What we still don't know about addition and multiplication

Carl Pomerance, **Dartmouth College**
Hanover, New Hampshire, USA

You would think that all of the issues surrounding addition and multiplication were sewed up in third grade!

Well in this talk we'll learn about some things they didn't tell you . . .

Here's one thing they *did* tell you:

Find 483×784.

$$
\begin{array}{r}
483 \\
\times\ 784 \\
\hline
1932 \\
3864 \\
3381 \\
\hline
378672
\end{array}
$$

If instead you had a problem with two 23-digit numbers, well you always knew deep down that math teachers are cruel and sadistic. Just kidding! (*Aside: evil laugh* . . .)

In principle if you really have to, you could work out 23-digits times 23-digits on paper, provided the paper is big enough, but it's a lot of work.

So here's the real question: How much work?

Of course the amount of work depends not only on how long the numbers are, but on what they are. For example, multiplying 10^{22} by 10^{22}, that's 23-digits times 23-digits, but you can do it in your head.

In general, you'll take each digit of the lower number, and multiply it painstakingly into the top number. It's less work if some digit in the lower number is repeated, and there are definitely repeats, since there are only 10 possible digits. But even if it's no work at all, you still have to write it down, and that's 23 or 24 digits. At the minimum (assuming no zeroes), you have to write down $23^2 = 529$ digits for the "parallelogram" part of the product. And then comes the final addition, where all of those 529 digits need to be processed.

So in general if you multiply two n-digit numbers, it would seem that you'd be taking n^2 steps, unless there were a lot of zeroes. This ignores extra steps, like carrying and so on, but that at worst changes n^2 to maybe $2n^2$ or $3n^2$. We say that the "complexity" of "school multiplication" for two n-digit numbers is of order n^2.

Here is what we don't know:
What is the *fastest* way to multiply?

There's a method known as the *Fast Fourier Transform* that allows you to multiply in about $n \log n$ steps. But we don't know if this is the best possible.

The function "$\log n$" can be thought of as natural log, or common log, or base-2 log, they are all within a constant factor of each other. The takeaway is that $\log n$ grows to infinity as n does, but eventually much more slowly than any root of n. For example, using the natural log, we have

$$\begin{aligned}
\log n &< n^{1/2} \quad \text{for} \quad n \geq 1 \\
\log n &< n^{1/4} \quad \text{for} \quad n \geq 5504 \\
\log n &< n^{1/10} \quad \text{for} \quad n \geq 3.431 \times 10^{15} \\
\log n &< n^{1/100} \quad \text{for} \quad n \geq 1.286 \times 10^{281}
\end{aligned}$$

So, "$n \log n$" is really just barely bigger than "n".

Let's play **Jeopardy Multiplication!**

Here are the rules: I give you the answer to the multiplication problem, and you give me the problem phrased as a question. And you can't use "1".

So, if I say "15", you say "What is 3×5?"

OK, let's play.

21

Good. That was easy. Let's up the ante.

91

Good. That was easy. Let's up the ante.

91

What is 7×13?

Let's do 8051.

Let's do 8051.

(Thinking, thinking ... . Hmm,

$$8051 = 8100 - 49 = 90^2 - 7^2 = (90 - 7)(90 + 7) = 83 \times 97.$$

Got it!)

What is 83×97?

So, here's what we don't know:
How many steps does it take to come up with the answer, if you are given an n-digit number which *can be* factored?
(A trick problem would be: 17. The only way to write it as $a \times b$ is to use 1, and that was ruled out. So, prime numbers cannot be factored, and the thing we don't know is how long it takes to factor the non-primes.)

The best answer we have so far is about $10^{n^{1/3}}$ steps, and even this is not a theorem, but our algorithm (the *number field sieve*) seems to work in practice.

This is all crucially important for the security of Internet commerce. Or I should say that Internet commerce relies on the premise that we *cannot* factor much more quickly than that.

Here's something else, also related to multiplication.

Let's look at the multiplication table, but not necessarily up to 10×10, but more generally the $N \times N$ multiplication table.

It has N^2 entries. It is a symmetric matrix, so most entries appear at least twice. What we don't know:

How many different numbers appear in the table?

Let $M(N)$ be the number of distinct entries in the $N \times N$ multiplication table.

$\times$	1	2	3	4	5
1	**1**	**2**	**3**	**4**	**5**
2	2	4	**6**	**8**	**10**
3	3	6	**9**	**12**	**15**
4	4	8	12	**16**	**20**
5	5	10	15	20	**25**

So, $M(5) = 14$.

$\times$	1	2	3	4	5	6	7	8	9	10
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	2	4	6	8	10	**12**	**14**	**16**	**18**	**20**
3	3	6	9	12	**15**	18	**21**	**24**	**27**	**30**
4	4	8	12	16	20	24	**28**	**32**	**36**	**40**
5	5	10	15	20	**25**	30	**35**	40	**45**	**50**
6	6	12	18	24	30	36	**42**	**48**	**54**	**60**
7	7	14	21	28	35	42	**49**	**56**	**63**	**70**
8	8	16	24	32	40	48	56	**64**	**72**	**80**
9	9	18	27	36	45	54	63	72	**81**	**90**
10	10	20	30	40	50	60	70	80	90	**100**

$M(10) = 42.$

It may be too difficult to expect a neat exact formula for $M(N)$.

Instead, we could ask for its order of magnitude, or even approximate order of magnitude.

For example, does $M(N)$ go to infinity like a constant times N^2, or more slowly. That is, maybe there is a positive number c with

$$M(N) > cN^2$$

for all N. Or maybe for *every* positive number c,

$$M(N) < cN^2$$

for infinitely many choices for N or even for all large N.

Here are some values of $M(N)/N^2$ (Brent & Kung 1981):

N	$M(N)$	$M(N)/N^2$
1	1	1.0000
3	6	0.6667
7	25	0.5102
15	89	0.3956
31	339	0.3528
63	1237	0.3117
127	4646	0.2881
255	17577	0.2703
511	67591	0.2588
1023	258767	0.2473
2047	1004347	0.2397
4095	3902356	0.2327
8191	15202049	0.2266

And some more values (Brent & Kung 1981, Brent 2012):

N	$M(N)$	$M(N)/N^2$
$2^{14}-1$	59410556	0.2213
$2^{15}-1$	232483839	0.2165
$2^{16}-1$	911689011	0.2123
$2^{17}-1$	3581049039	0.2084
$2^{18}-1$	14081089287	0.2049
$2^{19}-1$	55439171530	0.2017
$2^{20}-1$	218457593222	0.1987
$2^{21}-1$	861617935050	0.1959
$2^{22}-1$	3400917861267	0.1933
$2^{23}-1$	13433148229638	0.1909
$2^{24}-1$	53092686926154	0.1886
$2^{25}-1$	209962593513291	0.1865

And some statistically sampled values (Brent & P 2012):

N	$M(N)/N^2$	N	$M(N)/N^2$
2^{30}	0.1774	2^{100000}	0.0348
2^{40}	0.1644	2^{200000}	0.0312
2^{50}	0.1552	2^{500000}	0.0269
2^{100}	0.1311	$2^{1000000}$	0.0240
2^{200}	0.1119	$2^{2000000}$	0.0216
2^{500}	0.0919	$2^{5000000}$	0.0186
2^{1000}	0.0798	$2^{10000000}$	0.0171
2^{2000}	0.0697	$2^{20000000}$	0.0153
2^{5000}	0.0586	$2^{50000000}$	0.0133
2^{10000}	0.0517	$2^{100000000}$	0.0122
2^{20000}	0.0457	$2^{200000000}$	0.0115
2^{50000}	0.0390	$2^{500000000}$	0.0095

Paul Erdős studied this problem in two papers, one in 1955, the other in 1960.

Paul Erdős, 1913–1996

In 1955, Erdős proved (in Hebrew) that $M(N)/N^2 \to 0$ as $N \to \infty$ and indicated that it was likely that $M(N)$ is of the shape $N^2/(\log N)^E$.

In 1960, at the prodding of Linnik and Vinogradov, Erdős identified (in Russian) the value of "E". Let

$$E = 1 - \frac{1 + \log\log 2}{\log 2} = 0.08607\ldots.$$

Then $M(N) = N^2/(\log N)^{E+o(1)}$ as $N \to \infty$.

(Here, "$o(1)$" is a function that tends to 0 as $N \to \infty$.)

However, the formula $N^2/(\log N)^E$ doesn't look too good with our numbers. For example, at $N = 2^{5\cdot 10^8}$, $1/(\log N)^E \approx .1841$, or close to 20 times higher than the experimental value .0095. While at $N = 2^{30}$ it is only 4 times higher.

In work of Tenenbaum progress was made (in French) in nailing down the "$o(1)$".

In 2008, Ford showed (in English) that $M(N)$ is of order of magnitude

$$\frac{N^2}{(\log N)^E(\log\log N)^{3/2}}.$$

No matter the language,
we still don't know an asymptotic estimate for $M(N)$,
despite this just being about multiplication tables!

We have seen there is a lot we don't about multiplication, but what about addition?

Here's a famous problem due to Erdős & Szemerédi that involves both concepts, in fact, their interaction:

Among all sets $\mathcal{A}$ of N positive integers what is the minimum value of

$$|\mathcal{A}+\mathcal{A}| \ + \ |\mathcal{A}\cdot\mathcal{A}|?$$

Here $\mathcal{A}+\mathcal{A}$ is the set of all numbers $a+b$ where $a, b \in \mathcal{A}$, and $|\mathcal{A}+\mathcal{A}|$ is the number of elements in this set. Similarly for $|\mathcal{A}\cdot\mathcal{A}|$.

The notation might be unfamiliar, so lets look at some numerical examples.

If $\mathcal{A}$ consists of the numbers $1, 2, 3, \ldots, N$, then the addition table involves numbers from 2 to $2N$, for a total of $2N - 1$ numbers. That's not many given that there are N^2 entries in the table!

But products mostly make up for this. We just saw that there are "close" to N^2 different products.

On the other hand, take $\mathcal{A}$ as the numbers $2, 4, 8, \ldots, 2^N$. Now the addition table contains more than $\frac{1}{2}N^2$ different numbers, but the multiplication table contains just $2N - 1$ numbers.

So, if we force one table to be small, the other is large. Erdős and Szemerédi say this is always the case.

The game players with the sum/product problem:
Erdős, Szemerédi, Nathanson, Chen, Elekes, Bourgain, Chang, Konyagin, Green, Tao, Solymosi, ...

The best that they can do is show that one of the tables has at least $N^{4/3}$ different entries.

This list of mathematicians contains two Fields Medalists, a Wolf Prize winner, an Abel Prize winner, four Salem Prize Winners, and two Crafoord Prize winners. And still the problem is not solved!

So far, all of the problems we've looked at have been fairly new, as far as Mathematics goes. Here's a very old problem that we still haven't solved and involves both sums and products, liberally interpreted.

A prime number, as we saw earlier, is a trick problem in Jeopardy Multiplication. It is a number larger than 1 that cannot be factored into two smaller (positive) whole numbers. Dating to correspondence in 1742 between Goldbach and Euler, it is conjectured that every even number starting at 4 can be represented as the sum of two primes.

271 years later: **We still don't know if Goldbach's conjecture is true.**

My message: We could use a little help with these problems!!