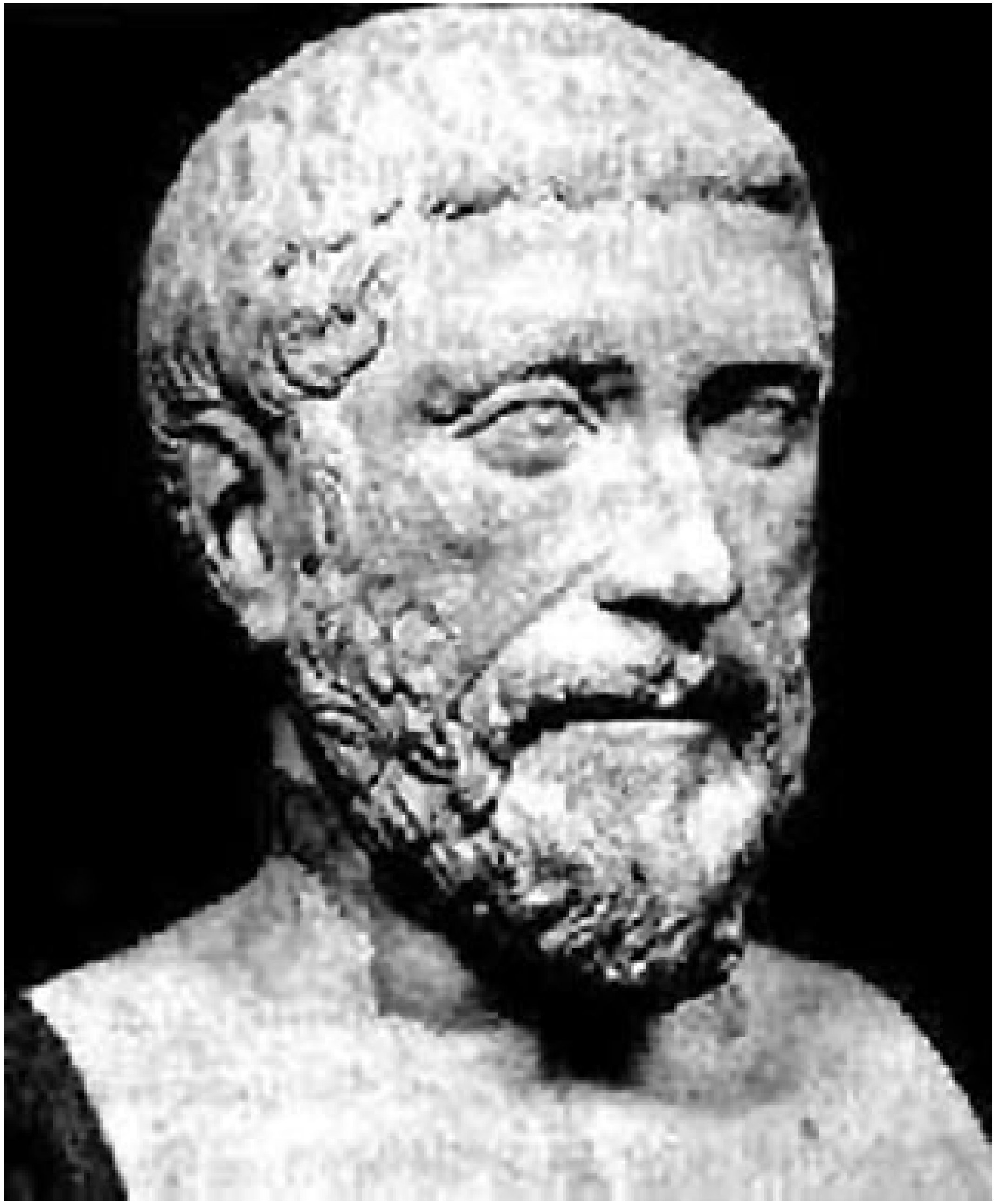
# Paul Erdős and the rise of statistical thinking in elementary number theory

Carl Pomerance, Dartmouth College

based on the joint survey with

Paul Pollack, University of Georgia

Let us begin at the beginning:



Pythagoras

## Sum of proper divisors

Let $s(n)$ be the sum of the *proper* divisors of $n$:

For example:

$$s(10) = 1 + 2 + 5 = 8, \quad s(11) = 1,$$
$$s(12) = 1 + 2 + 3 + 4 + 6 = 16.$$

In modern notation: $s(n) = \sigma(n) - n$, where $\sigma(n)$ is the sum of all of $n$'s natural divisors.

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

**Pythagoras**:

noticed that $s(6) = 1 + 2 + 3 = 6$

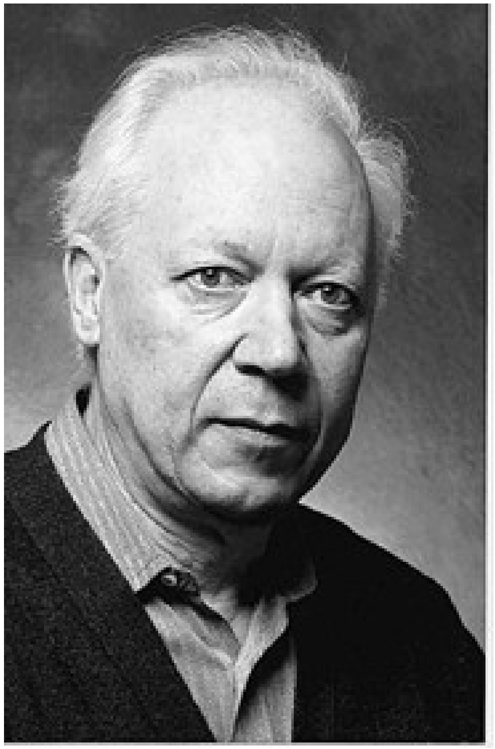
(If $s(n) = n$, we say $n$ is *perfect*.)

And he noticed that

$$s(220) = 284, \quad s(284) = 220.$$

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.

So 220 and 284 are amicable numbers.



In 1976, Enrico Bombieri wrote:

*“There are very many old problems in arithmetic whose interest is practically nil, e.g., the existence of odd perfect numbers, problems about the iteration of numerical functions, the existence of infinitely many Fermat primes* $2^{2^n}+1$*, etc.”*

Sir Fred Hoyle wrote in 1962 that there were two difficult astronomical problems faced by the ancients. One was a good problem, the other was not so good.

The good problem: Why do the planets wander through the constellations in the night sky?

The not-so-good problem: Why is it that the sun and the moon are the same apparent size?

Perfect numbers, amicable numbers, and similar topics were important to the development of elementary number theory.

Probabilistic number theory also owes its inspiration to some of these ancient problems.

The computational challenges posed by perfect numbers in particular have led to the blossoming of primality testing and more generally algorithmic number theory.

And, exponential diophantine equations, such as the Catalan equation $x^n + 1 = y^k$, have a link to the question of whether odd perfect numbers exist.

So, perhaps it could be argued that they are “good” problems, in the sense of Hoyle.

Though Bombieri's point of view is nevertheless understandable, these ancient problems continue to fascinate.

And they are fascinating to more than just number theorists:

St. Augustine wrote about perfect numbers in the bible: *“Six is a perfect number in itself, and not because God created all things in six days; rather the converse is true — God created all things in six days because the number is perfect.”*

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."*

In “Aim of the Wise”, attributed to Al-Majriti, ca. 1050 years ago, it is reported that the erotic effect of amicable numbers had been put to the test by:

*“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 . . . )

Nicomachus

**Nicomachus**, ca. 1900 years ago:

A natural number $n$ is *abundant* if $s(n) > n$ and is *deficient* if $s(n) < n$. These he defined in “Introductio Arithmetica” and went on to give what I call his ‘Goldilocks Theory’:

“ *In the case of too much, is produced excess, superfluity, exaggerations and abuse; in the case of too little, is produced wanting, defaults, privations* *and insufficiencies. And in the case of those that are found between the too much and the too little, that is in equality, is produced virtue, just measure, propriety, beauty and things of that sort — of which the most exemplary form is that type of number which is called perfect.”*

So, what is a modern number theorist to make of all this?

Answer: Think statistically.

Erich Bessel-Hagen, in a 1929 survey article, asked if the asymptotic density of the abundant numbers exist.

In his 1933 Berlin doctoral thesis, Felix Behrend proved that if the density exists, it lies between 0.241 and 0.314.

And later in 1933, Harold Davenport showed the density exists.

In fact, the density $D_\sigma(u)$ of those $n$ with $\sigma(n)/n \le u$ exists, and $D_\sigma(u)$ is continuous.

Note: The abundant numbers have density $1 - D_\sigma(2)$. A number of people have estimated this density, recently we learned it to 4 decimal places: 0.2476 . . . (Mitsuo Kobayashi, 2010).

Davenport strongly used a technical criterion of I. J. Schoenberg, who in 1928 proved an analogous result for the density of numbers $n$ with $n/\varphi(n) \le u$. Here $\varphi$ is Euler's function.

Beginning around 1935, Paul Erdős began studying this subject, looking for the great theorem that would unite these threads.

In addition Erdős began his quest for an elementary method.

This culminated in the Erdős–Wintner theorem in 1939.

## The Erdős–Wintner theorem:

For a positive-valued multiplicative arithmetic function $f$, let $g(n) = \log f(n)$. For $f$ to have a limiting distribution it is necessary and sufficient that

$$\sum_{|g(p)|>1} \frac{1}{p}, \qquad \sum_{|g(p)|\le 1} \frac{g(p)^2}{p}, \qquad \sum_{|g(p)|\le 1} \frac{g(p)}{p}$$

all converge. Further, if $\sum_{g(p)\neq 0} 1/p$ diverges, the distribution is continuous.

Example: $f(n) = \sigma(n)/n$, so that $g(p) = \log(1 + \frac{1}{p}) \approx \frac{1}{p}$.

Surely this beautiful theorem can justify the low origins of the definition of abundant numbers!

But what of other familiar arithmetic functions such as $\omega(n)$, which counts the number of distinct primes that divide $n$?

This function is additive, so it is already playing the role of $g(n)$.

However, $\omega(p) = 1$ for all primes $p$, so the 2nd and 3rd series diverge.

It's in how you measure.

Hardy and Ramanujan had shown that $\omega(n)/\log\log n \to 1$ as $n \to \infty$ through a set of asymptotic density 1. So there is a *threshold* function: we should be studying the difference $\omega(n) - \log\log n$.

**The Erdős–Kac theorem** (1939):

For each real number $u$, the asymptotic density of the set

$$\left\{n : \omega(n) - \log\log n \le u\sqrt{\log\log n}\right\}$$

is

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,\mathrm{d}t.$$

This is the Gaussian normal distribution, the Bell curve!

Einstein: “God does not play dice with the universe.”

Einstein: “God does not play dice with the universe.”

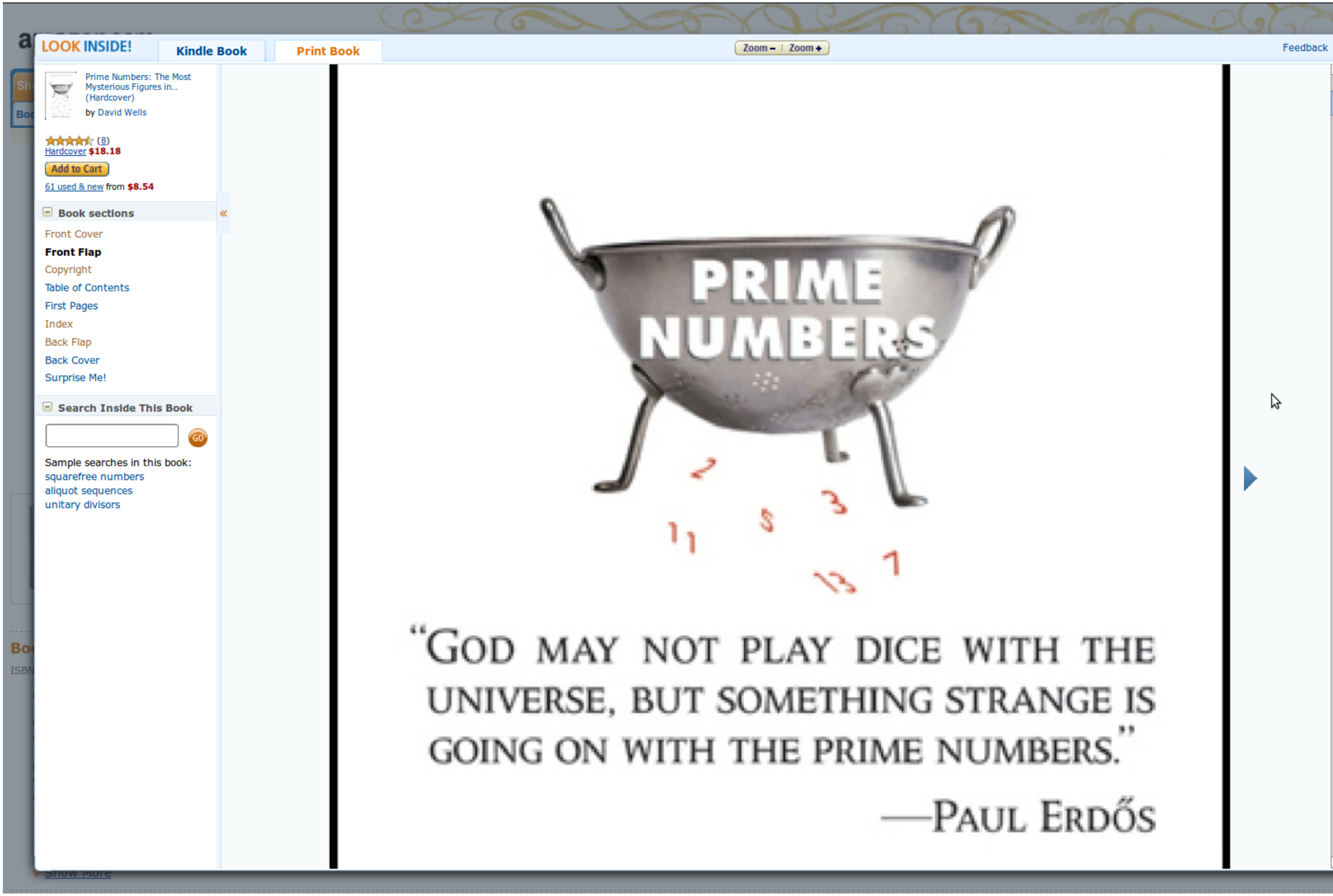
Erdős & Kac: Maybe so but something’s going on with the primes.

Einstein: “God does not play dice with the universe.”

Erdős & Kac: Maybe so but something’s going on with the primes.

(Note: I made this up, it was a joke . . . )

*Prime numbers, the most mysterious figures in math*, D. Wells



Prime Numbers: The Most Mysterious Figures in... (Hardcover)
by David Wells

(8)
Hardcover $18.18

61 used & new from $8.54

Sample searches in this book:
squarefree numbers
aliquot sequences
unitary divisors

"God may not play dice with the universe, but something strange is going on with the prime numbers."

—Paul Erdős

Some background on the Erdős–Kac theorem would be helpful, it didn't arise spontaneously.

In 1934, Paul Turán gave a simplified proof of the Hardy–Ramanujan theorem. Quoted in Elliott's *Probabilistic Number Theory*, Turán said in 1976: "... *I did not know what Chebyshev's inequality was and a fortiori the central limit theorem. Erdős, to my best knowledge, was at that time not aware too. It was*

*Mark Kac who wrote to me a few years later that he discovered when reading my proof in J.L.M.S. that this is basically probability and so was his interest turned to this subject.”*

Elliott also quotes Mark Kac: *“If I remember correctly I first stated (as a conjecture) the theorem on the normal distribution of the prime divisors during a lecture in Princeton in March 1939. Fortunately for me and possibly for Mathematics, Erdős was in the audience, and he immediately perked up. Before the lecture was over he had completed the proof, which I could not have done not having been versed in the number* *theoretic methods, especially those related to the sieve.”*

Let us return to the problem of amicable numbers introduced by Pythagoras 2500 years ago.

Recall: Two numbers are amicable if the sum of the proper divisors of one is the other and vice versa. The Pythagorean example: 220 and 284.

We have seen that amicable numbers have fascinated people through the intervening centuries. Thabit ibn Kurrah found a formula that gave a few examples. Euler found a few. So far we know about twelve million pairs, and probably there are infinitely many, but we have no proof.

How would Erdős approach this problem?

Why count of course!

Let $A(x)$ denote the number of integers in $[1, x]$ that belong to an amicable pair. We have no good lower bounds for $A(x)$ as $x \to \infty$, but what about an upper bound?

For perfect numbers, which are closely related to the amicables, we know a fair amount about upper bounds. First, from Davenport's theorem on the continuity of the distribution function of $\sigma(n)/n$ it is immediate that the perfect numbers have asymptotic density 0.

There are much better upper bounds for the distribution of perfect numbers. Erdős made a fundamental contribution here, but the champion result is due to Hornfeck and Wirsing: the number of perfect numbers in $[1, x]$ is at most $x^{o(1)}$.

But amicables presumably form a larger set, maybe much larger.

Erdős (1955) was the first to show that $A(x) = o(x)$, that is, the amicable numbers have asymptotic density 0.

His insight: the smaller member of an amicable pair is abundant, the larger is deficient. Thus, we have an abundant number with the sum of its proper divisors being deficient.

This property alone is enough to prove density 0.

Let us look at a sketch of the proof. Let $h(n) = \sigma(n)/n$. We are counting numbers $n \le x$ for which

$$h(n) > 2 \quad \text{and} \quad h(s(n)) < 2.$$

Erdős first used the continuity of the distribution function for $h$ so that instead of merely assuming $h(n) > 2$, we have the stronger assumption $h(n) > 2 + \delta$ (for some fixed tiny $\delta > 0$).

Note that $h(n)$ is the sum of $1/d$ for $d \mid n$ and $1 \le d$. For a parameter $y$, let $h_y(n)$ be the sum of $1/d$ for $d \mid n$ and $1 \le d \le y$.

Erdős next argued by an averaging argument that, for $y$ large, we usually have $h_y(n) \approx h(n)$, so that we may assume that

$$h_y(n) = \sum_{d|n,\, d\leq y} \frac{1}{d} > 2.$$

Now the key step: Let $M$ be the lcm of $\{1, 2, \ldots, \lfloor y \rfloor\}$. Almost all numbers $n$ are divisible by a prime $p$ to the first power with $p + 1 \equiv 0 \pmod{M}$. (Hint: use Dirichlet.)

Thus, for almost all numbers $n$, we have $M \mid \sigma(n)$, and so $s(n) = \sigma(n) - n$ has exactly the same divisors up to $y$ as $n$ does.

Assuming this,

$$h(s(n)) \geq h_y(s(n)) = h_y(n) > 2,$$

contradicting the assumption that $h(s(n)) < 2$. QED

I later gave a simplified proof using another Erdős insight: the distribution of *primitive* abundant numbers (1935). (And then in another paper, I showed the reciprocal sum of the amicable numbers is finite.)

Though Erdős did not contribute directly to computational number theory, his statistical viewpoint is part of the landscape here too.

For example, in Canfield, Erdős, P (1983), the distribution of “smooth” (or “friable”) numbers was worked out to enough detail to give accurate guidance to the construction and analysis of integer factorization algorithms.

This paper is his 13th most-cited on *mathscinet* (and Canfield's and my #1).

Fermat proved that if $p$ is a prime then $a^p \equiv a \pmod{p}$ for every integer $a$. It is an easy congruence to check. Can one reason from the converse??

Say a composite number $n$ is a *base-$a$ pseudoprime* if $a^n \equiv a \pmod{n}$.

Pseudoprimes exist. For example, $2^{341} \equiv 2 \pmod{341}$.

Erdős (1949, 1950) was the first to show that for each fixed base $a > 1$, the pseudoprimes are very rare in comparison to primes. Due to this, if one has a large random number and tests merely if $2^n \equiv 2 \pmod{n}$, accepting $n$ as prime if the congruence holds, one would almost surely be right!

Though there is of course some chance for error here, it is actually a practical way to recognize primes, it is fast, and it is extraordinarily simple.

Erdős was very interested in *Carmichael numbers*. These are numbers, like 561, which are pseudoprimes to every base. In 1956 he got the essentially best-known upper bound for $C(x)$, the number of Carmichael numbers in $[1, x]$:

$$C(x) \le x^{1-c\log\log\log x/\log\log x}.$$

He also gave a heuristic argument (based on a seminal paper of his from 1935) that this was essentially best possible.

The Erdős conjecture on Carmichael numbers: $C(x) \geq x^{1-\epsilon}$.

In 1993, Alford, Granville, P gave a rigorous proof, based on the Erdős heuristic, that $C(x) > x^{2/7}$ for all large $x$ and that $C(x) > x^{1-\epsilon}$ assuming the Elliott–Halberstam conjecture on the distribution of primes in residue classes.

And what was this seminal paper from 1935 just mentioned?

It was in:
Quarterly J. Math. Oxford Ser. **6** (1935), 205–213.

# ON THE NORMAL NUMBER OF PRIME FACTORS OF $p-1$ AND SOME RELATED PROBLEMS CONCERNING EULER'S $\phi$-FUNCTION

*By* PAUL ERDŐS (*Manchester*)

[Received 13 November 1934]

THIS paper is concerned with some problems considered by Hardy and Ramanujan, Titchmarsh, and Pillai. Suppose we are given a set $M$ of positive integers $m$. Let $N(n)$ denote the number of $m$ in the interval $(0, n)$. By saying that the normal number of prime factors of a number $m$ is $B(n)$, we mean that, as $n \to \infty$, there are only $o[N(n)]$ of the $m$ $(\leq n)$ for which the number of prime factors does

As mentioned, Hardy & Ramanujan showed that $n$ normally has about $\log\log n$ prime factors. Clearly then, primes are not normal! But are numbers $p-1$ normal?

In this paper, submitted for publication at the age of 21, Erdős showed that yes, $p-1$ is indeed normal with respect to the number of its prime factors.

Not only is this interesting on its own, the proof of the normality of $p-1$ was one of the early applications of Brun's sieve method, of which Erdős was so famous.

And the result was an essential tool in solving a problem of Pillai: how many numbers in $[1, x]$ are values of $\varphi$ (Euler's function)?

Erdős showed that this count of $\varphi$-values in $[1, x]$ is of the shape $x/(\log x)^{1+o(1)}$. And while he was on the topic, he proved the following astounding result:

*There is a positive constant $c$ such that for infinitely many numbers $N$, there are more than $N^c$ solutions to $\varphi(n) = N$.*

He gave a heuristic that "$c$" here can be taken as any number smaller than 1. It was this construction that was so important in the proof of the infinitude of Carmichael numbers.

The value of $c$ in the theorem has slowly climbed over the intervening years, with many players. Currently it is about 0.7, a result of Baker and Harman.

The count of $x/(\log x)^{1+o(1)}$ for $\varphi$-values in $[1, x]$ has been refined as well, with the current best result due to Ford: it is of magnitude

$$\frac{x}{\log x} \exp\left(c_1(\log_3 x - \log_4 x)^2 + c_2 \log_3 x + c_3 \log_4 x\right)$$

for certain explicit constants $c_1, c_2, c_3$.

The same is true for the set of values of $\sigma(n)$ in $[1, x]$.

In many ways, $\sigma$ and $\varphi$ are twins. Erdős asked in 1959 if there are infinitely many solutions to $\varphi(m) = \sigma(n)$.

Yes, if there are infinitely many twin primes:

If $p$, $p+2$ are both prime, then

$$\varphi(p+2) = p+1 = \sigma(p).$$

Infinitely many solutions to $\varphi(m) = \sigma(n)$?

Yes, if there are infintely many Mersenne primes:

If $2^p - 1$ is prime, then

$$\varphi(2^{p+1}) = 2^p = \sigma(2^p - 1).$$

Yes, if the Extended Riemann Hypothesis holds.

Infinitely many solutions to $\varphi(m) = \sigma(n)$?

Yes, if there are infintely many Mersenne primes:

If $2^p - 1$ is prime, then

$$\varphi(2^{p+1}) = 2^p = \sigma(2^p - 1).$$

Yes, if the Extended Riemann Hypothesis holds.

Ford, Luca, & P (2010): *Yes.*

I would like to close with one last ancient problem: prime numbers.

2300 years ago, Euclid was the first to consider counting primes: he proved there are infinitely many.

One might argue then that it is Euclid who first offered the statistical viewpoint.

Detail from Raphael's mural *The School of Athens*, ca. 1510

Further progress was made 2000 years later by Euler:

$$\sum_{p \le x} \frac{1}{p} \sim \log\log x.$$

Fifty years later: Gauss and Legendre conjectured that

$$\pi(x) := \sum_{p \le x} 1 \sim \frac{x}{\log x}.$$

Fifty years later: Chebyshev proved that $\pi(x)$ is of magnitude $x/\log x$. And Riemann laid out a plan to prove the Gauss–Legendre conjecture.

Fifty years later: Hadamard and de la Vallee Poussin proved it.

Fifty years later: Erdős and Selberg gave an elementary proof.

We're a bit overdue for the next installment ... .

I would like to think that beyond the “Prime Number Theorem”, Erdős was searching too for the “Amicable Number Theorem”, the “Perfect Number Theorem”, and so on.

In all of these problems and results we can see echoes of the past at the dawn of number theory and mathematics.

Perhaps the ancient problems will never be completely solved, but thinking about them statistically has made all the difference.

And leading the way, was **Paul Erdős**.

# Köszönöm