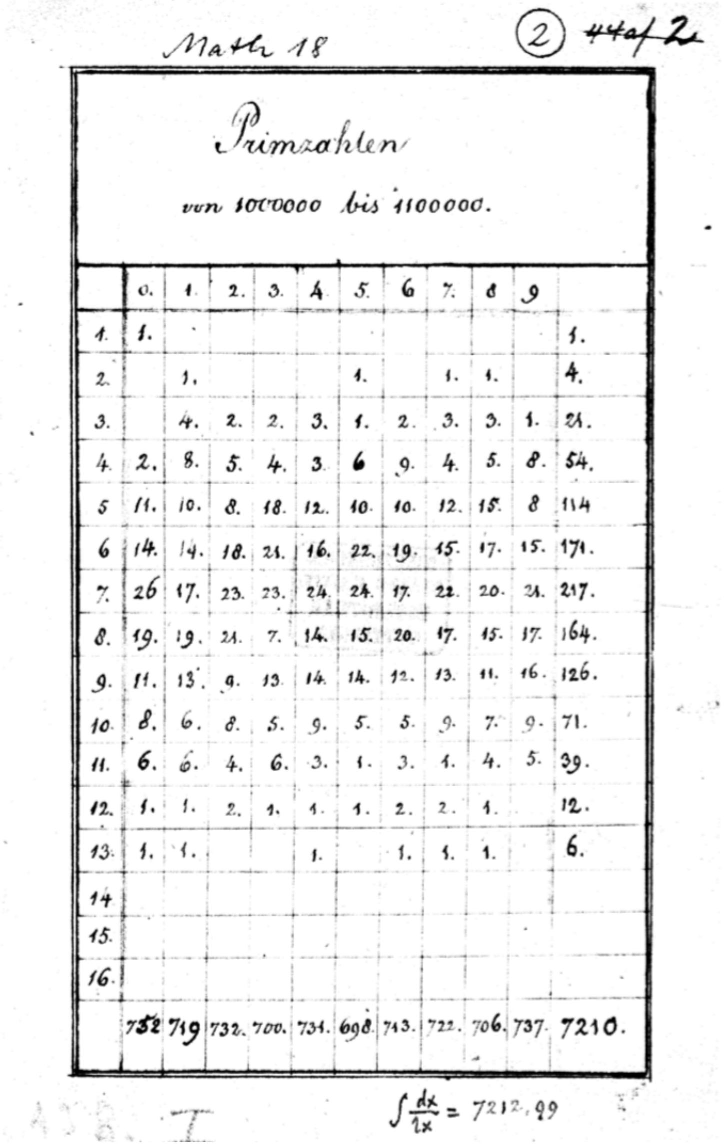
New York Number Theory Seminar
December 4, 2025

Is number theory a science?

Carl Pomerance

Dartmouth College



Math 18 ② ~~44a~~ 2

Primzahlen

von 1000000 bis 1100000.

	0.	1.	2.	3.	4	5.	6	7.	8	9	
1.	1.										1.
2.		1.				1.		1.	1.		4.
3.		4.	2.	2.	3.	1.	2.	3.	3.	1.	21.
4.	2.	8.	5.	4.	3.	6	9.	4.	5.	8.	54.
5	11.	10.	8.	18.	12.	10.	10.	12.	15.	8	114
6	14.	14.	18.	21.	16.	22.	19.	15.	17.	15.	171.
7.	26	17.	23.	23.	24.	24.	17.	22.	20.	21.	217.
8.	19.	19.	21.	7.	14.	15.	20.	17.	15.	17.	164.
9.	11.	13.	9.	13.	14.	14.	12.	13.	11.	16.	126.
10.	8.	6.	8.	5.	9.	5.	5.	9.	7.	9.	71.
11.	6.	6.	4.	6.	3.	1.	3.	1.	4.	5.	39.
12.	1.	1.	2.	1.	1.	1.	2.	2.	1.		12.
13.	1.	1.			1.		1.	1.	1.		6.
14											
15.											
16.											
	752	719	732.	700.	731.	698.	713.	722.	706.	737.	7210.

I

$\int \frac{dx}{lx} = 7212{,}99$

(Courtesy of Yuri Tschinkel and Brian Conrey)

Later in life, **Gauss** wrote that as a teenager he had investigated the distribution of primes, and he discovered that they tend to thin out as one gets to higher numbers according to the "law" $1/\log x$. That is, near x a random number is prime with probability $1/\log x$. And so, one would expect that the total number of primes in $[1, x]$ should be

$$\mathrm{li}(x) := \int_0^x \frac{\mathrm{d}t}{\log t}.$$

(The principal value is chosen for the singularity at $t = 1$, this makes little difference if one defines it instead as the integral from 2 to x.)

For example, **Staple** computed that

$$\pi(10^{26}) = 1{,}699{,}246{,}750{,}872{,}437{,}141{,}327{,}603,$$

while

$$\mathrm{li}(10^{26}) = 1{,}699{,}246{,}750{,}872{,}592{,}073{,}361{,}408. \ \ldots\ .$$

Gauss did not prove his "law", nor even the far weaker relation that

$$\pi(x) \sim x/\log x, \qquad x \to \infty$$

which would wait a century for a proof, and still has not been substantially improved in the next century plus.

Riemann though did come up with what might be a proof of the Gauss "law", but for one small detail! He proved that in the analytic continuation of

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

to the complex plane, IF the zeros with positive real part have real part $\frac{1}{2}$, THEN

$$\pi(x) = \mathrm{li}(x) + O\big(x^{1/2+o(1)}\big), \qquad x \to \infty.$$

In fact the converse holds. And, in fact, the **Riemann Hypothesis** is equivalent to the stronger and concrete inequality

$$|\pi(x) - \mathrm{li}(x)| < x^{1/2} \log x, \qquad x \geq 2.$$

Note too that if the label "prime" is assigned to each integer $n \geq 3$ with probability $1/\log n$, assuming independence in the assignment of labels, then with very high probability, the number of $n \leq x$ with a "prime" label is $\mathrm{li}(x) + O(x^{1/2+o(1)})$, which I assume that Gauss knew.

Going at the Riemann Hypothesis computationally, many people have checked to see if the zeros with positive real part have real part $\frac{1}{2}$, starting with Riemann himself, who found the first 3 zeros. **Alan Turing** worked on the problem, and many others. We now know after **Platt & Trudgian** that the first 1.2363×10^{13} zeros are on the $\frac{1}{2}$-line.

Now that we've dealt (!) with the **Riemann Hypothesis**, lets try our hand on the **twin prime conjecture**. The weak form of this conjecture merely asserts there are infinitely many pairs of primes that differ by 2. A still weaker form says that there is some fixed integer $g > 0$ which is a gap between two primes infinitely often, and this has actually been proved, by **Zhang**, with improvements by many others. So we now know that there is some $g \le 246$ which is a prime gap infinitely often. However, we do not know any specific g with this property!

But what is the strong form of the twin prime conjecture? Let $\pi_2(x)$ denote the number of primes $p \le x$ with $p + 2$ also prime.

One might be tempted to say that

$$\pi_2(x) \sim \int_2^{\infty} \frac{\mathrm{d}t}{(\log t)^2} \sim \frac{x}{(\log x)^2}$$

based on the thought that an integer n being prime and $n+2$ being prime are “independent” events.

However, this very same thought would lead one to conjecture that there are about $x/(\log x)^2$ primes $p \le x$ with $p+1$ prime, which is clearly nonsense. In fact, n and $n+2$ are not independent events for being prime. For example, if $n > 2$ is prime, then n is odd, and then $n+2$ must be odd as well, which implies that if n is prime, then $n+2$ has a better chance at being prime than a random number. For other small primes this goes the other way.

For example, if $n \neq 3$ is prime, then $n \equiv 1$ or 2 (mod 3), and we know asymptotically these two choices are about equally likely. But then $n+2$ has about a 50% chance of being 0 (mod 3), instead of a $33\frac{1}{3}$% like a random number. Putting these thoughts together we come up with the strong form of the twin prime conjecture:

Let $c = 2\prod_{p} \dfrac{1 - 1/(p-1)}{1 - 1/p} = 1.320323631693739147855762422002\ldots,$

where the product is over odd primes p. Then

$$\pi_2(x) \approx c\int_2^x \frac{\mathrm{d}t}{(\log t)^2}, \quad x \text{ large.}$$

Let's check it out:

$$\pi_2(10^{18}) = 808{,}675{,}888{,}577{,}436,$$

$$c\int_2^x \frac{\mathrm{d}t}{(\log t)^2} = 808{,}675{,}901{,}493{,}607.4\ldots$$

The count to 10^{18} was by **Oliveira e Silva** in 2016.

Well it's not exactly proved, but it seems about as certain as any physical law.

Do we ever have to revise our understanding? Note that the "fudge factor" c in the twin prime conjecture was already formulated by **Hardy & Littlewood** and the need for something like that (**Sylvester**, in the context of Goldbach's conjecture) was known before.

Take the issue of primes in short intervals. It was widely believed that if $\theta > 2$ is a constant, then the number of primes in the interval $(x, x + (\log x)^\theta)$ is $\sim (\log x)^{\theta-1}$. This is supported strongly by the Cramér model (the same model we've been using, where n is labeled "prime" with probability $1/\log n$).

It then came as a complete surprise when **Helmut Maier** *disproved* this conjecture! There is a constant $\delta > 0$ (depending on θ) such that the interval infinitely often has more than $(1 + \delta)(\log x)^{\theta - 1}$ primes, and infinitely often has fewer than $(1 - \delta)(\log x)^{\theta - 1}$ primes.

How did he do this? He showed that small primes occasionally can interact in a way to have slightly more multiples in these short intervals than expected, and sometimes they gang up to have fewer hits in these intervals. (The small primes play a role as we've seen with twin primes, but there it's not a case of ganging up, they have a very steady effect.)

Note that he did not prove that the interval $(x, x + (\log x)^\theta)$, $\theta > 2$, always has primes for x large, rather it was a sequence of special x's that he uncovered.

This reasoning also led **Andrew Granville** to revise another Cramér conjecture. It was thought that if $g(x)$ is the largest gap between consecutive primes $\leq x$, then $\limsup g(x)/(\log x)^2 = 1$. Granville conjectures instead that $\limsup g(x)/(\log x)^2 = 2e^{-\gamma} > 1$. His heuristic for this parallels the Maier proof, showing again that small primes can sometimes conspire to sieve out a little more than you first might think.

The numerical evidence here is weak, champion prime gaps are few and far between.

We are all familiar with the fact that **Andrew Wiles** has proved the famous Fermat Conjecture about n-th powers. Why was it a conjecture? Do you think that everyone realized that elliptic curves are modular, and therefore the Fermat Conjecture holds?

Certainly not. In fact there is an elementary heuristic that sort of supports the conjecture, and this was published by **Erdős & Ulam**. Consider the set S of powers a^n where a, n are positive integers and $n \ge 4$. The number of members of S in $[1, x]$ is $O(x^{1/4})$. Now consider the set S_2 comprised of sums of 2 members of S. The number of members of S_2 in $[x/2, x]$ is $O(x^{1/2})$. Now a random number in $[x/2, x]$ is in S with probability $O(1/x^{3/4})$. So the expected number of members of $S_2 \cap [x/2, x]$ that are in S is $O(1/x^{1/4})$. Now let x vary over the powers of 2, so we see that we expect only finitely many solutions to $s_1 + s_2 = s_3$, with $s_1, s_2, s_3 \in S$. Since no small examples exist, it's likely there are none.

There are a couple of things wrong with this argument. For example, for $n \geq 4$, we have $2^n \in S$ and $2^n + 2^n = 2^{n+1} \in S$. So, there are infinitely many solutions to $s_1 + s_2 = s_3$. We patch this by requiring that in S_2, the two powers that we add together are coprime.

There is a second thing wrong. It doesn't work for third powers! In fact, the argument suggests that there are infinitely many solutions to $a^3 + b^3 = c^3$. OK, that case is ruled out by other arguments, in fact, rigorous arguments that go back centuries.

So, that is the "science" behind the Fermat Conjecture. A similar, but more involved argument can be brought to bear on the a, b, c conjecture. This may have been proved by **Mochizuki**, but many of those who have tried to understand his argument are not persuaded.

Next up, factoring algorithms.

Here we are concerned with discovering a nontrivial factorization for a composite number. The subject has a venerable history, and now in the computer age, we can attack numbers with hundreds of digits. Here are some of the various algorithms used:

Trial division,
The ρ method,
The $p-1$ method,
The elliptic curve method,
The quadratic sieve,
The number field sieve.

The first, and slowest, on this list is rigorous. All the others are heuristic.

From “A tale of two sieves” (Notices AMS, 1996):

Factoring big numbers is a strange kind of mathematics that closely resembles the experimental sciences, where nature has the last and definitive word. If some method to factor n runs for a while and ends with the statement “d is a factor of n”, then this assertion may be easily checked; that is, the integers have the last and definitive word. One can thus get by quite nicely without proving a theorem that a method works in general. But, as with the experimental sciences, both rigorous and heuristic analyses can be valuable in understanding the subject and moving it forward.

One of the oldest problems: **perfect numbers**.

A number n is perfect if $s(n)$, the sum of the divisors of n that are less than n, is n itself.

Euclid: If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect. For example, $p = 2, 3, 5, 7$ all work.

Euler: Every even perfect number is given by Euclid's formula.

Unsolved: Are there infinitely many even perfect numbers? Are there any odd perfect numbers?

Let's turn our scientific minds to these questions.

Due to the Euclid–Euler theorem, the first question is equivalent to: Are there infinitely many Mersenne primes, i.e. primes of the form $2^p - 1$?

It is easy to see that if $2^p - 1$ is prime, then p must be prime too. But this is not sufficient, for example, $2^{11} - 1 = 23 \cdot 89$. We also know that if p is prime, then all prime factors of $2^p - 1$ must be 1 (mod p), and so $> 2p$. The probability that a random number n is prime given that n has all prime factors $> \log n$ is

$$\frac{1}{\log n} \prod_{q \le \log n} \left(1 - \frac{1}{q}\right)^{-1} \sim \frac{e^\gamma \log\log n}{\log n} \sim \frac{e^\gamma}{\log 2} \frac{\log p}{p},$$

when $n = 2^p - 1$. so we might expect the number of Mersenne prime exponents $p \le x$ is $\sim c \log x$, where $c = e^\gamma / \log 2 \approx 2.56954$.

The heuristic that the number of Mersenne exponents $p \le x$ is $\sim c \log x$ is roughly reflected in the available data. However, these exponents are quite sparsely distributed, with only 51 of them known up to 10^8, so we would not expect a very tight fit. For $x = 10^8$, the formula gives 47.3.

It is widely believed that there are no odd perfect numbers. Do we agree? Euler proved that if n is an odd and $s(n)$ is also odd, then n is of the form $p^j m^2$, where $p \nmid m$, p is prime, and $p \equiv j \equiv 1 \pmod 4$. Let $\sigma(n) = s(n) + n$, the sum of all of n's positive divisors. Simplifying a little, by Euler, an odd perfect number n is of the form pm^2 where $p \mid \sigma(m^2)$.

Given m, the number of choices for p is $\leq \log m$. One might argue that the chance that $\sigma(n)$ is divisible by m^2 is $O(1/m^2)$, so noting that there are $\leq \log m$ values of n in play, the probability is $O(\log(m)/m^2)$. Summing, this converges, so we expect only finitely many odd perfect numbers, and no large ones. Well, we've already checked up to fairly high bounds, so there you have it, no odd perfect numbers.

Someone once objected to this "argument" saying that even perfect numbers >6 are also of the form pm^2 with $p \mid \sigma(m^2)$, and we believe there are infinitely many of these. However, with even perfect numbers, we in fact have $p = \sigma(m^2)$. We can look at this possibility for odd perfect numbers. In fact, we know that odd perfect numbers, if any exist, have many different prime factors, at least 8. Then, using that σ is multiplicative, we cannot have $\sigma(m^2)$ prime. So, this case does not exist for odd perfect numbers.

In 1932, **Lehmer** asked if there are any composite numbers n with $\varphi(n) \mid n-1$, where φ is Euler's function. He proved that any such n is odd, squarefree, and has at least 7 prime factors. Reading this paper carefully, I do not believe he actually conjectured that there are no such composite numbers n, though this assertion is popularly known as Lehmer's conjecture. Nevertheless, Lehmer remarked that the problem has a similar flavor as the existence of odd perfect numbers.

Here, putting on my science hat, I actually think there are infinitely many examples, and I think I know why none have been found so far. First, one might argue that the chance that n is in the residue class 1 (mod $\varphi(n)$) is $1/\varphi(n)$. This is totally false in the case that n is an odd prime, since the "chance" is 1. But we're dealing with composites.

Just like with perfects, candidates n have some special properties. We have already seen that they are odd and squarefree. But more seriously, they have the property that $\gcd(n, \varphi(n)) = 1$, and Erdős has proved that this places n in a set of density 0. In fact, the number of such $n \le x$ is $\sim x/(e^\gamma \log\log\log x)$. Well

$$\sum_n \frac{1}{e^\gamma \varphi(n) \log\log\log n}$$

diverges, so there should be infinitely many examples, perhaps as many as $\log x/\log\log\log x$ of them in $[1, x]$.

So, why haven't we found any? Various elementary arguments plus some computing has shown that any example has at least 15 prime factors and is $> 10^{30}$. So, a casual search is not likely to succeed.

McNew & Wright (2016) have studied composites n with $\varphi(n) \mid (n-1)^k$, calling such examples k-Lehmer numbers. Here some 2-Lehmer numbers are known, conjecturally infinitely many. They prove that for each $k \geq 3$ there are infinitely many k-Lehmer numbers that are not $(k+1)$-Lehmer numbers.

The **Birch & Swinnerton-Dyer** conjecture is also amenable to scientific thinking, but let us leave that for another time.

For now, lets close out with an elementary problem of **Erdős & Straus**. Their conjecture: For every integer $n > 1$ there are positive integers x, y, z with

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

This has been verified up to 10^{18} (**Mihnea & Dumitru**).

This seems like a strange conjecture to make, what is the context? There is a whole cottage industry of so-called Egyptian fractions. According to the Rhind papyrus (ca. 1550 BCE), the Egyptian civilization liked to write fractions as sums of unit fractions.

Now of course $\frac{4}{n}$ can be written as a sum of 4 unit fractions, but can it be done with 3? (Note that it can be shown that $\frac{3}{n}$ is not the sum of 2 unit fractions infinitely often.)

Erdős and Straus had much more modest numerical verification, so why would they make this conjecture about $\frac{4}{n}$? Well, many numbers n can be dealt with almost immediately. For example, say $n \equiv 3 \pmod 4$, so $n = 4k - 1$ for some $k \geq 1$. Then

$$\frac{4}{n} = \frac{4}{4k-1} = \frac{1}{k} + \frac{1}{k(4k-1)},$$

so in fact, only 2 unit fractions are used (and using $\frac{1}{j} = \frac{1}{2j} + \frac{1}{2j}$, one can stretch to 3 terms). An immediate corollary is that if n cannot be written as a sum of two squares, then the Erdős–Straus conjecture holds for n.

Proof. If n cannot be written as a sum of 2 squares, then it must be divisible by a prime $p \equiv 3 \pmod 4$, say $n = kp$. We've seen that $4/p$ is the sum of 3 unit fractions, so dividing the equation through by k we get that $4/n$ is the sum of 3 unit fractions. □

Another quick proof shows that if $n+1$ is not the sum of 2 squares, then $4/n$ is representable, so any counterexamples must have both n and $n+1$ the sum of two squares.

Corollary. The set of n for which the Erdős–Straus conjecture holds has asymptotic density 1. In fact, the number of exceptions $\le x$ is $O(x/\log x)$.

In fact there are many more congruences in which n might lie and which force $\frac{4}{n}$ to be a sum of 3 unit fractions.

Mordell discusses the problem and in his book he shows that $\frac{4}{p}$ is a sum of 3 unit fractions for all primes p except perhaps for those $p \equiv 1,\ 11^2,\ 13^2,\ 17^2,\ 19^2,$ or $23^2 \pmod{840}$.

An elementary argument shows that for each prime $q \equiv 3 \pmod 4$, the number of residues mod q for which the conjecture holds is at least the greatest integer at most

$$\frac{1}{2} \sum_{d|(q+1)/4} |\mu(d)| \tau\Big(\frac{q+1}{4d}\Big),$$

where τ counts the number of divisors.

If these residue classes were random, the fact that there are so many makes it highly likely that all sufficiently large n would be captured.

In a recent paper just posted to arXiv, **Andreas Weingartner** and I look at a generalization of the Erdős–Straus conjecture. **Andrzej Schinzel** conjectured that for $m \ge 4$ and for $n \ge N_m$, the fraction $\frac{m}{n}$ is the sum of 3 unit fractions. We show there are farily large exceptional values of n, thus showing that if N_m exists it must be fairly large. In fact, we show that for most primes p near $e^{m^{1/3}}$, we have $\frac{m}{p}$ not the sum of 3 unit fractions, but for most primes p near $e^{m^{1/2}}$ and larger, $\frac{m}{p}$ is the sum of 3 unit fractions. Arguing probabilistically, we think the transition occurs near the larger expression $e^{m^{1/2}}$.

So, is number theory a science?

I believe it is often helpful to think this way. After all, proof is hard! While we wait for AI to prove our conjectures, at least we can have some fun.

Thank you