What we still don't know about addition and multiplication

Ross Program, July 18, 2023

Carl Pomerance
Dartmouth College (emeritus)
University of Georgia (emeritus)

Find 483×784.

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

To a lot of people, this is higher math!

But a mathematician would ask: how much work is necessary in general to multiply?

Say we're mutliplying two 23-digit numbers.

Of course the amount of work depends not only on the length of the numbers. 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 a
                        × b 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 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.

Addition of two n-digit numbers is clearly of order n (unless you do something silly like adding 1 lots of times), and the same goes for subtraction. Could the complexity of multiplication also be of order n?

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

Here is Karatsuba's idea: leverage that addition and subtraction are cheap and use high school algebra!

Say the numbers A and B each have n digits. Let $m = n/2$ (okay, we assume that n is even). Write

$$A = A_1 10^m + A_0, \quad B = B_1 10^m + B_0,$$

where A_1, A_0, B_1, B_0 are all smaller than 10^m, so have at most m digits. Then our product AB is

$$AB = (A_1 B_1)10^{2m} + (A_1 B_0 + A_0 B_1)10^m + A_0 B_0,$$

so our problem is broken down to 4 smaller multiplication problems, each of size $m \times m$, namely

$$A_1 B_1, \quad A_1 B_0, \quad A_0 B_1, \quad A_0 B_0,$$

and each of these would seem to take 1/4 as much work as the original problem.

So, unfortunately 4 problems each taking 1/4 as much work, is no savings!

However, we also have

$$(A_1 + A_0)(B_1 + B_0) = A_1B_1 + (A_1B_0 + A_0B_1) + A_0B_0,$$

so we can really do it in 3 multiplications, not 4 (!). Namely,

$$A_1B_1, \quad A_0B_0, \quad (A_1 + A_0)(B_1 + B_0).$$

After we do these, we have our three coefficients, where the middle one, $A_1B_0 + A_0B_1$, is the third product minus the first two:

$$A_1B_0 + A_0B_1 = (A_1 + A_0)(B_1 + B_0) - A_1B_1 - A_0B_0.$$

This idea can then be used on each of the three smaller multiplication problems, and so on down the fractal road, ending in about $n^{1.6}$ elementary steps.

Karatsuba's method was later improved by Toom, Cook, Schönhage, & Strassen. Instead of complexity n^c with a constant $c > 1$, they achieved something almost as fast as $n \cdot \ln(n)$. This was the *Fast Fourier Transform*.

Small improvements were made by Fürer in 2007, by De, Kurur, Saha, & Saptharishi in 2008, and by Harvey & van der Hoeven in 2019, so we now know that the complexity of multiplication is at most of order $n \cdot \ln(n)$.

But, we don't know if we have reached the limit! In particular:

What is the *fastest* way to multiply?

Let's play **Multiplication Jeopardy!**

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.

91

91

What is 7×13?

91

What is 7×13?

Another one: 247

91

What is 7×13?

Another one: 247

What is 13×19?

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 (known as 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.

A couple of words about factoring, that is, on how to win at **Multiplication Jeopardy**.

The trick with 8051 (due to **Fermat**), namely that $8051 = 8100 - 49$, is sort of generalizable as might be illustrated by 1649.

A couple of words about factoring, that is, on how to win at **Multiplication Jeopardy**.

The trick with 8051 (due to **Fermat**), namely that $8051 = 8100 - 49$, is sort of generalizable as might be illustrated by 1649.

We look for a square just above 1649. The first is $41^2 = 1681$. Well

$$41^2 - 1649 = 32 \quad \text{and } \mathbf{32} \text{ is } \mathbf{not} \text{ a square.}$$

Try again. The next square is $42^2 = 1764$ and

$$42^2 - 1649 = 115 \quad \text{and } \mathbf{115} \text{ is } \mathbf{not} \text{ a square.}$$

Trying again, the next square is $43^2 = 1849$ and

$$43^2 - 1649 = 200 \quad \text{and } \mathbf{200} \text{ is } \mathbf{not} \text{ a square.}$$

But wait, look at our 3 non-squares: 32, 115, 200.

Note that we can **make** a square out of two of them:

$$32 \times 200 = 6400 = 80^2.$$

From the previous slide we have

$$41^2 \equiv 32 \pmod{1649} \text{ and } 43^2 \equiv 200 \pmod{1649},$$

so

$$41^2 \times 43^2 \equiv 32 \times 200 \pmod{1649}.$$

This can be rewritten as

$$(41 \times 43)^2 \equiv 80^2 \pmod{1649}.$$

Now $41 \times 43 \equiv 114 \pmod{1649}$, so we have

$$114^2 \equiv 80^2 \pmod{1649}.$$

It is not true that $1649 = (114 - 80)(114 + 80)$, but it is true that the **greatest common divisor** of $114 - 80 = 34$ with 1649 is 17. (And finding the greatest common divisor of two numbers is speedy.)

Hey! That proves that 1649 is divisible by 17. Dividing, the other factor is 97. So, we have it: **What is 17×97?**

The various elements here can actually be made into a speedy algorithm, the **quadratic sieve**. The **number field sieve** is a fancier version but has the same underlying flavor of assembling squares whose difference is divisible by N, the number to be factored.

Despite our success with factoring, it still is very difficult. Hard numbers with 300 decimal digits are beyond our reach at present. The really amazing thing is we can apply our ignorance to make a secure cryptographic system!

Here are three famous unsolved problems involving both addition and multiplication:

Goldbach's conjecture: **Every even number starting with 4 is the sum of two primes.**

The twin prime conjecture: **There are infinitely many pairs of primes that differ by 2.**

The ABC conjecture: **If $A+B=C$ where no prime divides all three, must the product of the primes dividing ABC exceed $C^{1-\epsilon}$? (Assume $\epsilon > 0$ is arbitrary but fixed and C is large.)**

Here's another problem that I only recently heard about.

Find 2 numbers a, b where $a + b = a \times b$:

Here's another problem that I only recently heard about.

Find 2 numbers a, b where $a + b = a \times b$:

Easy, take $a = b = 2$.

Are there any other integral solutions?

Here's another problem that I only recently heard about.

Find 2 numbers a, b where $a + b = a \times b$:

Easy, take $a = b = 2$.

Are there any other integral solutions? No.

How about 3 numbers with the same sum and product?

Here's another problem that I only recently heard about.

Find 2 numbers a, b where $a + b = a \times b$:

Easy, take $a = b = 2$.

Are there any other integral solutions? No.

How about 3 numbers with the same sum and product?

$1 + 2 + 3 = 1 \times 2 \times 3$.

Again, there are no other solutions, and the same goes for 4 numbers ($1, 1, 2, 4$ is the unique choice).

But if I ask for 5 numbers with equal sum and product, there are 3 solutions:

$$1, 1, 1, 2, 5 \qquad 1, 1, 1, 3, 3 \qquad 1, 1, 2, 2, 2$$

With some work one finds that with 444 numbers there is a unique solution.

Here's what we don't know:

Is 444 the largest n such that there is a unique solution to n numbers with the same sum and product?

This has been searched for up to 10^{13} and each n to this height has at least two solutions. See A033179 on OEIS.

One can also ask a weaker question:

Are there infinitely many n where there is a unique solution to the sum-equals-product problem with n integers?

Here's a famous problem (in disguised form):

Consider $\ln(A(N))$, where $A(N)$ is the least common multiple of $1, 2, \ldots, N$. It is uncannily close to N, or so it seems.

For example: $\ln(A(100{,}000{,}000)) \approx 99{,}998{,}242.8$.

For $N \geq 3$, do we always have $|\ln(A(N)) - N| < \sqrt{N}(\ln(N))^2$?

The Clay Mathematics Institute offers $1,000,000 for a proof!

Here's an unsolved problem concerning just 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 added to themselves.

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 $2N$ 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.

Here's an example where there are many different sums:

+	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**

So, sometimes there are few distinct sums and sometimes many.

What structure is forced on the set if there are few distinct sums?

We know the answer when there are very few distinct sums:

Gregory Freiman

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	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**

So $M(10) = 42$.

It is really amazing that though $M(N)$ is not far below N^2 looking "from a distance", if we look "close up" we see that $M(N)/N^2$ tends to 0 as N grows larger and larger.

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

After **Erdős**, **Tenenbaum**, and **Ford**, we now know the (complicated) order of magnitude for $M(N)$ as N grows. (It's $N^2/(\ln(N))^E(\ln(\ln(N)))^{1.5}$, where $E = 0.086\ldots$ is an explicitly known constant.)

Paul Erdős, 1913–1996

Find an asymptotic formula for $M(N)$ as N grows?

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

Look at **both** the addition and multiplication tables for N carefully chosen numbers.

We've seen that if we take the first N numbers we get close to N^2 distinct entries in the multiplication table, but few in the addition 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.

If we take N *random* numbers, then it's likely both tables have close to $\frac{1}{2}N^2$ distinct entries.

The question is: **If we choose our numbers so that the number of distinct entries in one table is small, must the other always be large?** (More precisely, if $\epsilon > 0$ is fixed and N is sufficiently large, must every choice of N numbers have the number of distinct entries in the addition and multiplication tables combined be $> N^{2-\epsilon}$?)

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

The best that's been proved (**Solymosi**) is that one table must have at least $N^{4/3}$ different entries. (Improved recently by **Rudnev & Stevens** to $N^{4/3+2/1167}$.)

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