Counting in number theory
Lecture 1: Elementary number theory

Carl Pomerance, Dartmouth College

Rademacher Lectures, University of Pennsylvania
September, 2010

Historically, number theorists have been interested in numbers with special properties.

Examples dating back to Euclid include the prime numbers and perfect numbers.

(A perfect number is the sum of its proper divisors; for example $6 = 1 + 2 + 3$.)

Euclid teaching

Euclid: *There are infinitely many primes.*

Euclid: *The following formula produces perfect numbers:*

$$2^{n-1}(2^n - 1), \ \textit{when } 2^n - 1 \textit{ is prime.}$$

For example, $2^n - 1$ is prime for $n = 2, 3, 5$, and 7, so we have the perfect numbers

$6 = 2(2^2{-}1)$, $28 = 2^2(2^3{-}1)$, $496 = 2^4(2^5{-}1)$, $8128 = 2^6(2^7{-}1)$.

Two obvious questions:

- Are all perfect numbers given by the formula of Euclid?
- Are there infinitely many perfect numbers?

On the first question, all we know is the theorem of Euler that all *even* perfect numbers are given by Euclid's formula. It is conjectured there are no odd perfect numbers, and we know some stringent conditions that imply you will not casually discover one.

On the second question, it is conjectured that Euclid's formula gives infinitely many perfect numbers.

Leonhard Euler

Presumably Euclid already knew that if $2^n - 1$ is prime, then n is prime, and that this condition is not sufficient:

$$2^{11} - 1 = 23 \times 89.$$

We now refer to primes $2^n - 1$ as Mersenne primes after a 17th century monk who had an incorrect conjecture about them!

We know 47 examples of Mersenne primes, the largest being

$$2^{43112609} - 1.$$

TIME Magazine’s 29-th greatest invention of 2008.

A more contemporary way of looking at some of these ancient questions is to study them statistically.

For example, if there are infinitely many Mersenne primes, how do they grow?

We know of course that there are infinitely many primes, but how do *they* grow?

Karl Friedrich Gauss

Gauss, as a teenager, studied an extensive table of primes, and noticed they tend to thin out according to a fairly precise law: near x the proportion of numbers that are prime is about $1/\log x$ (natural log). Thus, if $\pi(x)$ is the number of primes in the interval $[1, x]$, then we should have

$$\pi(x) \approx \int_2^x \frac{dt}{\log t}.$$

Call this integral $\mathrm{li}(x)$.
But what is meant by that pesky symbol "$\approx$"?

One possibility: Gauss meant that

$$\pi(x)/\mathrm{li}(x) \to 1, \quad \text{as } x \to \infty.$$

Using L'Hôpital's rule, it is easy to see that

$$\frac{\mathrm{li}(x)}{x/\log x} \to 1, \quad \text{as } x \to \infty.$$

So,

$$\frac{\pi(x)}{\mathrm{li}(x)} \to 1 \quad \iff \quad \frac{\pi(x)}{x/\log x} \to 1.$$

Then why would Gauss use the more difficult function li(x)?

Probably because he meant the stronger assertion:

$$|\pi(x) - \mathrm{li}(x)| \quad \text{is much smaller than li}(x).$$

Let's check it out.

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

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

From computations of Gourdon, based on algorithms of Meissel, Lehmer, Lagarias, Miller, Odlyzko and more recently Deléglise, Rivat, Zimmermann:

$$\begin{aligned} \pi(10^{22}) &= 201{,}467{,}286{,}689{,}315{,}906{,}290 \\ \mathrm{li}(10^{22}) &= 201{,}467{,}286{,}691{,}248{,}261{,}498 \\ 10^{22}/\log(10^{22}) &= 197{,}406{,}582{,}683{,}296{,}285{,}296 \end{aligned}$$

In fact, the Riemann Hypothesis is equivalent to the assertion:

$$|\pi(x) - \mathrm{li}(x)| \le x^{1/2} \log x, \quad x \ge 3.$$

(I call this the calculus-class version of the RH.)

In case you're interested, here is the precalculus-class version of the RH:

Let $F(x)$ denote the natural logarithm of the least common multiple of the integers in $[1, x]$. Then, for all $x \geq 3$,

$$|F(x) - x| \leq x^{1/2}(\log x)^2.$$

We don't yet know the RH, but we do know the Prime Number Theorem:

Hadamard, de la Vallée-Poussin (1896) *As* $x \to \infty$, *we have* $\pi(x)/\text{li}(x) \to 1$.

The RH implies that $\pi(x) = \text{li}(x) + O(x^{1/2+\epsilon})$ for each $\epsilon > 0$, but we don't even know if there is any positive fixed ϵ with $\pi(x) = \text{li}(x) + O(x^{1-\epsilon})$.

Jacques Hadamard

Charles-Jean de la Vallée-Poussin

Now let us turn our statistical eye on the other problem of Euclid, namely perfect numbers. Let $P(x)$ denote the number of perfect numbers in $[1, x]$. What can we say about $P(x)$?

Since it is not even known that there are infinitely many perfect numbers, getting a lower bound for $P(x)$ that tends to infinity seems fairly hopeless.

But what about an upper bound for $P(x)$?

And what might we conjecture for $P(x)$?

It seems natural to partition the perfect numbers into evens and odds, given the Euclid–Euler theorem that gives a formula for the even ones.

Let $P_0(x)$ denote the number of even perfects in $[1, x]$, and let $P_1(x)$ denote the number of odd perfects in $[1, x]$.

Since an even perfect number is of the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime (and so n is prime), it follows that

$$P_0(x) \le \pi(\log x) = O\left(\frac{\log x}{\log\log x}\right).$$

Experimentally and heuristically, $P_0(x)$ grows much smaller than $\log x/\log\log x$. Note that when n is prime, $2^n - 1$ has no prime factors below n. Note too that a random number m is prime with probability about $1/\log m$ and if m has no factors below $\log_2 m$, this probability is enhanced to $(c\log\log m)/\log m$ where $c = e^\gamma$ and γ is the Euler–Mascheroni constant. So, if $2^n - 1$ behaves like a "random" number of the same magnitude, it is prime with probability $(e^\gamma \log n)/(n\log 2)$. Summing this expression over prime numbers n with $2^{n-1}(2^n - 1) \le x$ then suggests that

$$\frac{P_0(x)}{(e^\gamma/\log 2)\log\log x} \to 1, \quad x \to \infty.$$

This roughly corresponds to reality in that even perfects seem to be growing at a rate proportional to $\log\log x$ and the constant is in the range 2.5 to 3.

We don't know any odd perfect numbers, and it is thought that there are none. In this case, $P_1(x)$ would be identically 0. Can we at least show that $P_1(x)$ is at most a small function of x? Here is a history of efforts:

Volkmann (1955) : $O(x^{5/6})$

Hornfeck (1955) : $O(x^{1/2})$

Kanold (1956) : $o(x^{1/2})$

Erdős (1956) : $O(x^{1/2-\delta})$ (some fixed $\delta > 0$)

Kanold (1957) : $O(x^{1/4+\epsilon})$ (every fixed $\epsilon > 0$)

Hornfeck & Wirsing (1957) : $O(x^{\epsilon})$

Wirsing (1959) : $x^{O(1/\log\log x)}$

Here's a proof of the second result: $P_1(x) = O(x^{1/2})$:

Let $\sigma(n)$ denote the sum of all of n's positive divisors, so n is perfect if and only if $\sigma(n) = 2n$. Using that σ is multiplicative it is easy to prove another result of Euler: *If n is an odd perfect number, then $n = p^k m^2$ where p is a prime that is $1 \pmod 4$ not dividing m and $k \equiv 1 \pmod 4$.*

Next, using that $n = p^k m^2$ is perfect,

$$2 = \frac{\sigma(n)}{n} = \frac{\sigma(p^k)}{p^k}\frac{\sigma(m^2)}{m^2},$$

so that in lowest terms, the fraction $2m^2/\sigma(m^2)$ has denominator a power of p. We conclude that m determines p and thus the odd perfect number n.

But if $n \le x$, then $m \le x^{1/2}$, so $P_1(x) \le x^{1/2}$.

Let's try our hand at some other difficult or intractable elementary problems, again from a statistical point of view:

- twin primes
- amicable and sociable numbers
- Carmichael numbers

The twin prime conjecture dates from 1849 or perhaps earlier. In that year, de Polignac published the more general conjecture that for each even number k there are infinitely many pairs of primes p, p' with $p' - p = k$. The twin prime conjecture is the special case $k = 2$.

Twin primes certainly appear fairly common. After 2, the first prime that is not part of a twin pair is 23, and in fact, up to 100, just 9 of the 25 primes are *not* part of a twin pair.

The problem remains unsolved, but short of proving there are infinitely many, what can we do?

First, we can ask why it is a conjecture, other than that there is numerical evidence.

If we take the probabilistic view that the proportion of numbers near x that are prime is about $1/\log x$, then the proportion of n near x where n and $n+2$ are both prime perhaps should be about $1/(\log x)^2$, and the number of such n below x should be about

$$\int_2^x \frac{dt}{(\log t)^2}.$$

However, there is a problem with this reasoning since n and $n+2$ being prime are not "indepependent events". For example, if $n > 2$ is prime, then $n+2$ is odd, so it should have an *enhanced* chance of being prime. Similarly, if $n > 3$ is prime it is either 1 or 2 (mod 3), these two events should be equally likely (yes, this is a theorem), and so $n+2$ is equally likely to be 0 or 1 (mod 3). That is, if n is prime, then the chance that $n+2$ is divisible by 3 is about 1/2, instead of 1/3 as with a random integer.

Working through this idea we come up with the revised possibility: The number of primes $n \le x$ with $n + 2$ prime is approximately

$$2c\int_2^x \frac{dt}{(\log t)^2}, \quad c = \prod_{p>2} \frac{1 - 1/(p-1)}{1 - 1/p} = 0.66016\ldots\ .$$

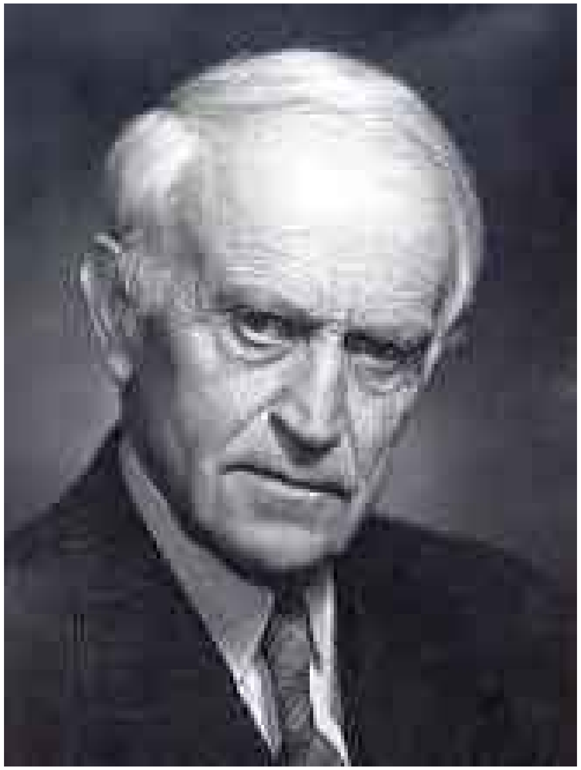
Let's check it out at $x = 2^{60}$ (from the website of Oliveira e Silva):

$$\begin{aligned} \text{Actual count}: &\ \ 925{,}800{,}651{,}712{,}810 \\ \text{Predicted count}: &\ \ 925{,}800{,}674{,}606{,}702. \end{aligned}$$

We do know that the order of magnitude of the prediction, $O(x/(\log x)^2)$, is correct as an upper bound. This was proved by Brun close to 100 years ago. From this result we know that actually twin primes thin out much faster than the primes do, in fact

$$\text{Euler}: \quad \sum_{p \text{ prime}} \frac{1}{p} = \infty$$

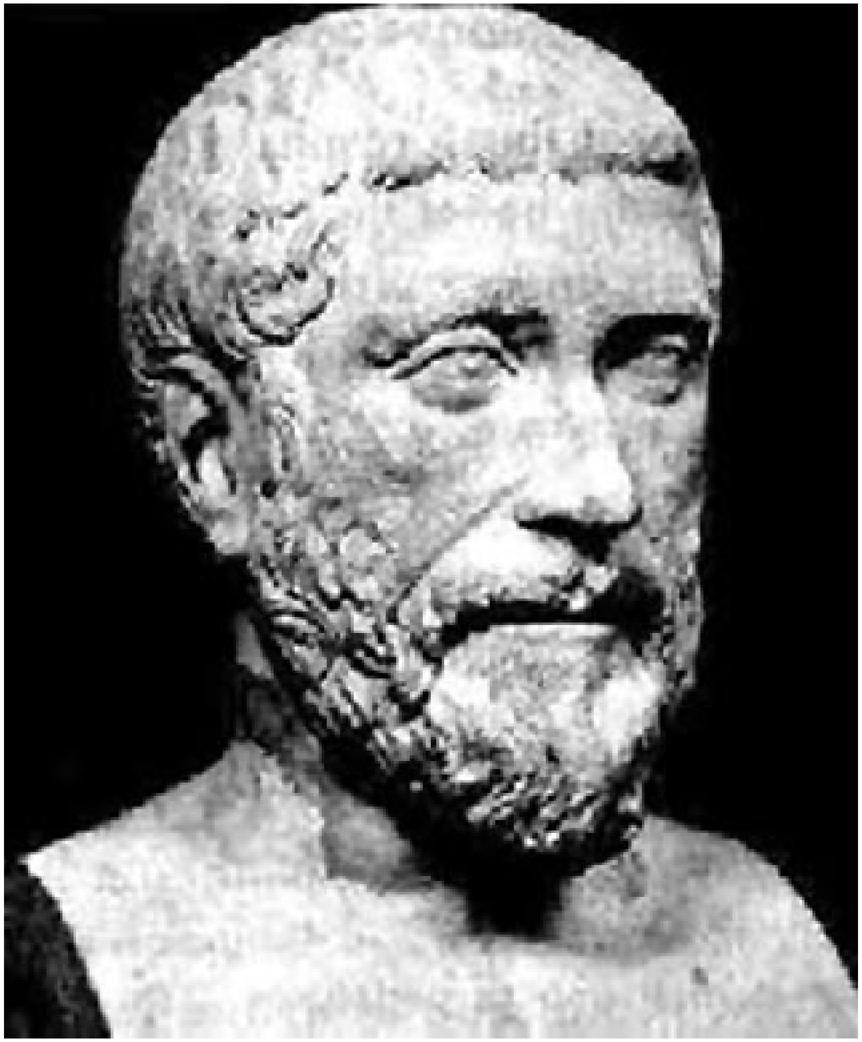
$$\text{Brun}: \quad \sum_{p,p+2 \text{ primes}} \left(\frac{1}{p} + \frac{1}{p+2}\right) = B < \infty.$$



Viggo Brun

It is difficult to compute Brun's constant B, the sum of the reciprocals of the twin primes. It is effective, in a theoretical sense, but not so much in a practical sense. Probably it is about 1.902, but all we know rigorously is that it is in the interval (1.83, 2.34), the lower bound coming from calculation with known twin primes, and the upper bound with a numerically explicit version of Brun's proof in the recent thesis of Klyve.

As for lower bounds, we know that there are infinitely many primes p such that either $p + 2$ is prime or $p + 2$ is the product of two primes (Chen). And we have the new sensational result of Goldston, Pintz, & Yıldırım that there are indeed infinitely many gaps between consecutive primes that are *much* smaller than the average gap.



Pythagoras

Let $s(n) = \sigma(n) - n$, the sum of n's divisors smaller than n.

The function $s(n)$ was considered by Pythagoras, about 2500 years ago.

Pythagoras: $s(220) = 284$, $s(284) = 220$.

If $s(n) = m$, $s(m) = n$, and $m \neq n$, we say n, m are an *amicable pair* and that they are *amicable* numbers.

In Genesis it is related that Jacob gave his brother Esau a lavish gift so as to win his friendship. The gift included 220 goats and 220 sheep.

Abraham Azulai, ca. 500 years ago:

“Our ancestor Jacob prepared his present in a wise way. This number 220 is a hidden secret, being one of a pair of numbers such that the parts of it are equal to the other one 284, and conversely. And Jacob had this in mind; this has been tried by the ancients in securing the love of kings and dignitaries.”

Ibn Khaldun, ca. 600 years ago in “Muqaddimah”:

“Persons who have concerned themselves with talismans affirm that the amicable numbers 220 and 284 have an influence to establish a union or close friendship between two individuals.”

Ibn Khaldun

Al-Majriti, ca. 1050 years ago reports in “Aim of the Wise” that he had put to the test the erotic effect of

“giving any one the smaller number 220 to eat, and himself eating the larger number 284.”

(This was a very early application of number theory, far predating public-key cryptography . . .)

Eugène Catalan

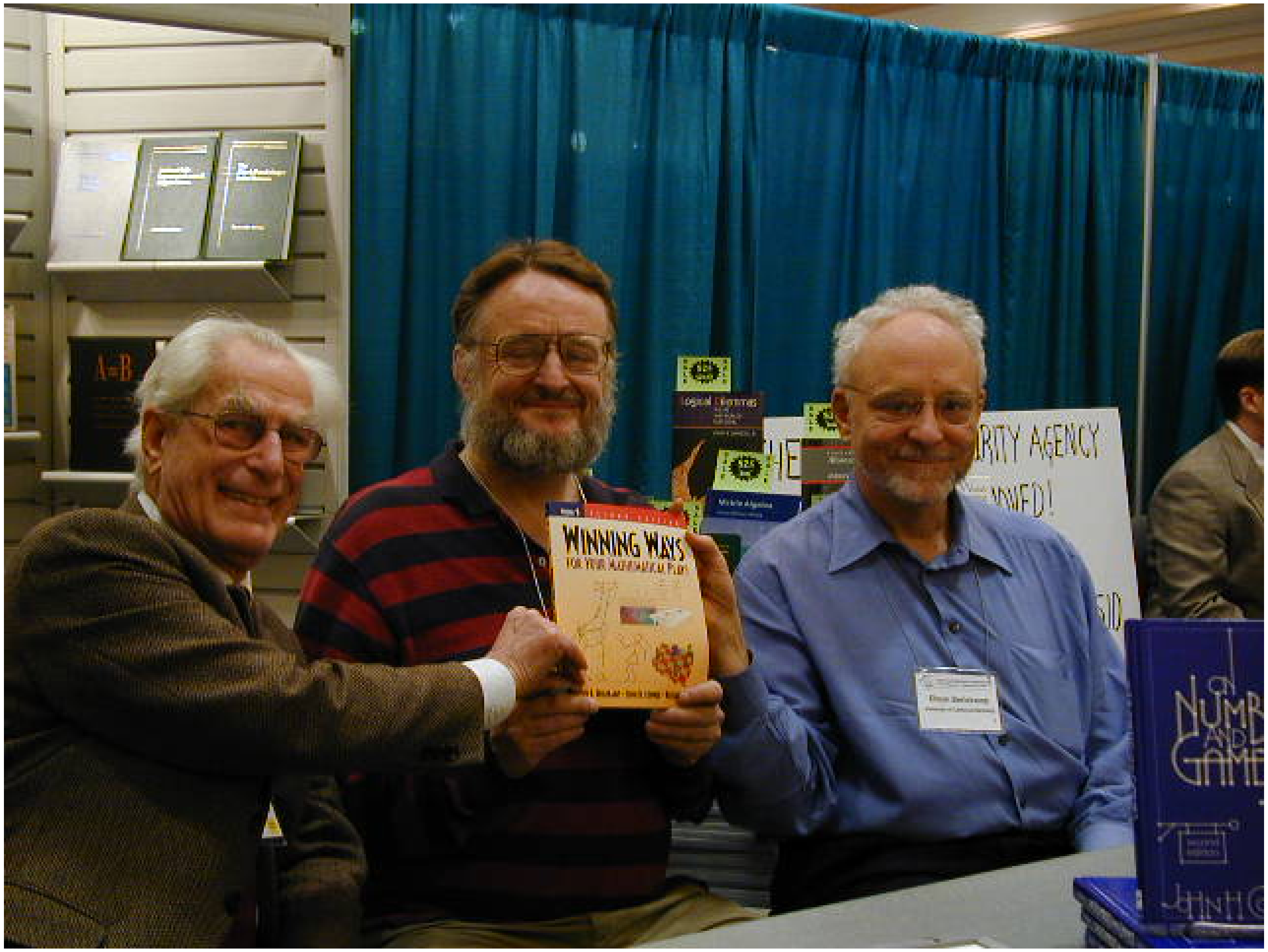
Leonard Dickson

In 1888, Catalan suggested that we iterate the function s and conjectured that one would always end at 0 or a perfect number. For example:

$$s(12) = 16, \;\; s(16) = 15, \;\; s(15) = 9, \;\; s(9) = 4, \;\; s(4) = 3, \;\; s(3) = 1,$$

and $s(1) = 0$. Perrott in 1889 pointed out that one might also land at an amicable number. In 1907, Meissner said there may well be cycles of length > 2. And in 1913, Dickson amended the conjecture to say that the sequence of s-iterates is always bounded.

Now known as the Catalan–Dickson conjecture, the least number n for which it is in doubt is 276. Guy and Selfridge have the counter-conjecture that in fact there are a positive proportion of numbers for which the sequence is unbounded.



Richard Guy, John Conway, & Elwyn Berlekamp

John Selfridge

Suppose that

$$n_1 \xrightarrow{s} n_2 \xrightarrow{s} n_3 \xrightarrow{s} \dots \xrightarrow{s} n_k \xrightarrow{s} n_1,$$

where $n_1, n_2, \dots, n_k$ are distinct. The numbers appearing here are called *sociable* (of order k).

Thus, sociable numbers of order 1 are perfect and sociable numbers of order 2 are amicable.

Though Meissner first posited in 1907 that there may be sociable numbers of order > 2, Poulet found the first ones in 1918: one cycle of length 5 and another of length 28. The smallest of order 5 is 12,496, while the smallest of order 28 is 14,316.

Today we know of 175 sociable cycles of order > 2, all but 10 of which have order 4. (The smallest sociable number of order 4 was found by Cohen in 1970 is 1,264,460.)

We know 47 perfect numbers and about 12 million amicable pairs.

We know the perfect numbers are sparse. What about the other amicables and other sociables?

Let $S_k(x)$ denote the number of integers in $[1, x]$ that are sociable of order k.

Let $\log_k x$ denote here the k-fold iteration of log.

$$\begin{aligned}
\text{Erdős (1955)}: &\ S_2(x) = o(x)\\
\text{Erdős \& Rieger (1973)}: &\ S_2(x) = O\left(x/(\log_4 x)^{1/2-\epsilon}\right)\\
\text{Erdős \& Rieger (1975)}: &\ S_2(x) = O(x/\log_3 x)\\
\text{Erdős (1976)}: &\ S_k(x) = o(x) \text{ for each fixed } k\\
\text{P (1977)}: &\ S_k(x) = O\left(x/\exp(c(\log_3 x \log_4 x)^{1/2}))\right)\\
\text{P (1981)}: &\ S_2(x) = O\left(x/\exp((\log x)^{1/3})\right)
\end{aligned}$$

Let $S(x) = \sum_k S_k(x)$ denote the number of sociable numbers in $[1, x]$.

Kobayashi, Pollack, & P (2009) : $S(x) \le (c + o(1))x$, where $c \approx 0.002$ is the density of the odd numbers n with $s(n) > n$.

Mitsuo Kobayashi

Paul Pollack

Our last topic is Carmichael numbers.

Fermat's "little theorem": *If n is prime, then*

$$a^n \equiv a \pmod{n} \tag{1}$$

for every integer a.

Proof: It is true for $a = 0$. Assume true at a. Then

$$(a+1)^n \equiv a^n + 1 \equiv a + 1 \pmod{n}.$$

Thus it is true for every integer a in $[0, n-1]$ so it is true for every integer a. □

A Carmichael number is a composite number where (1) holds for every integer a.

Do any exist? An easy criterion for n to be a Carmichael number is that

- n is composite,
- n is squarefree,
- $p - 1 \mid n - 1$ for each prime $p \mid n$.

This criterion was discovered by Korselt in 1899, some 11 years before Carmichael found the first examples.

Robert D. Carmichael

One can see that

$$\begin{aligned} 561 &= 3 \times 11 \times 17, \\ 1105 &- 5 \times 13 \times 17, \\ 1729 &= 7 \times 13 \times 19 \end{aligned}$$

all satisfy the criterion, so are Carmichael numbers. But are there infinitely many of them? Let $C(x)$ denote the number of Carmichael numbers in $[1, x]$.

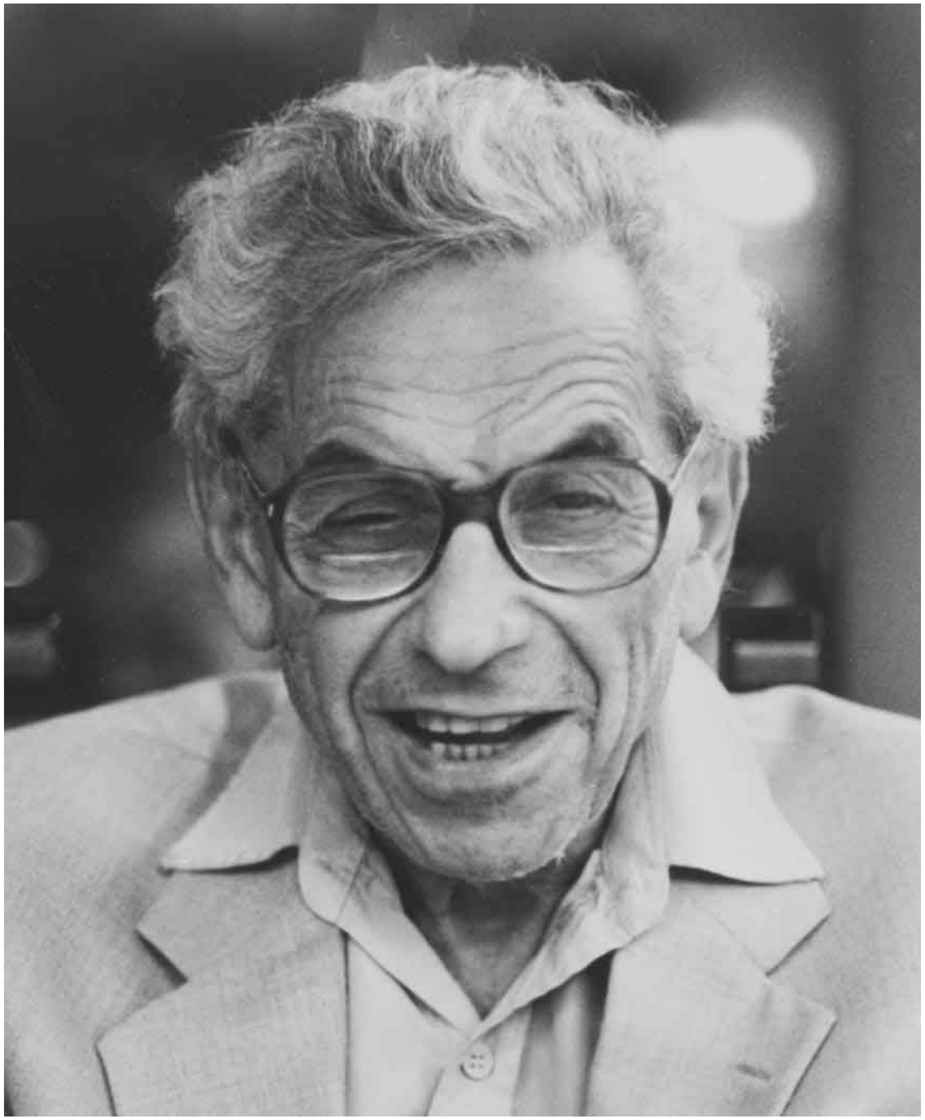
Erdős (1956): $C(x) \le x^{1-c(\log_3 x/\log_2 x)}$.

And Erdős gave a heuristic that $C(x) > x^{1-o(1)}$.

(For a survey that codifies the Erdős ideas see:
CP, *Two methods in elementary analytic number theory*, in Number theory and applications, Kluwer, 1989, pp. 135–161.)

Alford, Granville, & P (1994): $C(x) > x^{2/7}$ for all large x.

We dedicated the paper to Erdős for his 80th birthday.



Paul Erdős

THANK YOU!