Digits

Carl Pomerance

Dartmouth College (emeritus)

Arithmetic, Algebra, and Algorithms,

in honor of **Hendrik Lenstra**,

ICMS, 10–14 April, 2023

Hendrik and I first met at a 3-week conference in Kingston, Ontario about 44 years ago. Among some problems we discussed:

After **Euler** and **Dirichlet** we know that if $a \neq \square$, then the density of the set of odd primes p with $a^{(p-1)/2} \equiv 1 \pmod{p}$ is $\frac{1}{2}$. (This is the *analytic* density—for natural density one uses the Prime Number Theorem for residue classes.)

Note that $p-1$ is the exponent of the group $(\mathbf{Z}/p\mathbf{Z})^\times$, and so this generalizes to Carmichael's function $\lambda(n)$ for $(\mathbf{Z}/n\mathbf{Z})^\times$. So, what can be said about the set of positive integers $n > 2$ coprime to a with $a^{\lambda(n)/2} \equiv 1 \pmod{n}$?

With a fixed, find the density of those n coprime to a with $a^{\lambda(n)/2} \equiv 1 \pmod{n}$.

Perhaps you'd think that the density should be $\frac{1}{2}\varphi(a)/a$. Instead, we came up with a heuristic that for most values of a the density of the set of such n does *not* exist. (Though in some easily proved cases one has the density at $\varphi(a)/a$.)

Suppose n is odd. Then $v_2(\lambda(n)) = \max\{v_2(p-1) : p \mid n\}$. If m is the multiplicative order of $a \mod n$, then $v_2(m) = v_2(\lambda(n))$ if and only if $(a/p) = -1$ for some prime $p \mid n$ with $v_2(p-1) = v_2(\lambda(n))$.

So the issue boils down to whether $\max\{v_2(p-1) : p \mid n\}$ occurs for a unique prime $p \mid n$, two primes, three primes, etc.

This situation can be modeled by a simple game, and the probability depends on how close the number of distinct primes dividing n is to a power of 2. Since the number of primes dividing n is usually close to $\log\log n$, as n goes to infinity one sees different behaviors, and so the oscillation.

Shuguang Li and I later used these thoughts to show that an analogue of Artin's conjecture (what is the distribution of n such that the order of a fixed $a \pmod n$ is $\lambda(n)$?) has oscillations.

It's pleasant to recall these things, but I'm not going to talk further about them.

As we know, Hendrik is famous for his algorithms.

Algorithmic records held by Hendrik:

1. The fastest practical smoothness test for an individual number as well as the fastest factoring method for most "hard" numbers (namely, the Elliptic Curve Factoring Method).

2. The fastest rigorous smoothness test for an individual number (namely, the Hyperelliptic Curve Factoring Method, with **Jonathan Pila** and me, inspired by work of **Len Adleman** and **Ming-Deh Huang**).

3. The fastest deterministic factoring method for primitive polynomials in $\mathbf{Z}[x]$ (with **Arjen Lenstra** and **Laci Lovász**).

4. The fastest practical integer factoring algorithm (the General Number Field Sieve, with **Joe Buhler** and me, inspired by an idea of **John Pollard**, and augmented by ideas of **Len Adleman**, **Jean-Marc Couveignes**, and others).

5. The fastest rigorous integer factoring method (the Class Groups Method, with me, after work of **Martin Seysen** and **Arjen Lenstra**).

6. The fastest deterministic primality test (the Gaussian Periods Test, with me, after work of **Manindra Agrawal**, **Neeraj Kayal**, and **Nitin Saxena**).

I'm sure I must have left out some other records!

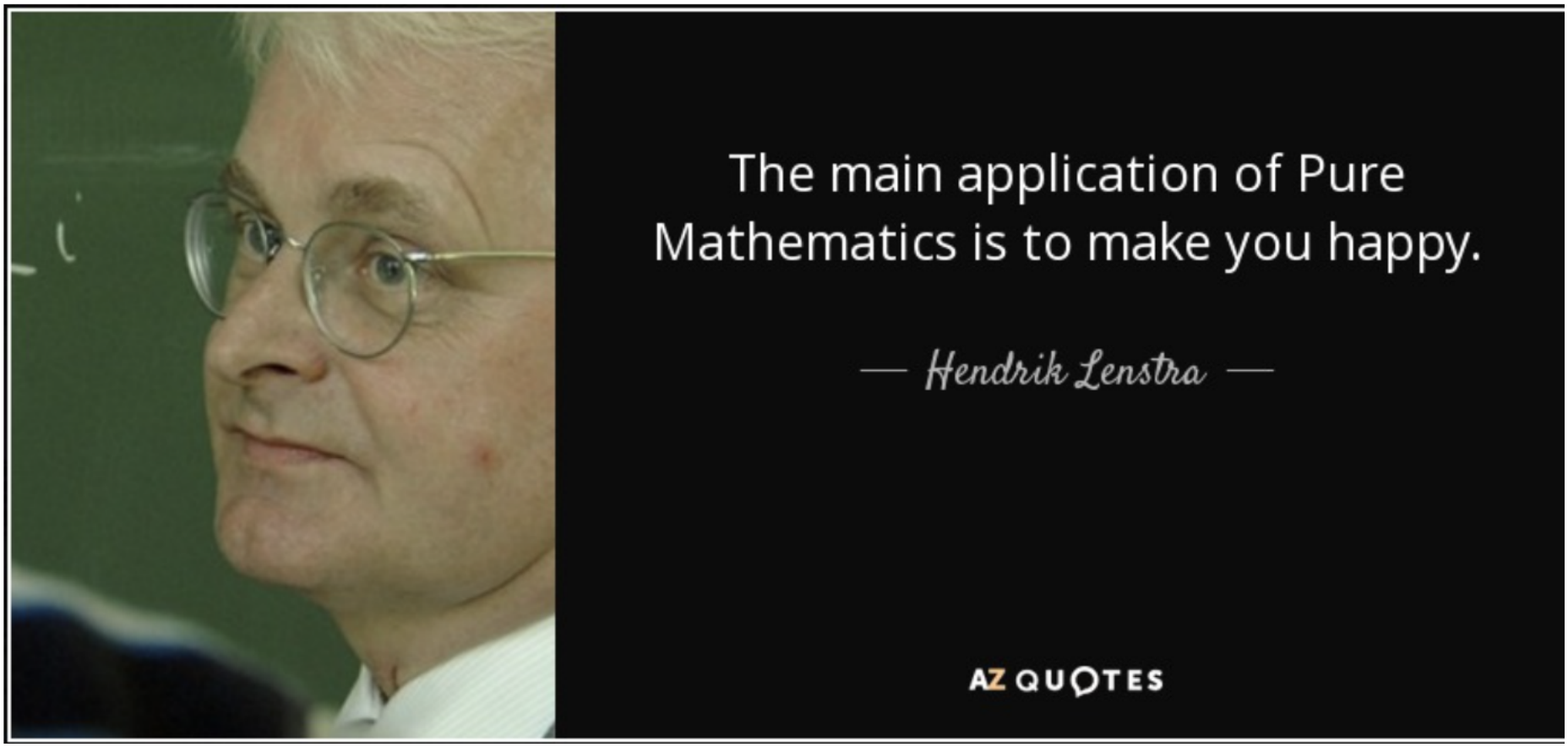
For more on the history of modern factoring methods, see "General purpose integer factoring" by **Arjen Lenstra**. For more on the improvement of the AKS primality test, see our paper, the survey of **Andrew Granville**, or my book with **Richard Crandall**.

In thinking of what I could talk about at this conference, I have sketched out above a couple of possible paths.

Instead, I'm talking about digits.

I'm probably setting a poor example for all of the younger people here, but in my dotage, I've been working more and more on fun problems.

And what's more fun than problems about digits?


The main application of Pure Mathematics is to make you happy.
— Hendrik Lenstra —
AZ QUOTES

Synopsis:

1. On an interesting property of ...
2. Niven numbers
3. Benford's law
4. The "105 problem"
5. Digitally delicate primes
6. Primes with missing digits
7. The Sheldon conjecture

One of my first papers:

ON AN INTERESTING PROPERTY OF 112359550561797752809

J. L. HUNSUCKER and CARL POMERANCE
University of Georgia, Athens, Georgia 30602

This appeared in the Fibonacci Quarterly in 1975. The "interesting" property: If you multiply it by 99 it is the same as appending the digit 1 to the beginning and to the end. It is the least number with this property, and finding it had been posed as a problem by **J. A. Hunter** in the Journal of Recreational Mathematics.

Hunsucker and I showed a connection to the Fibonacci numbers and we raised the issue of the set of bases b for which the analogous property holds for some n. That is, given a base b, is there an n such that if n is multiplied by $b^2 - 1$, then this is the same as appending a 1 to the beginning and to the end of n. We showed that such bases b have asymptotic density 0, and there are infinitely many such bases assuming that $x^2 - x - 1$ assumes a prime value (for $x \equiv 3 \pmod 4$) infinitely often.

I was present for the birth of "Niven numbers" in 1977. **Erdős** was at a small conference at Miami University of Ohio and he persuaded the organizers to have me come and join him for a few days. The conference was low key, mostly with educational themes. Also speaking was **Ivan Niven**, who gave a talk featuring a ridiculously easy problem that he saw in the Sunday comics of his newspaper:

Find a number between 10 and 20 divisible by the sum of its digits.

He went on to say that a mathematician would generalize this by asking for the distribution of numbers divisible by the sum of their digits or perhaps also generalizing to other bases.

I felt sure I could prove these "Niven numbers" have density 0, but I couldn't. And remarkably, neither could Erdős. Also attending the meeting was **Curtis Cooper** from Central Missouri State U. and he and his colleague **Robert Kennedy** wrote several papers on the topic. A few years later I ran into them at an AMS meeting at the University of Texas, and there a very easy proof occurred to me.

Let $s(n)$ be the sum of the digits of n. One can look at how this is distributed when the numbers n have k digits, k large. The average digit is 4.5, so by the central limit theorem, $s(n)$ is usually very close to $4.5k$. So, ignoring the density 0 set of those n where $s(n)$ is not between $(4.5-\epsilon)k$ and $(4.5+\epsilon)k$, we can focus on just those n divisible by some number in this interval, whether it is $s(n)$ or not. The number of such n's is $O(\epsilon 10^k)$. QED

I sketched out a proof for them, and then they published my proof, thanking me!

That's okay, the real problem was to find an asymptotic formula for the number of Niven numbers up to to x. And I later did this in a joint paper with **Mauduit** and **Sárközy**. We found out late in the game that another trio had similar results, but with slightly weaker error bounds: **De Koninck**, **Doyon**, and **Kátai**.

My former student **Paul Pollack** and collaborators have recently been looking at how statistical properties of leading digits fall out with familiar arithmetic functions. A statistical anomaly, known as Benford's law, asserts that the leading digits of numbers in a data set, like populations of counties, etc., are not uniformly distributed, with "1" appearing most frequently, followed by "2", etc. In fact it is the fractional part of the (base 10) logarithm that is uniform, so "1" appears with proportion $\log 2/\log 10 \approx 0.301$, etc.

With φ Euler's function, do the leading digits of the numbers $\varphi(n)$ follow Benford's law? The answer is no. But for the closely related function $\lambda(n)$ the answer is, unexpectedly, yes.

The "105 problem" of **Ron Graham**:

Prove there are infinitely many integers n such that $\binom{2n}{n}$ is coprime to 105.

Note that this condition is equivalent to n having 3 properties:

1. In base 3, n has only digits 0 and 1.
2. In base 5, n has only digits 0, 1, and 2.
3. In base 7, n has only digits 0, 1, 2, and 3.

Based on the three conditions being "independent events", a heuristic implies there are infinitely many such n. Recently **Ernie Croot** reported on some possible ways to attack this problem (at the **Granville** birthday conference in 2022).

In the late 90s I was thinking of the covering conjecture of **Erdős**:

For each B is there a finite set of classes $a_i \pmod{m_i}$, where $B \le m_1 < m_2 < \cdots < m_k$ and the union of these residue classes is $\mathbb{Z}$?

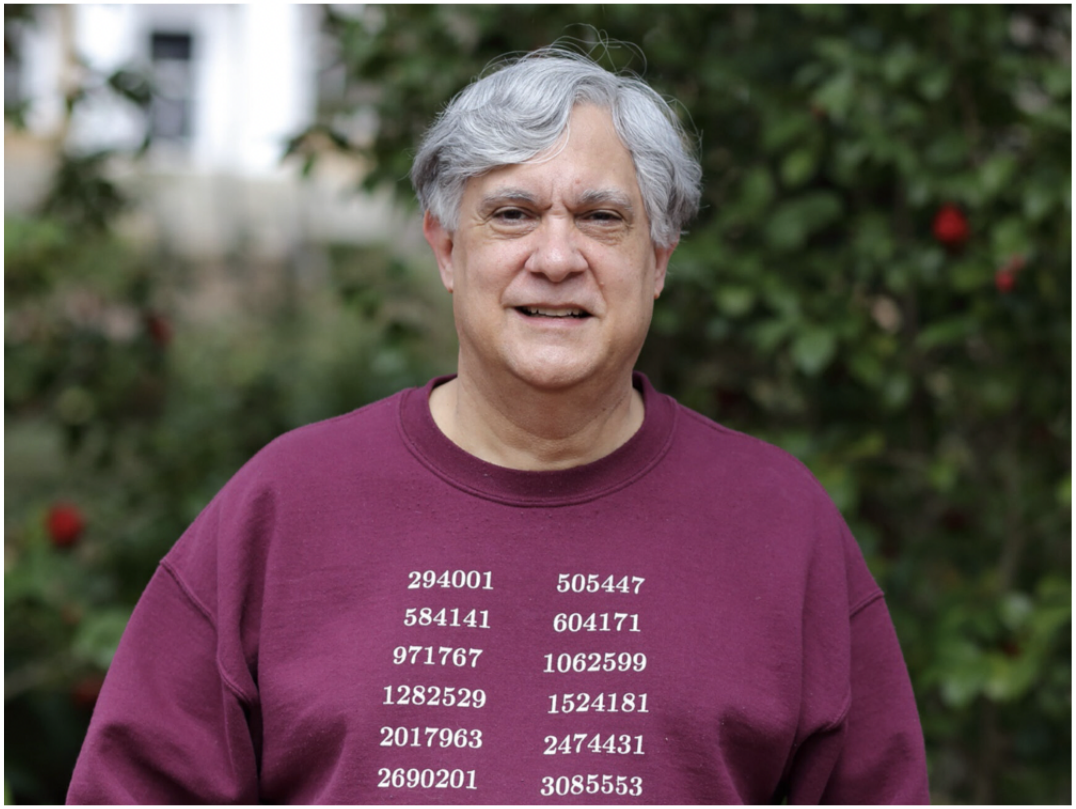
I wondered instead about choosing for the m_i's all of the integers m in $[B, 2B]$, asking what is the largest proportion of $\mathbb{Z}$ that can be removed. Would it be density 1/2, which would be the case if the m's are pairwise coprime (which they're not), or would it be $\log 2$, if the classes were completely disjoint (which they're not)? Or something in between?

I discussed this problem with my former student **Gang Yu**, who later took a job at U. South Carolina and he discussed the problem with **Michael Filaseta** and **Kevin Ford**. Later, **Sergei Konyagin** came on board, and the 5 of us proved, among other things, that the m's in $[B, 2B]$ behave like they are pairwise coprime.

We had a useful lemma in our paper that the referee pointed out to us was reminiscent of the **Lovász** Local Lemma in combinatorics. A few years later, **Robert Hough** used a generalization of this lemma to answer the **Erdős** problem in the negative: If B is sufficiently large, one cannot cover $\mathbb{Z}$ with a finite number of distinct moduli all at least B, one class per modulus.

Nevertheless, covering congruences proved useful in a digit problem connected with prime numbers.

Say a prime number p is "base-b digitally delicate" if changing any one of its base-b digits results in a composite number. Here are some examples in base 10:



Cohen and **Selfridge** proved (1975) that there are a positive proportion of digitally delicate primes in base 2, and **Sun** (2000) gave another proof. These articles were based on the paper where **Erdős** introduced covering congruences. **Erdős** himself (1979) proved there are infinitely many base-10 digitally delicate primes.

Tao proved (2012) that for any base, a positive proportion of the primes are digitally delicate.

One can actually view p as having infinitely many digits, with an infinite string of 0's as a preamble. So, say p is "widely digitally delicate" if changing any one of these infinitely many digits results in a composite number.

Filaseta and **Southwick** proved (2021) that a positive proportion of the primes are widely digitally delicate in base 10, and a few other bases. Yet no actual base-10 examples were known, until recently when **Jon Grantham** constructed one with over four thousand digits.

Last year, **Filaseta** and **Juillerat** showed in fact that there are arbitrarily long strings of consecutive primes that are base-10 widely digitally delicate.

An unsolved problem: Are there infinitely many primes that are NOT digitally delicate? Or even not widely digitally delicate?

Talking about digits of primes, must all large primes contain every digit? Clearly no in base 2 iff there are infinitely many Mersenne primes! What about base 10?

In 2019, **Maynard** showed that for any base-10 digit a, there are infinitely many primes that do not have a in their decimal expansion. In fact, he shows that among all integers up to x missing a, the chance one is prime is of magnitude $1/\log x$.

He very skillfully used the **Hardy–Littlewood** circle method and other tools to accomplish this. He also showed that for each k and sufficiently large bases b one can find the expected proportion of primes missing k pre-assigned base-b digits.

For a gentle survey, see **Granville**'s lecture at the JMM: www.ams.org/meetings/lectures/2023-Booklet-Master-EBOOK.pdf

This brings us to the sitcom "The Big Bang Theory". Here's some dialog from a show that first aired in 2010. (One can also watch this by googling "The alien parasite hypothesis", the name of the episode.)

Sheldon: What is the best number? By the way there's only one correct answer.

Raj: Five million, three hundred eighteen thousand, eight?

Sheldon: Wrong. **The best number is 73.** You're probably wondering why.

Leonard: No.

Howard: Uh-uh.

Raj: We're good.

Sheldon: **73 is the 21-st prime number. Its mirror, 37, is the 12-th, and its mirror, 21, is the product of multiplying, hang on to your hats, 7 and 3.** Eh? Eh? Did I lie?

Leonard: We get it. 73 is the Chuck Norris of numbers.

Sheldon: Chuck Norris wishes. In binary, 73 is a palindrome one zero zero one zero zero one, which backwards is one zero zero one zero zero one, exactly the same. All Chuck Norris backwards gets you is Sirron Kcuhc.

Figure 1. Sheldon always knew 73 was the best.
PHOTO CREDIT: Michael Yarish/©2019 Warner Bros. Entertainment Inc.

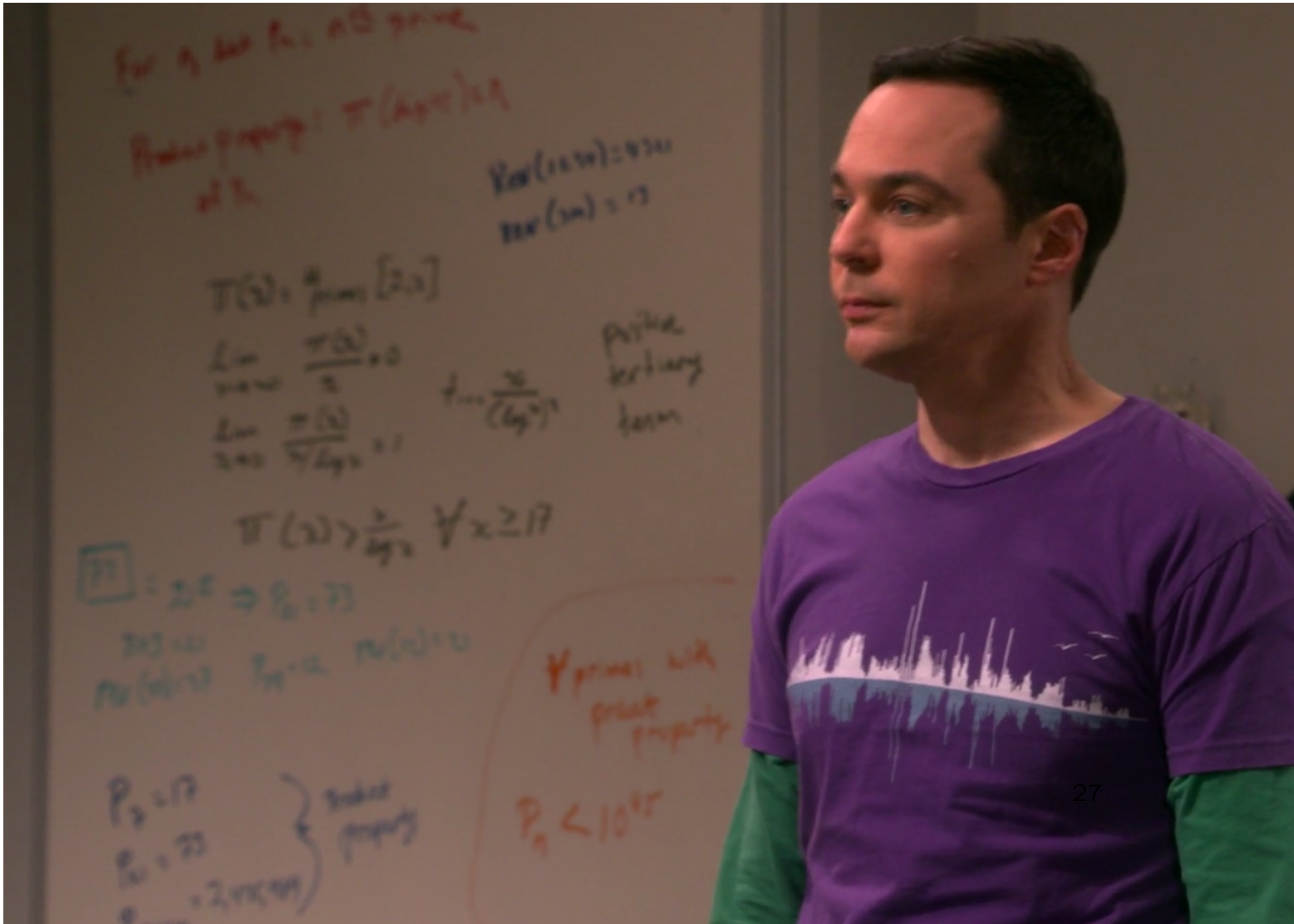
About 5 years ago, with **Chris Spicer**, we proved that 73 is indeed unique with the twin properties:

1. It is the nth prime p where n is the product of the digits of p. (The product property)

2. If one reverses the digits of p one gets the mth prime, where m is the reverse of n. (The mirror property)

Note that just the product property shows it's a finite problem, since if p has k digits, then $\pi(p)$ is of magnitude $10^k/k$, while the product of p's digits is $< 9^k$.

Further, the index n is 7-smooth, so comes from a much sparser set than the primes.



Thank you