Mathematicians Discover the Perfect Way to Multiply

Kevin Hartnett

Four thousand years ago, the Babylonians invented multiplication. Last month, mathematicians perfected it.

On March 18, two researchers described the fastest method ever discovered for multiplying two very large numbers (Harvey and van der Hoeven 2019). The paper marks the culmination of a long-running search to find the most efficient procedure for performing one of the most basic operations in math.

"Everybody thinks basically that the method you learn in school is the best one, but in fact it's an active area of research," said Joris van der Hoeven, a mathematician at the French National Center for Scientific Research and one of the coauthors.

The complexity of many computational problems, from calculating new digits of pi to finding large prime numbers, boils down to the speed of multiplication. Van der Hoeven describes their result as setting a kind of mathematical speed limit for how fast many other kinds of problems can be solved.

"In physics you have important constants like the speed of light which allow you to describe all kinds of phenomena," van der Hoeven said. "If you want to know how fast computers can solve certain mathematical problems, then integer multiplication pops up as some kind of basic building brick with respect to which you can express those kinds of speeds."

Most everyone learns to multiply the same way. We stack two numbers, multiply every digit in the bottom number by every digit in the top number and do addition at the end. If you're multiplying two two-digit numbers, you end up performing four smaller multiplications to produce a final product.

The grade school or "carrying" method requires about n^2 steps, where n is the number of digits of each of the numbers you're multiplying. So three-digit numbers require nine multiplications, while 100-digit numbers require 10,000 multiplications.

The carrying method works well for numbers with just a few digits, but it bogs down when we're multiplying numbers with millions or billions of digits (which is what computers do to accurately calculate pi or as part of the worldwide search for large primes).[1] To multiply two numbers with one billion digits requires one billion squared, or 10^{18}, multiplications, which would take a modern computer roughly 30 years.

For millennia it was widely assumed that there was no faster way to multiply. Then, in 1960, the 23-year-old Russian mathematician Anatoly Karatsuba took a seminar led by Andrey Kolmogorov, one of the great mathematicians of the 20th century. Kolmogorov asserted that there was no general procedure for doing multiplication that required fewer than n^2 steps. Karatsuba thought there was—and after a week of searching, he found it.

Karatsuba's method involves breaking up the digits of a number and recombining them in a novel way that allows you to substitute a small number of additions and subtractions for a large number of multiplications. The method saves time because addition takes only $2n$ steps, as opposed to n^2 steps.

"With addition, you do it a year earlier in school because it's much easier, you can do it in linear time, almost as fast as reading the numbers from right to left," said Martin Fürer, a mathematician at Pennsylvania State University who in 2007 created what was at the time the fastest multiplication algorithm.

When dealing with large numbers, you can repeat the Karatsuba procedure, splitting the original number into almost as many parts as it has digits. And with each splitting, you replace multiplications that require many steps to compute with additions and subtractions that require far fewer.

"You can turn some of the multiplications into additions, and the idea is additions will be faster for computers," said David Harvey, a mathematician at the University of New South Wales and a coauthor on the new paper.

Karatsuba's method made it possible to multiply numbers using only $n^{1.58}$ single-digit multiplications. Then, in 1971, Arnold Schönhage and Volker Strassen published a method capable of multiplying large numbers in $n \times \log n \times \log(\log n)$ multiplicative steps, where log n is the logarithm of n. For two

How to Multiply Big Numbers Fast

For millennia, it took about n^2 steps of single-digit multiplications to multiply two n-digit numbers. Then in 1960, the Russian mathematician Anatoly Karatsuba proposed a better way.

Traditional Way to Multiply 25 × 63

Requires **four** single-digit multiplications and some additions.

STEP A	B	C	D		E
25 × 63 = 1200	25 × 63 = 15	25 × 63 = 60	25 × 63 = 300	=	1575

Karatsuba Method for 25 × 63

Requires **three** single-digit multiplications plus some additions and subtractions.

STEP A	B	C	D	E	F	G
Break numbers up.	Multiply the tens.	Multiply the ones.	Add the digits.	Multiply the sums.	Subtract B and C from E.	Assemble the numbers.
25 → 2 5 63 → 6 3	2 × 6 = 12	5 × 3 = 15	2 + 5 = 7 6 + 3 = 9	7 × 9 = 63	63 − 15 − 12 = 36	1200 + 360 + 15 = 1575

MULTIPLIED SAVINGS: As numbers increase in size, the Karatsuba method can be used repeatedly, breaking large numbers into small pieces to save an increasing number of single-digit multiplications.

Traditional way to multiply 2,531 × 1,467 requires **16** single-digit multiplications.

2531 × 1467 + 2531 × 1467 + 2537 × 1467 + 2531 × 1467 = 3712977

Karatsuba method to multiply 2,531 × 1,467 requires **9** single-digit multiplications.

STEP A	B	C	D	E	F	G
25 31 14 67	25 × 14 = 350	31 × 67 = 2077	25 + 31 = 56 14 + 67 = 81	56 × 81 = 4536	4536 − 2077 − 350 = 2109	350 + 2109 + 2077 = 3712977

	A	B	C	D	E	F	G
Run Karatsuba method on:	2 5 1 4	3 1 6 7	5 6 8 1				

Lucy Reading-Ikkanda/Quanta Magazine

one-billion-digit numbers, Karatsuba's method would require about 165 trillion additional steps.

Schönhage and Strassen's method, which is how computers multiply huge numbers, had two other important long-term consequences. First, it introduced the use of a technique from the field of signal processing called a fast Fourier transform. The technique has been the basis for every fast multiplication algorithm since.

Second, in that same paper, Schönhage and Strassen conjectured that there should be an even faster algorithm than the one they found—a method that needs only $n \times \log n$ single-digit operations—and that such an algorithm would be the fastest possible. Their conjecture was based on a hunch that an operation as fundamental as multiplication must have a limit more elegant than $n \times \log n \times \log(\log n)$.

"It was kind of a general consensus that multiplication is such an important basic operation that, just from an aesthetic point of view, such an important operation requires a nice complexity bound," Fürer said. "From general experience the mathematics of basic things at the end always turns out to be elegant."

Schönhage and Strassen's ungainly $n \times \log n \times \log(\log n)$ method held on for 36 years. In 2007, Fürer beat it, and the floodgates opened. Over the past decade, mathematicians have found successively faster multiplication algorithms, each of which has inched closer to $n \times \log n$, without quite reaching it. Then, last month, Harvey and van der Hoeven got there.

Their method is a refinement of the major work that came before them. It splits up digits, uses an improved version of the fast Fourier transform and takes advantage of other advances made over the past 40 years. "We use [the fast Fourier transform] in a much more violent way, use it several times instead of a single time, and replace even more multiplications with additions and subtractions," van der Hoeven said.

Harvey and van der Hoeven's algorithm proves that multiplication can be done in $n \times \log n$ steps. However, it doesn't prove that there's no faster way to do it. Establishing that this is the best possible approach is much more difficult. At the end of February, a team of computer scientists at Aarhus University posted a paper arguing that if another unproven conjecture is also true, this is indeed the fastest way multiplication can be done (Afshani et al 2019).

And while the new algorithm is important theoretically, in practice it won't change much, since it's only marginally better than the algorithms already being used. "The best we can hope for is we're three times faster," van der Hoeven said. "It won't be spectacular."

In addition, the design of computer hardware has changed. Two decades ago, computers performed addition much faster than multiplication. The speed gap between multiplication and addition has narrowed considerably over the past 20 years to the point where multiplication can be even faster than addition in some chip architectures. With some hardware, "you could actually do addition faster by telling the computer to do a multiplication problem, which is just insane," Harvey said.

Hardware changes with the times, but best-in-class algorithms are eternal. Regardless of what computers look like in the future, Harvey and van der Hoeven's algorithm will still be the most efficient way to multiply.

Note

1. See www.mersenne.org (accessed August 19, 2019).

References

Afshani, P, C Freksen, L Kamma and K G Larsen. 2019. "Lower Bounds for Multiplication via Network Coding." arXiv: 1902.10935 [cs.DS], February 28. https://arxiv.org/abs/1902.10935 (accessed August 19, 2019).

Harvey, D, and J van der Hoeven. 2019. "Integer Multiplication in Time $O(n \log n)$." HAL hal-02070778, March 18. https://hal.archives-ouvertes.fr/hal-02070778/document (accessed August 19, 2019).

Schönhage, A, and V Strassen. 1971. "Schnelle Multiplikation großer Zahlen" [Fast multiplication of large numbers]. *Computing* 7, no 3–4 (September): 281–92.

Kevin Hartnett is a senior writer at Quanta Magazine *covering mathematics and computer science. His work has been included in Princeton University Press's Best Writing on Mathematics series in 2013, 2016 and 2017. From 2013 to 2016 he wrote Brainiac, a weekly column for the* Boston Globe*'s Ideas section.*

Reprinted with permission from QuantaMagazine .org, an editorially independent publication of the Simons Foundation, whose mission is to enhance public understanding of science by covering research developments and trends in mathematics and the physical and life sciences, April 11, 2019, www.quantamagazine.org/mathematicians-discover-the-perfect-way-to-multiply-20190411/. Minor changes have been made to fit ATA style.