Dartmouth Algebra & Number Theory Seminar

June 2, 2026

Problems and Results in Combinatorial Number Theory

Carl Pomerance, Dartmouth College

The last few days have been a busy time for combinatorial number theory, broadly construed.

First, a disproof of the Erdős unit distance conjecture was announced. This is the conjecture that if one has n points in the plane, then the number of pairs of points at a unit distance is $\leq n^{1+o(1)}$.

REMARKS ON THE DISPROOF OF THE UNIT DISTANCE CONJECTURE

NOGA ALON, THOMAS F. BLOOM, W. T. GOWERS, DANIEL LITT, WILL SAWIN, ARUL SHANKAR, JACOB TSIMERMAN, VICTOR WANG, AND MELANIE MATCHETT WOOD

ABSTRACT. We present a short, digested, human-verified version of the recent OpenAI-generated counterexample to the Erdős unit distance conjecture, and a sequence of reflections on it. The argument relies crucially on ideas that may, at least in retrospect, be attributed to Ellenberg-Venkatesh, Golod-Shafarevich, and Hajir-Maire-Ramakrishna.

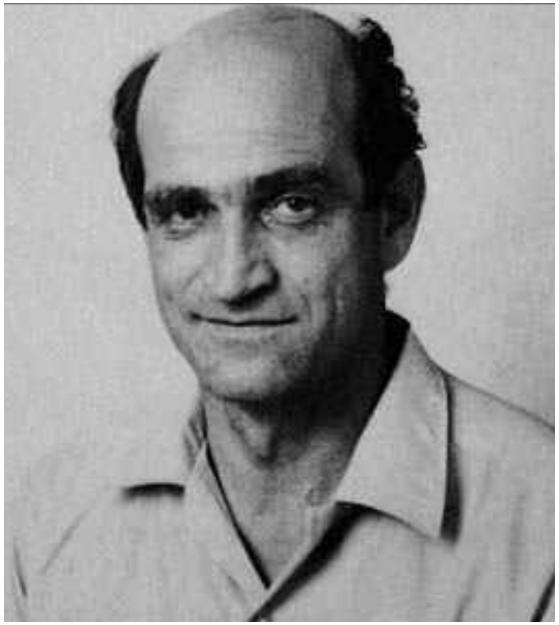
Then, there was a breakthrough on the sum-product problem. The origin of this problem, due to Erdős and Szemerédi, is to look at both the $n \times n$ addition table and multiplication table, and notice that the addition table has few distinct numbers compared with the multiplication table. If one changes the n numbers from $\{1, 2, \ldots, n\}$ to $\{2^1, 2^2, \ldots, 2^n\}$, then the addition table has many distinct numbers, while the multiplication table has few. They conjectured that this is always the case: given a set A of n integers, then $|A + A| + |A \cdot A| > n^{2-o(1)}$. In fact, this was conjectured as well when A is a set of real numbers. And now, this generalization to reals has been disproved.

THE SUM-PRODUCT CONJECTURE IS FALSE FOR REAL NUMBERS

THOMAS F. BLOOM, WILL SAWIN, CARL SCHILDKRAUT, AND DMITRII ZHELEZOV

Lets talk about the Erdős–Straus conjecture.

Paul Erdős



Ernst Straus

(Drawing by LeUyen Pham, illustrator of The Boy Who Loved Math, by Deborah Heiligman)

In 1948, Paul Erdős and Ernst Straus conjectured that for every integer $n \geq 2$, there are positive integers x, y, z such that

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

The first question: **Why make this conjecture???**

The Rhind papyrus, ca. 1500 BCE

Apparently the ancient Egyptians were especially fond of fractions with numerator 1, so-called *unit fractions*. To represent other fractions, they would find some unit fractions that summed to what they wanted.

For example, consider 5/7. We have

$$\frac{5}{7} = \frac{1}{2} + \frac{1}{5} + \frac{1}{70}.$$

The Rhind papyrus gave a list of such representations, now called Egyptian fractions.

One might try and describe the set of rationals which have a representation as a sum of k unit fractions.

When $k = 1$, we have the unit fractions themselves.

When $k = 2$, we have the identity

$$\frac{2}{n} = \frac{1}{n} + \frac{1}{n},$$

which shows that each $2/n$ is in class 2 for n odd. But there are many more fractions in the class 2, for example 5/6 is.

Theorem (**Stewart, 1964**). If $(m,n) = 1$, we have m/n the sum of 2 unit fractions if and only if m is a divisor of the sum of two coprime divisors of n.

For example, 2 and 3 are coprime divisors of 6 and 5 is a divisor of $2+3$, so 5/6 is the sum of 2 unit fractions. But 5/7 is not, nor is 4/17, nor is any m/p with p an odd prime and $m \nmid p+1$.

So, the situation when m/n is or is not the sum of two unit fractions is basically understood.

Which brings us to the sum of three unit fractions:

$$\frac{m}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

Note that if $m \leq 3$, then the problem is trivial.

So, the case of $m = 4$, the arena of the Erdős–Straus conjecture, is the first interesting case.

But why would one suspect that for every $n \geq 2$ with $m = 4$ there is a solution? Could this really be true?

First note that if each $4/p$ with p prime is a sum of three unit fractions, then so is each $4/n$. Indeed, if $p \mid n$, say $n = jp$, then dividing a representation for $4/p$ by j gets a representation for $4/n$.

One can use the Stewart theorem and similar ideas to get many congruence classes for which the conjecture holds. Finding these classes helps enormously with computation.

Using congruences, as reported in Mordell's famous book on Diophantine equations, one learns that the Erdős–Straus conjecture holds for every prime p except possibly for the quadratic residues mod 840, that is, except for those p with

$$p \equiv 1,\ 121,\ 169,\ 289,\ 361,\ \text{or } 529 \pmod{840}.$$

Using congruences such as these, about 12 years ago, Salez verified the Erdős–Straus conjecture to 10^{17}. Just recently, Mihnea and Dumitru extended the search to 10^{18}.

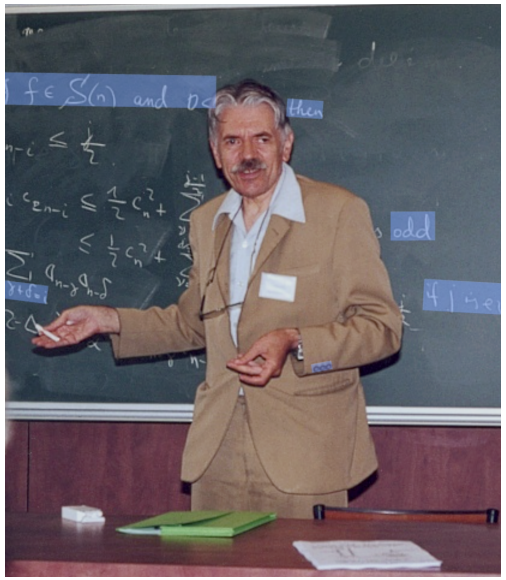
Robert C. Vaughan

In 1970 Vaughan used the existence of many congruences and the large sieve to get an excellent upper bound for the number of possible exceptions up to N: It is $O(N/\exp(c(\log N)^{2/3}))$ for an appropriate positive constant c.

If you can't prove it, generalize it. . .


Wacław Sierpiński

Sierpiński conjectured that every $5/n$ for $n \geq 2$ is a sum of three unit fractions.



Andrzej Schinzel

Schinzel then generalized further: For every $m \geq 4$, we have m/n the sum of three unit fractions for all $n > N_m$, a constant depending on m.

The Ramanujan Journal (2026) 69:31
https://doi.org/10.1007/s11139-025-01312-2

Exceptions to the Erdős–Straus–Schinzel conjecture

Carl Pomerance[1] · **Andreas Weingartner**[2]

For Krishnaswami Alladi on his 70th birthday

Received: 9 December 2025 / Accepted: 25 December 2025 / Published online: 14 January 2026

Andreas Weingartner

With Weingartner, we have investigated the Schinzel conjecture numerically for m up to 15. For example, when $m = 8$ we have checked up to 10^{13} and the only exceptional n found are $1, 2, 3, 11, 17, 131, 241$. See the table on the next slide.

m	all exceptions $n \le N$	Count	N
4	1	1	10^{18}
5	1	1	10^{18}
6	1	1	10^{13}
7	1, 2	2	10^{13}
8	1, 2, 3, 11, 17, 131, 241	7	10^{13}
9	1, 2, 5, 11, 19	5	10^{12}
10	1, 2, 3, 7, 11, 43, 61, 67, 181	9	10^{12}
11	1, 2, 3, 4, 37	5	10^{12}
12	1, 2, 3, 5, 7, 13, 25, 29, 31, 37, 73, 97, 193, 433, 577, 1129, 1657, 1873, 2521, 2593, 3433, 10369, 12049, 12241	24	10^{12}
13	1, 2, 3, 4, 5, 7, 14, 53, 61, 67, 79, 211, 281	13	10^{12}
14	1, 2, 3, 4, 5, 17, 19, 29, 59, 257, 353, 841	12	10^{12}
15	1, 2, 3, 4, 8, 16, 17, 19, 23, 31, 34, 47, 53, 61, 79, 113, 122, 137, 151, 197, 226, 233, 271, 541, 1103, 1171, 1367, 4201, 6301, 12601, 16831, 20521	32	10^{12}

Already in his 1970 paper, Vaughan proved a general upper bound for the distribution of exceptions to the Schinzel conjecture: The number of $n \leq N$ for which m/n is not the sum of three unit fractions is $O(N/\exp(c(m)(\log N)^{2/3})$, where $c(m) > 0$.

With Weingartner, we were able to prove this with $c(m) = c/\varphi(m)^{1/3}$, with c an absolute positive constant, uniformly for $m \leq (\log N)^2$.

But mainly my work with Weingartner deals with the exceptional set in the Schinzel variant. Schinzel's conjecture is that for each m there is some N_m such that when $n > N_m$ we have m/n the sum of three unit fractions. How large is this N_m? For example, the Erdős–Straus conjecture is that $N_4 = 1$. And empirically it seems that $N_8 = 241$. We show that as m gets large, exceptions become enormous.

Theorem (Pomerance & Weingartner). For each $\epsilon > 0$ there is a bound m_ϵ such that if $m > m_\epsilon$ there is a number $n > \exp(m^{1/3-\epsilon})$ with m/n not the sum of three unit fractions.

We conjecture (and give a heuristic) that the largest counterexample to the Schinzel conjecture is near to $\exp(m^{1/2})$.

Our proof uses many ideas from a recent paper of Elsholtz and Tao on counting the number of triples x, y, z where $4/n = 1/x + 1/y + 1/z$. They also do a good job of citing the many researchers who have obtained partial results.

Christian Elsholtz

Paul Erdős & Terence Tao

#A47 INTEGERS 26 (2026)

REMARKS ON THE MIDDLE BINOMIAL COEFFICIENT

Carl Pomerance

Mathematics Department, Dartmouth College, Hanover, New Hampshire
carlp@math.dartmouth.edu

Received: 1/15/26, Accepted: 3/23/26, Published: 4/3/26

A few years ago I was listening to the various end-of-year student presentations, as are going on today. One was in combinatorics and mentioned Catalan numbers, namely numbers of the form

$$\frac{1}{n+1}\binom{2n}{n}.$$

It struck me that this expression is not obviously integral, though there are many combinatorial proofs that it is. What might be a number-theoretic proof? And are there other expressions than $n+1$ that are guaranteed to divide $\binom{2n}{n}$?

So I wrote a largely expository paper that was published in the American Mathematical Monthly. One of the theorems proved is that for each fixed $k>0$, $n+k \mid \binom{2n}{n}$ for all n in a set of asymptotic density 1. I left it as an exercise for the reader to show that $(n+1)\ldots(n+k)\mid\binom{2n}{n}$ almost always.

Fast forward to last Fall. A group trying to use AI to prove some Erdős conjectures rediscovered my paper, and began improving it. Now if it were a student doing this, I'd cheer them on. But I didn't want to be bested by a machine. So, I proved a best possible variant: For any constant $\alpha < 1/\log 4$ and all positive $k < \alpha \log n$, we have $(n+1)\ldots(n+k) \,|\, \binom{2n}{n}$ on a set of asymptotic density 1.

Plus some other results.

One of the crew using AI, Boris Alexeev, fed my proof into the machine, which promptly found some errors! So, I guess it had the last laugh.

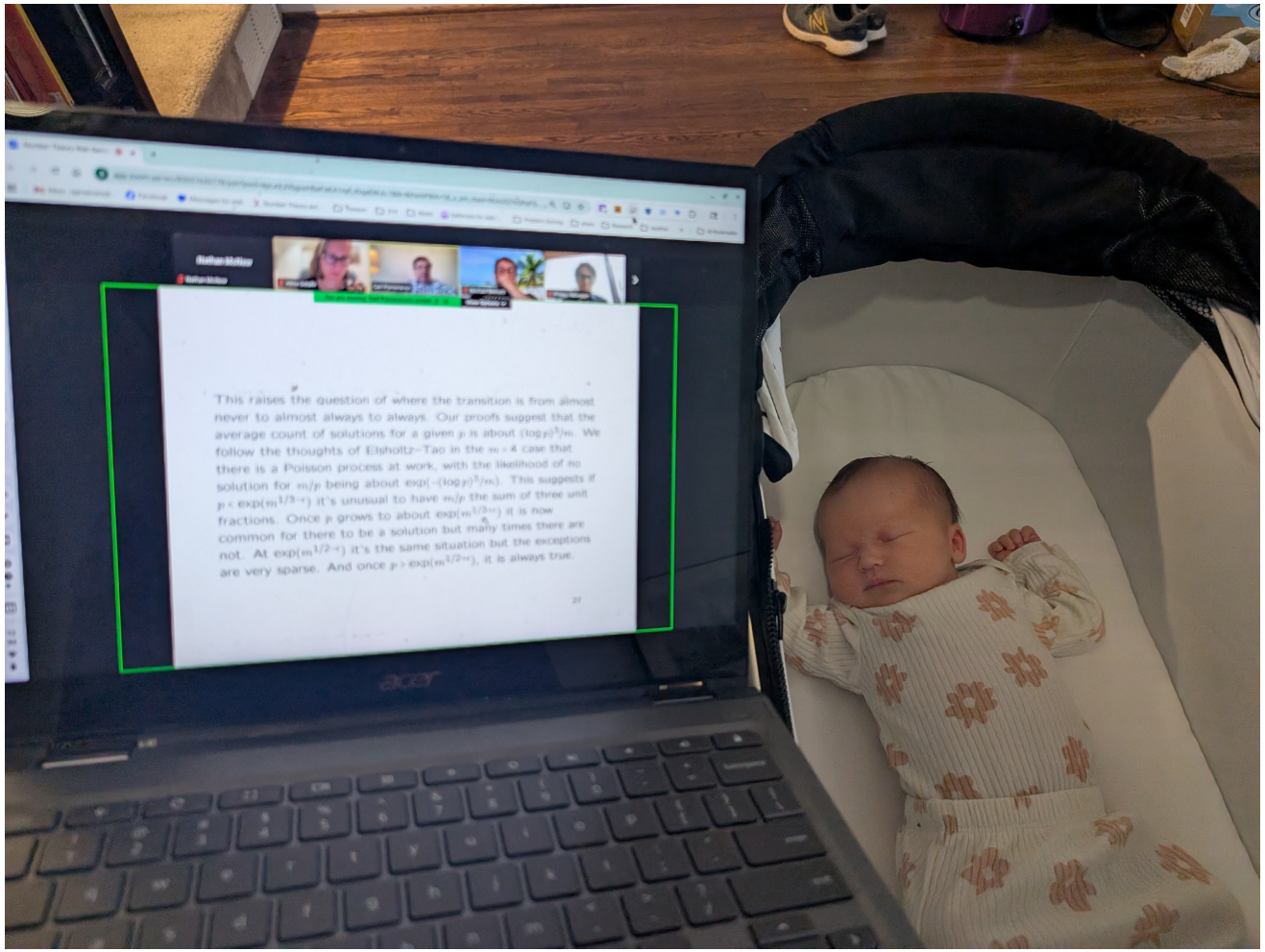
MATCHABLE NUMBERS

NATHAN MCNEW AND CARL POMERANCE

ABSTRACT. We say a natural number n is matchable if there is a bijection from the set of $\tau(n)$ divisors of n to the set $\{1, 2, \ldots, \tau(n)\}$, where corresponding numbers are relatively prime. We show that the set of matchable numbers has an asymptotic density, which we compute, and we show that every squarefree number is matchable. We also present some related unsolved problems.

(To appear in Mathematika)

Nathan McNew


This raises the question of where the transition is from almost never to almost always to always. Our proofs suggest that the average count of solutions for a given p is about $(\log p)^3/m$. We follow the thoughts of Elsholtz–Tao in the $m = 4$ case that there is a Poisson process at work, with the likelihood of no solution for m/p being about $\exp(-(\log p)^3/m)$. This suggests if $p < \exp(m^{1/3-\epsilon})$ it's unusual to have m/p the sum of three unit fractions. Once p grows to about $\exp(m^{1/3+\epsilon})$ it is now common for there to be a solution but many times there are not. At $\exp(m^{1/2-\epsilon})$ it's the same situation but the exceptions are very sparse. And once $p > \exp(m^{1/2+\epsilon})$, it is always true.
27
acer

Hazel McNew

Is there a *coprime matching* between the set of $\tau(n)$ divisors of n and $\{1,2,\ldots,\tau(n)\}$? If so, we say n is matchable. This concept was introduced by Bernardo Recamán on mathoverflow in 2022. He asked if more numbers are matchable than not.

For example, 6 is matchable:

$$1 \iff 4,\ 2 \iff 3,\ 3 \iff 2,\ 6 \iff 1.$$

And 8 is not matchable: The divisors are $\{1,2,4,8\}$ which contains 3 even numbers, but $\{1,2,3,4\}$ contains only 2 odd numbers. Similarly all the multiples of 4, starting with 8, are not matchable.

If m is composite, then $27m$ is not matchable. (Use a similar argument with multiples of 3: there are too many of them among the divisors of $27m$.)

So the upper density of the set of matchable numbers is $\leq (1 - 2^{-2})(1 - 3^{-3})$.

This generalizes to all primes, and we get the upper density of the matchable numbers is at most

$$\alpha := \prod_p (1 - p^{-p}) = 0.72199023441955\ldots .$$

Theorem. (McNew and Pomerance) The asymptotic density of the set of matchable numbers exists and is α.

On the way to proving this we show that every squarefree number is matchable.

Say an integer n is an M-number if it is not divisible by any p^p with p prime. So the asymptotic density of the set of M-numbers is α. We show that but for a possible exceptional set of density 0, every M-number is matchable, and that the set of non-M-numbers that are matchable has asymptotic density 0. We conjecture that the first of these density-0 sets is empty.

Say n is strongly matchable if there is a coprime matching between the $\tau(n)$ divisors of n and every coprime arithmetic progression of length $\tau(n)$. For example, though 4 is matchable, it is not strongly matchable: Try matching $\{1,2,4\}$ with $\{2,3,4\}$. Every strongly matchable number is an M-number, and we conjecture the converse. We are able to prove that a positive proportion of the M-numbers are strongly matchable.

ON A FAMILY OF SUBGROUPS OF THE MULTIPLICATIVE GROUP MOD n

CARL POMERANCE

ABSTRACT. For each pair j, n with $n > j$, we consider the subgroup of the multiplicative group mod n of residues with order dividing $n - j$. We generalize some results in the case $j = 1$ due to Erdős and the current author. The case $j = 0$ is of particular interest.

(To appear in the Bulletin of the Australian Mathematical Society)

Last November Hendrik Lenstra wrote to me asking about the function

$$\psi(n) = \#\{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^n = 1\}.$$

He writes: So that you may judge for yourself how interesting or non-interesting the function ψ is, let me tell you the ring-theoretic result in which I encountered it. It comes from work that I have been doing together with Mike Daas (a recent Leiden PhD, now in Luxemburg) and Lars Pos (a Leiden bachelor student), on the subject of a classical theorem of Jacobson from 1945. This theorem asserts that if n is a positive integer, and R is a ring with the property that all $x \in R$ satisfy $x^{n+1} = x$, then R is commutative.

Continuing: For $n = 1$ this is very classical: using $x^2 = x$ for $x = -1, a, b, a + b$, one deduces readily $ab = ba$. So, four x's are sufficient. I was quite surprised when I learnt that, still for $n = 1$, TWO x's suffice, namely $x = a$ and $x = ab - ba$. That is a charming and not entirely trivial exercise! (Whether a single x does it, we do not know!) How is this for general n? One of our results is the following upper bound for the number of (cleverly chosen) x's that suffice:

$$\varphi(n) + \psi(n) + 2\lceil \log(\tau(n))/\log 2 \rceil + E,$$

where $E \in \{0, 1, 2, 3\}$. [which he describes explicitly]

So the issue is to understand the function

$$\psi(n) = \#\{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^n = 1\}.$$

MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 173
JANUARY 1986, PAGES 259–279

On the Number of False Witnesses for a Composite Number

By Paul Erdös and Carl Pomerance*

Abstract. If a is not a multiple of n and $a^{n-1} \not\equiv 1 \bmod n$, then n must be composite and a is called a "witness" for n. Let $F(n)$ denote the number of "false witnesses" for n, that is, the number of $a \bmod n$ with $a^{n-1} \equiv 1 \bmod n$. Considered here is the normal and average size of $F(n)$ for n composite. Also considered is the situation for the more stringent Euler and strong pseudoprime tests.

This paper deals with the function

$$F(n) = \#\{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^{n-1} = 1\},$$

and among other things, it finds the normal order and average order when n is composite.

So, I thought it would be interesting to define a family of subgroups:

$$F_j(n) = \#\{a \in (\mathbb{Z}/n\mathbb{Z})^* : a^{n-j} = 1\},$$

where Lenstra's $\psi(n)$ is $F_0(n)$ and the $F(n)$ from the paper with Erdős is $F_1(n)$.

It was not completely straightforward, but I did manage to show that the results for $F_1(n)$ do indeed generalize to each $F_j(n)$. Interestingly, Lenstra's case $j = 0$ was the most difficult.

LINES IN THE PRIME NUMBER GRAPH

Scott Duke Kominers
Harvard University, Cambridge, Massachusetts, USA
kominers@fas.harvard.edu

Rudi Mrazović
University of Zagreb, Zagreb, Croatia
Rudi.Mrazovic@math.hr

Carl Pomerance
Dartmouth College, Hanover, New Hampshire, USA
carlp@math.dartmouth.edu

Patrick Solé
I2M, (CNRS, Aix-Marseille University), Marseille, France
patrick.sole@telecom-paris.fr

Abstract

The prime number graph is the set of points (n, p_n) where p_n denotes the n^{th} prime. Let $L(n)$ be the minimum number of straight lines needed to cover the first n points in this set. Let $B(n)$ be the largest number of points (k, p_k) with $k \leq n$ covered by a single line. Recently Sloane conjectured that $L(n) = O(n/\log n)$. We prove a much stronger bound, as well as upper and lower estimates for $B(n)$. Our proofs use the Prime Number Theorem with remainder and are considerably improved with the assumption of the Riemann Hypothesis.

Photo Credit: Rose Lincoln

Kominers

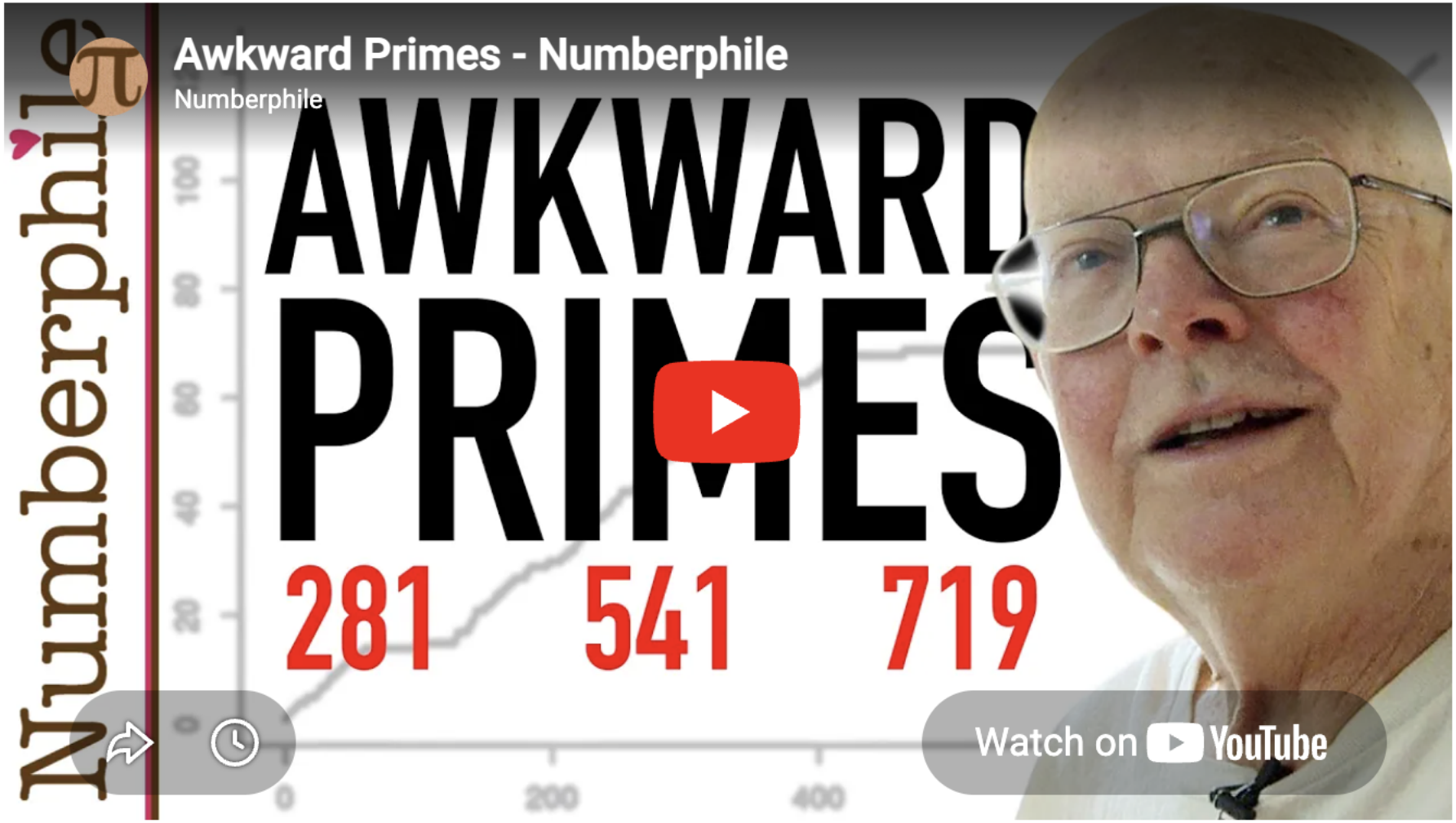
Mrazović

Solé

The paper was just posted to arXiv and is being submitted for publication.

Our project was inspired by a recent numberphile video, with Brady Haran interviewing Neil Sloane, the founder of OEIS.

One can graph the primes. With p_n the nth prime, plot the point (n, p_n). Let $L(n)$ be the fewest number of lines that contain all prime points (j, p_j) for $j \leq n$. Then Neil Sloane says a prime p_n is **awkward** if it requires an extra line, that is, $L(n) > L(n-1)$.



OEIS founder Neil Sloane on lines of primes, awkward primes... and a 'party pooper prime'.

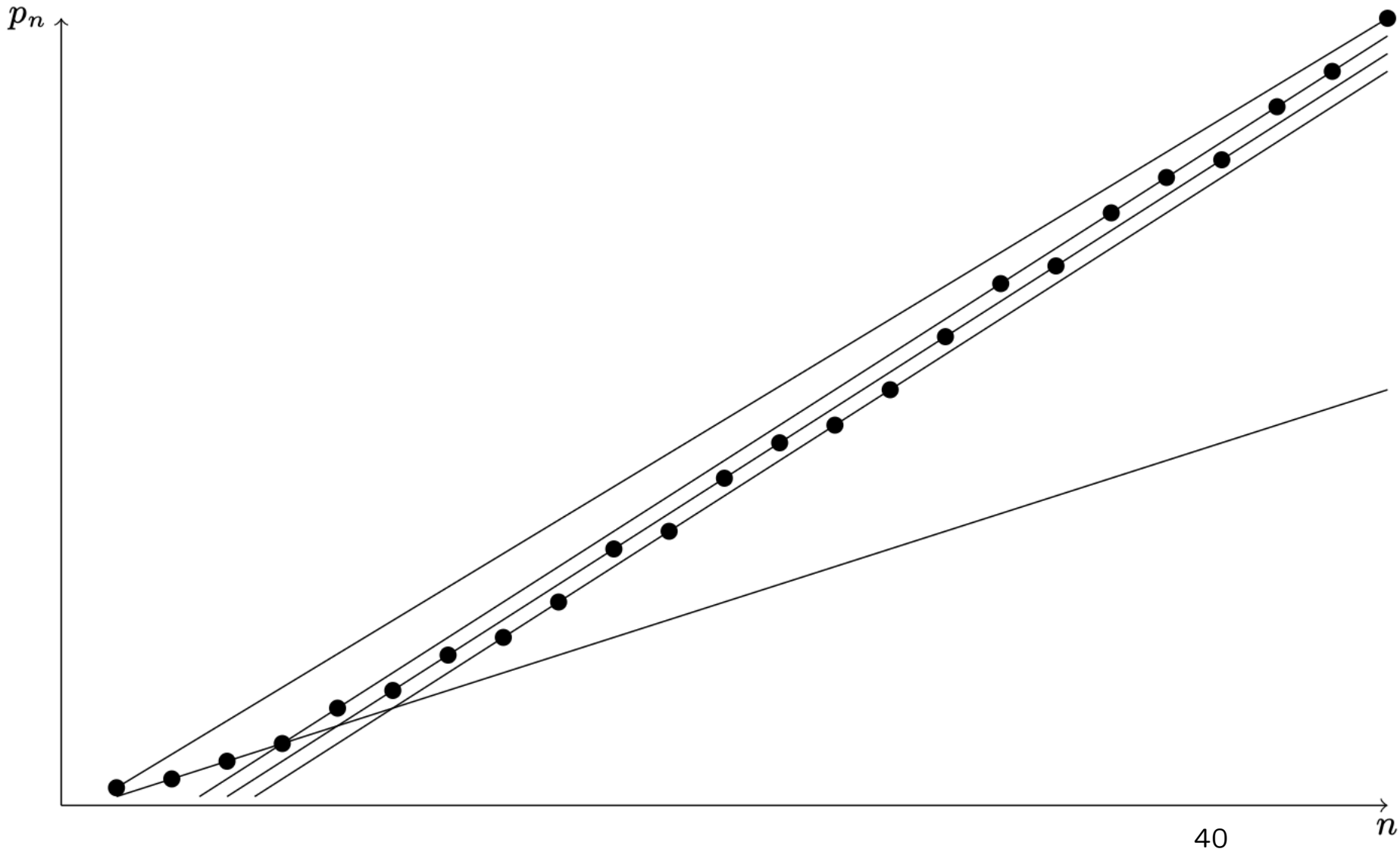


Figure 1: First 24 points of the prime number graph covered by $L(24) = 5$ lines.

Sloane conjectured that the number of awkward primes up to the nth prime is $O(n/\log n)$. We prove a much stronger result that implies the count is $O(n/\log^k n)$ for any fixed k, and is even smaller on assumption of the Riemann Hypothesis.

Why should one want to graph the primes? Sloane did it just for fun, and for me, that's sufficient reason. However, the idea is not new with him.

MATHEMATICS OF COMPUTATION, VOLUME 33, NUMBER 145
JANUARY 1979, PAGES 399–408

The Prime Number Graph

By Carl Pomerance

Abstract. Let p_n denote the nth prime. The *prime number graph* is the set of lattice points (n, p_n), $n = 1, 2, \ldots$. We show that for every k there are k such points that are collinear. By considering the convex hull of the prime number graph, we show that there are infinitely many n such that $2p_n < p_{n-i} + p_{n+i}$ for all positive $i < n$. By a similar argument, we show that there are infinitely many n for which $p_n^2 > p_{n-i}p_{n+i}$ for all positive $i < n$, thus verifying a conjecture of Selfridge. We make some new conjectures.

I introduced the prime number graph 47 years ago to settle a problem of Erdős and Straus. We've come full circle!

Thank You!