaciones para el ordenador no son tan costosas).

Para ilustrarlo echemos las cuentas sobre el ejemplo anterior (78 x 53). Elegimos como base B una con la que estamos familiarizados,
B
= 10. Entonces,

$$78 = 7 \cdot 10 + 8$$

$$53 = 5 \cdot 10 + 3$$

Repitiendo exactamente las mismas operaciones, tenemos que

$$78 \cdot 53 = (7 \cdot 10 + 8)\,(5 \cdot 10 + 3) = (7 \cdot 5)\,10^2 + [(7 + 8)\,(5 + 3) - 7 \cdot 5 - 8 \cdot 3]\,10 + 8 \cdot 3 = 35 \cdot 10^2 + [15 \cdot 8 - 35 - 24] \cdot 10 + 24 = 3500 + 610 + 24 = 4134$$

Como vemos, en lugar de cuatro multiplicaciones para hacer el producto, sólo hemos necesitado tres: 7x5, 15x8 y 8x3 (multiplicar por potencias de 10 no se considera porque no es más que añadir ceros y para eso no hace falta tiempo de memoria). Salen tres, como comprobamos de la expresión general del número de operaciones

$2^{(\log_2 3)} = 3$

Las sumas/restas son más que en el modo tradicional: 6. Está claro que para hacer a mano resulta más engorroso que el método tradicional, pero no así para el ordenador. La máquina sólo interpreta el algoritmo implementado y efectúa las operaciones a toda velocidad. Comparemos para valores de *n* grandes, el número de operaciones:

n	Tradicional n^2	Karatsuba $n^{(\log_2 3)}$
5	25	12.81861919
10	100	38.45585757
100	10^4	1478.852982
10^9	10^{18}	$1.83 \cdot 10^{14}$
10^{12}	10^{24}	$1.046 \cdot 10^{19}$

Está claro que el ahorro es considerable: frente a 10000 multiplicaciones, sólo 1479 con el método de Karatsuba, etc. Pero la cosa no termina aquí: para nosotros es más intuitivo trabajar con la base decimal (B = 10): el ordenador, que, dependiendo del modelo, puede ser a 32-bits o 64-bits, mejora su efectividad en base B = 2.

Un último apunte del método. Si lo desarrollamos para números con 3, 4, … dígitos, hay entremedias otros productos de cifras con menos dígitos, pero más de uno (que es el expuesto arriba). En estos casos intermedios, el ordenador emplea a su vez el algoritmo de forma anidada para efectuar esos productos.

Otros algoritmos

Unos años después, en 1966, los matemáticos Andrei Toom y Stephen Cook generalizaron el método de Karatsuba estableciendo un nuevo algoritmo, conocido (¡cómo no!) como ***algoritmo Toom-Cook***
. Con él, el número de operaciones es proporcional a

n
log n
e
^(sqrt(log2(
n
)), cantidad menor que las anteriores (más abajo describo algunos valores para n para que se aprecie la mejora). En 1971, dos matemáticos alemanes, Arnold Schönhage y Volker Strassen desarrollaron otro procedimiento, conocido como
algoritmo Schönhage–Strassen
, basado en la
transformada rápida de Fourier
, para el que el número de operaciones es del orden de n log
n
log(log(
n
)). Y conjeturaron (no aprendieron de lo que le pasó a Kolmogorov), sin prueba alguna, que seguramente existen otros algoritmos que mejoren el suyo, es decir, que para números enormes requieran menos operaciones.

Hace unos meses, en abril de 2019, David Harvey, de la Universidad de Nueva Galés del Sur (UNSW), en Sidney (Australia), y Joris van der Hoeven, de la École Polytechnique de Francia, han comunicado que han encontrado un nuevo **algoritmo que al parecer mejora aún más el número de operaciones** , aunque de momento hay que ser cautos ya que su trabajo aún no se ha revisado convenientemente por fuentes externas (la famosa «revisión por pares»). Su estimación del número de operaciones aún no se ha acabado de determinar ya que sólo poseen datos con ejemplos concretos. Respecto a los métodos anteriores:

n	Karatsuba n^($\log_2 3$)	Toom-Cook $n \log n$ e^(sqrt($\log_2(n)$))	Schönhage–Strassen $n \log n \log(\log(n))$
5	12.8186	36.9331	3.8295
10	38.4558	142.4845	19.2043
100	1478.8529	6062.743	703.2922
10^9	1.83·10^14	4.91·10^12	6.28·10^10
10^12	1.046·10^19	1.52·10^16	9.17·10^13

Obsérvese que el algoritmo de Toom-Cook es peor respecto al número de operaciones para valores pequeños de n, mientras que el de Schönhage–Strassen es mejor en cualquier caso que ningún otro método conocido, hasta ver qué sucede con el propuesto por Harvey-van der Hoeven. En los ejemplos que han testado, parece ser que han logrado que los ordenadores efectúen multiplicaciones de números del orden de 10^9 en tan sólo 30 segundos.

Todo esto, más allá de disminuir el tiempo de las máquinas para multiplicaciones de números grandes, se contempla dentro de un campo llamado ***teoría de la complejidad computacional*** , que tiene otras implicaciones y aplicaciones en otros asuntos.

Moraleja

Como las antiguas fabulas, podemos extraer algunas conclusiones del trabajo de los matemáticos. La primera es que, **en matemáticas, en ciencia en general, nunca nada está completamente cerrado** , por elemental que sea o parezca (no hay nada más elemental que multiplicar dos números), todo es susceptible de ser mejorado. La segunda, que aquí no caben prepotencias ni soberbias: cualquiera puede descubrir algo que el más docto catedrático ni siquiera soñó (un dicho castellano lo define muy bien: donde menos se espera, salta la liebre).
La lógica y la razón se imponen a cualquier otro argumento . Más de uno debiera aplicarse el ejemplo. ¿No me digan que las matemáticas no son maravillosas, que además de resolver problemas, estimar situaciones, calcular todo tipo de obras de ingeniería, analizar conflictos, etc., nos dan lecciones de humildad?

Para acabar

Una última recomendación sobre la multiplicación. Si desean conocer más detalles de cómo hemos llegado al método convencional, conocer otros procedimientos utilizados a través de la Historia y las civilizaciones, y un montón de curiosidades, todo ello descrito de un modo sencillo y ameno, acaba de publicarse un libro, « Los secretos de la multiplicación » (ver imagen), de uno de nuestros colaboradores en esta sección y muy implicado en la divulgación de las matemáticas en la sociedad, Raúl Ibáñez.

Y respecto al ejercicio de las sillas que propuse hace unas semanas, el quiz de la cuestión era utilizar el mínimo común múltiplo (que también nos enseñaron en el colegio). Si la cantidad de sillas fuera múltiplo de 2, 3, 4, 5, 6, 8, 9 y 10, entonces sería de la forma 360 n, porque el $mcm(2, 3, 4, 5, 6, 8, 9, 10) = 360$. Pero nos dicen que siempre sobra una silla. Vale, pues es de la forma $360n + 1$. Miramos entonces aquel número de esa forma menor que mil (nos lo dice el enunciado) que para algún valor de n, sea múltiplo de 7. Sólo hay dos, 361 y 721, y éste segundo es el que es múltiplo de 7. **Como ven, no hace falta ni calculadora, ni ordenador, sólo pensar un poquillo**. Que ustedes lo pasen bien .

Alfonso J. Población Sáez es profesor de la Universidad de Valladolid y miembro de la Comisión de divulgación de la RSME.

El ABCDARIO DE LAS MATEMÁTICAS es una sección que surge de la colaboración con la Comisión de Divulgación de la Real Sociedad Matemática Española (RSME)