What we still don't know about addition and multiplication

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

Christie Lecture, Bowdoin College
April 7, 2014

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.

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

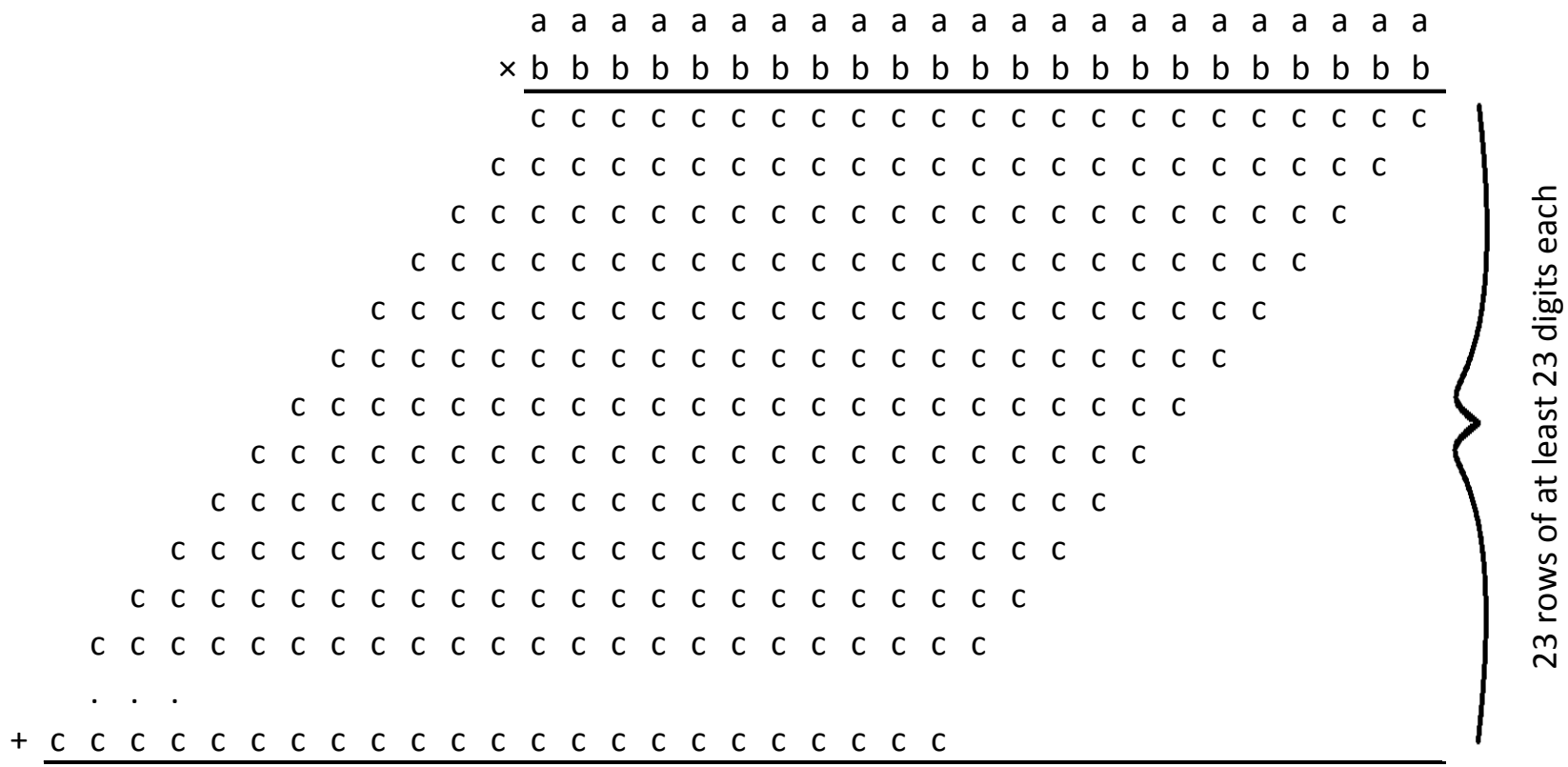
If instead you had a problem with two 23-digit numbers, well you always knew deep down that math teachers are cruel and sadistic. Just kidding! (*Aside: evil laugh* . . .)

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.


a a a a a a a a a a a a a a a a a a a a a a
× b b b b b b b b b b b b b b b b b b b b b b
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
c c c c c c c c c c c c c c c c c c c c c c
. . .
+ c c c c c c c c c c c c c c c c c c c c c c
23 rows of at least 23 digits each

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.

A. A. Karatsuba (1937–2008): Devised a faster way to multiply two n-digit numbers, in about $n^{1.6}$ elementary steps.

Karatsuba's method was later improved by Toom, Cook, Schönhage, & Strassen. After their efforts we have the *Fast Fourier Transform* that allows you to multiply in about $n \cdot L(n)$ steps, where $L(n)$ is short-hand for the number of digits of n. (So $L(n)$ is the number of digits of the number of digits of the numbers being multiplied!)

We don't know if the Fast Fourier Transform is best possible. In particular:

What is the *fastest* way to multiply?

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. You must use whole numbers larger than 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,

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 figure out the factors 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.

Let's look at an unsolved problem concerning addition.

We all recall the addition table:

+	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	11
2	3	4	5	6	7	8	9	10	11	12
3	4	5	6	7	8	9	10	11	12	13
4	5	6	7	8	9	10	11	12	13	14
5	6	7	8	9	10	11	12	13	14	15
6	7	8	9	10	11	12	13	14	15	16
7	8	9	10	11	12	13	14	15	16	17
8	9	10	11	12	13	14	15	16	17	18
9	10	11	12	13	14	15	16	17	18	19
10	11	12	13	14	15	16	17	18	19	20

The 10×10 array of sums has all the numbers from $\mathbf{2}$ to $\mathbf{20}$ for a total of 19 different sums.

If you were to try this for the $N \times N$ addition table we'd see all of the numbers from $\mathbf{2}$ to $\mathbf{2}N$ for a total of $2N - 1$ different sums.

Now, what if we were to be perverse and instead of having the numbers from 1 to N, we had some arbitrary list of N different numbers.

Can you arrange it so there are *fewer* than $2N - 1$ different sums?

The 10×10 array of sums has all the numbers from **2** to **20** for a total of 19 different sums.

If you were to try this for the $N \times N$ addition table we'd see all of the numbers from **2** to $\mathbf{2}N$ for a total of $2N - 1$ different sums.

Now, what if we were to be perverse and instead of having the numbers from 1 to N, we had some arbitrary list of N different numbers.

Can you arrange it so there are *fewer* than $2N - 1$ different sums?

If you answered "No, there are always at least $2N - 1$ different sums," you'd be right.

Now consider the reverse problem. You have a list of N different numbers, you form the addition table with themselves, and you find that there are just $2N - 1$ different sums.

Must the list be the numbers from 1 to N?

Now consider the reverse problem. You have a list of N different numbers, you form the addition table with themselves, and you find that there are just $2N - 1$ different sums.

Must the list be the numbers from 1 to N?

$\times$	2	5	8	11	14
2	**4**	**7**	**10**	**13**	**18**
5	**7**	**10**	**13**	**16**	**19**
8	**10**	**13**	**16**	**19**	**22**
11	**13**	**16**	**19**	**22**	**25**
14	**16**	**19**	**22**	**25**	**28**

There are the 9 different sums: 4, 7, 10, 13, 16, 19, 22, 25, 28, all others are repeats of these.

In fact: *If there are just $2N-1$ distinct sums when adding an N-element set to itself, then the N-element set must be an arithmetic progression.*

But what if there are $2N$ sums, or $3N-4$ sums, etc.? What structure is imposed?

Gregory Freiman: *If there are at most $C \cdot N$ distinct sums, where C is fixed, then the set is contained within some low-dimensional generalized arithmetic progression.*

As before, let $L(N)$ denote the number of digits of N.

What we still don't know:

What structure is imposed on a list of N numbers if there are few pairwise sums, but more than $C \cdot N$, say at most $N \cdot L(N)$ pairwise sums?

Imre Ruzsa has a neat unsolved problem that relates the number of pairwise sums among a given set of N numbers to the number of differences. It would seem that the two counts are always of the same magnitude. But Ruzsa proved this is not true. He asks for every set of N numbers if there is a second set, where the number of sums of the first set is approximately equal to the number of differences of the second, and vice versa. **Is this true?**

Here's something with multiplication tables.

Let's look at the $N \times N$ multiplication table using the numbers from 1 to N. With addition, we were able to count exactly how many distinct numbers appear in the table.

How many different numbers appear in the $N \times N$ multiplication 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

$$M(N)/N^2 > c$$

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

$$M(N)/N^2 < c$$

for infinitely many choices for N or perhaps 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 $M(N)/N^2$ tends to 0 as N runs off to infinity.

In 1960, at the prodding of Linnik and Vinogradov, Erdős identified (in Russian) how quickly $M(N)/N^2$ tends to 0. Recall that $L(N)$ denotes the number of (decimal) digits of N. There is a constant (let's call it E for Erdős),

$$E = 0.08607133\ldots,$$

such that $M(N)/N^2$ is about $1/L(N)^E$. That is,

$$M(N) \text{ is about } N^2/L(N)^E.$$

A conjecture both deep and profound
is whether a circle is round.
In a paper of Erdős,
written in Kurdish,
a counterexample is found.

Leo Moser

Erdős says that $M(N)$ is "*about*" $N^2/L(N)^E$. What's with this weasel word "*about*"? Answer: We're saying that no other exponent on $L(N)$ than the Erdős constant E does better. But there could be lower order factors.

In work of Tenenbaum progress was made (in French) in nailing this down.

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

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

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

Let me close with one unified problem about addition and multiplication together. It's due to **Erdős & Szemerédi**.

Look at **both** the addition and multiplication tables and count the number of distinct entries.

We've seen that if we take the first N numbers we get about $N^2/L(N)^E$ entries (since the $2N-1$ from the addition table is just "noise" compared to the huge number from the multiplication table).

At the other extreme, if we take for our N numbers the powers of 2, namely $1, 2, 4, \ldots, 2^{N-1}$, then there are at least $\frac{1}{2}N^2$ distinct entries in the addition table and only $2N-1$ entries in the multiplication table.

The question is: if we make one of these small, must the other always be large?

×	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

+	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	11
2	3	4	5	6	7	8	9	10	11	12
3	4	5	6	7	8	9	10	11	12	13
4	5	6	7	8	9	10	11	12	13	14
5	6	7	8	9	10	11	12	13	14	15
6	7	8	9	10	11	12	13	14	15	16
7	8	9	10	11	12	13	14	15	16	17
8	9	10	11	12	13	14	15	16	17	18
9	10	11	12	13	14	15	16	17	18	19
10	11	12	13	14	15	16	17	18	19	20

Many products Few sums

$$\{1, 2, \ldots, N\}$$

×	1	2	4	8	16	32	64	128	256	512
1	1	2	4	8	16	32	64	128	256	512
2	2	4	8	16	32	64	128	256	512	1024
4	4	8	16	32	64	128	256	512	1024	2048
8	8	16	32	64	128	256	512	1024	2048	4096
16	16	32	64	128	256	512	1024	2048	4096	8192
32	32	64	128	256	512	1024	2048	4096	8192	16384
64	64	128	256	512	1024	2048	4096	8192	16384	32768
128	128	256	512	1024	2048	4096	8192	16384	32768	65536
256	256	512	1024	2048	4096	8192	16384	32768	65536	131072
512	512	1024	2048	4096	8192	16384	32768	65536	131072	262144

+	1	2	4	8	16	32	64	128	256	512
1	2	3	5	9	17	33	65	129	257	513
2	3	4	6	10	18	34	66	130	258	514
4	5	6	8	12	20	36	68	132	260	516
8	9	10	12	16	24	40	72	136	264	520
16	17	18	20	24	32	48	80	144	272	528
32	33	34	36	40	48	64	96	160	288	544
64	65	66	68	72	80	96	128	192	320	576
128	129	130	132	136	144	160	192	256	384	640
256	257	258	260	264	272	288	320	384	512	768
512	513	514	516	520	528	544	576	640	768	1024

Few products Many sums

$$\{1, 2, 4, \ldots, 2^{N-1}\}$$

Must one always be large?

Put more precisely: **If we have N distinct numbers, must one of**

- **the number of distinct pairwise sums,**
- **the number of distinct pairwise products,**

be greater than $N^{1.999}$ for all large values of N?

We don't know.

And it's not for lack of trying.

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

The best that's been proved (**Solymosi**) is that there are 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, two Crafoord Prize winners, and an Aisenstadt Prize winner.

And still the problem is not solved!

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

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

THANK YOU