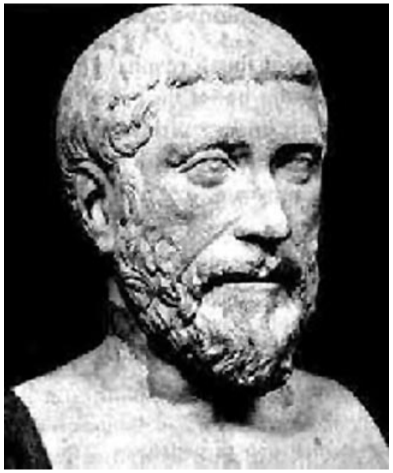
The first function

Carl Pomerance, Dartmouth College

U. Georgia, emeritus

U. Georgia Colloquium, Dec. 3, 2014



As we all know, functions in mathematics are ubiquitous and indispensable.

But what was the very first function mathematicians studied?

I would submit as a candidate, the function $s(n)$ of 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.

Pythagoras noticed that $s(6) = 1 + 2 + 3 = 6$
If $s(n) = n$, we say n is *perfect*.

And he noticed that

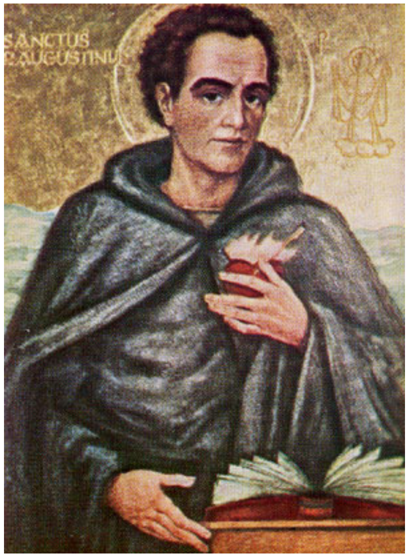
$$s(220) = 284, \quad s(284) = 220.$$

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.

This talk:

- The age of numerology
- The age of formulas and examples
- The age of statistics
- Is it good mathematics?



St. Augustine wrote about perfect numbers: *“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.”*

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 Genesis: To win his brother's friendship, Jacob gave his brother Esau 220 goats and 220 sheep.

"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."
(Abraham Azulai, ca. 400 years ago)

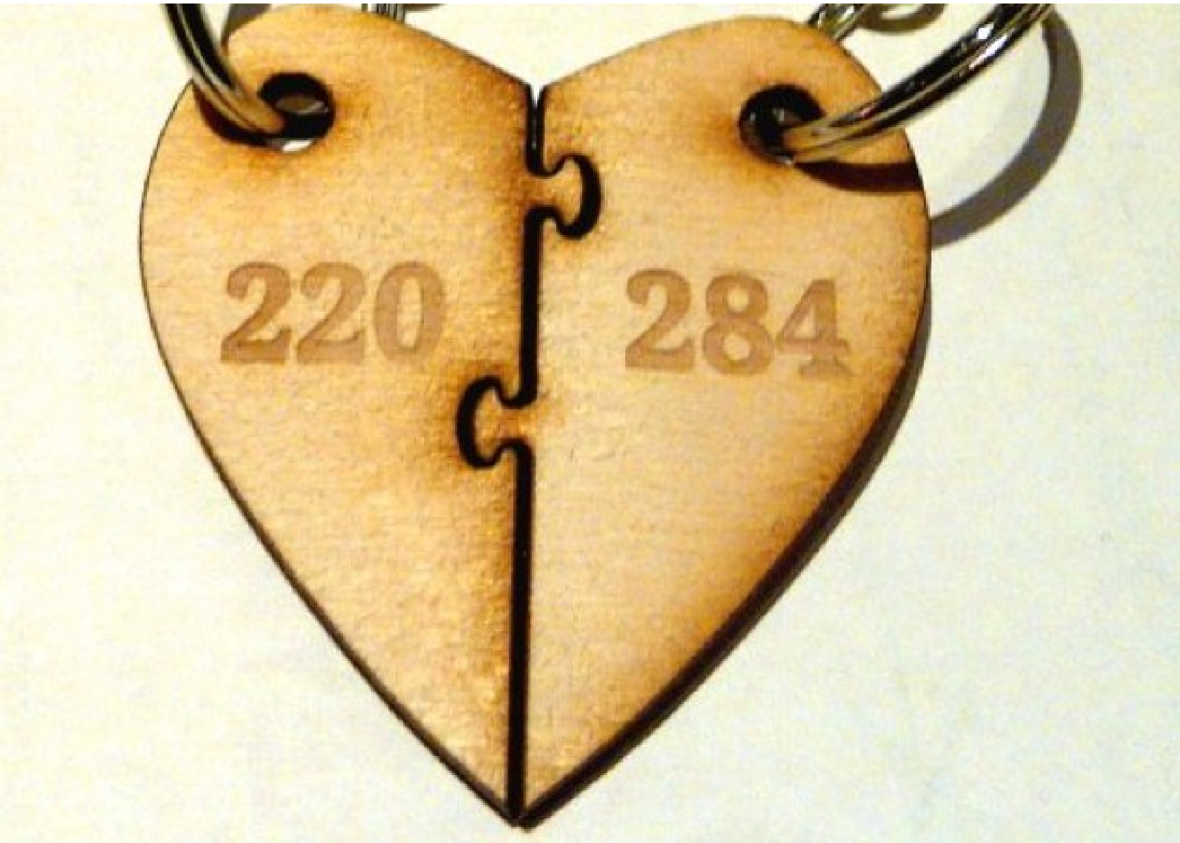
In “Aim of the Wise”, attributed to Al-Majriti, ca. 1050 years ago, it is reported that the erotic effect of amicable numbers was successfully put to the test by:

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

In case you’re curious, it’s reported elsewhere that this might involve pomegranate seeds or raisins.

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

And here's a more modern application:



Available for £9 from mathsgear.co.uk

The age of computation and formulas overlaps the age of numerology:

Euclid came up with a formula for perfect numbers 2300 years ago:
If $2^p - 1$ *is prime, then* $2^{p-1}(2^p - 1)$ *is perfect.*

Euler proved that all even perfect numbers are given by Euclid's formula.

What about odd perfect numbers? Well, there are none known.

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

Probably Euclid knew that a necessary condition for $2^p - 1$ to be prime is that p is prime, and that this condition is not sufficient. He gave as examples $p = 2, 3, 5, 7$, but not 11, presumably because he knew that $2^{11} - 1$ is composite. Here are Euclid's perfects:

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

By 1640, Fermat knew that prime exponents 13, 17, 19 work, and 23 doesn't. In 1644, Mersenne wrote that in the range 29 to 257, the only primes that work are 31, 67, 127, and 257. The correct list in this range is 31, 61, 89, 107, and 127, but Mersenne was not shown to be wrong till 1883, with the discovery of 61 by Pervouchine. Mersenne was right that there are few primes that work in this range, and we still call primes of the form $2^p - 1$ *Mersenne primes*.

We now know 48 Mersenne primes, the largest having exponent 57,885,161 (though they have only been exhaustively searched for to about half this level).

The modern search for Mersenne primes uses the Lucas–Lehmer test:
Let $M_p = 2^p - 1$. Consider the iteration $s_0 = 4$, $s_1 = 14$, $s_2 = 194$, ..., where the rule is $s_k = s_{k-1}^2 - 2 \pmod{M_p}$. Then, for $p > 2$, M_p is prime if and only if the $s_{p-2} = 0$.

This test makes best sense when viewed through the lens of finite fields. In my survey article "*Primality testing: variations on a theme of Lucas*" I argued that the whole edifice of primality testing rests squarely on a foundation laid by Lucas 140 years ago.

Probably there are no odd perfect numbers. Here's why I think so:
One might view the residue $s(n) \pmod{n}$ as "random", where the event that n is perfect implies $s(n) \equiv 0 \pmod{n}$. It's been known since Euler (and easy to prove) that an odd perfect number n must be of the form pm^2 where p is prime and $p \mid \sigma(m^2)$ $(= s(m^2) + m^2)$. In particular, there are at most $c \log m$ possibilities for p, once m is given. Once one of these p's is chosen, we will have $s(pm^2) \equiv 0 \pmod{p}$, so there remains at best a $1/m^2$ chance that pm^2 will be perfect. Since $\sum(c \log m)/m^2$ converges, there should be at most finitely many odd perfect numbers. But we know there are no small ones, so it is likely there are none.

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.

In 1929 in a survey article, Erich Bessel-Hagen asked if the asymptotic density of

$$\{n : s(n) > n\} = \{n : \sigma(n) > 2n\},$$

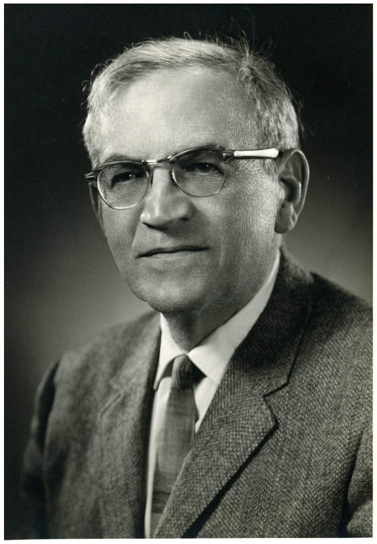
the set of abundant numbers, exists.

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, building on work of I. J. Schoenberg from 1928 dealing with Euler's function, 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.

Bessel-Hagen



Schoenberg

Davenport

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: $0.2476\ldots$
(Mitsuo Kobayashi, 2011).

The Schoenberg–Davenport approach towards the distribution function of $\sigma(n)/n$ was highly analytic and technical.

Beginning around 1935, Paul Erdős began studying this subject, looking for the great theorem that would unite and generalize the work on Euler's function and σ, and also to look for an elementary method.

This culminated in the Erdős–Wintner theorem in 1939:

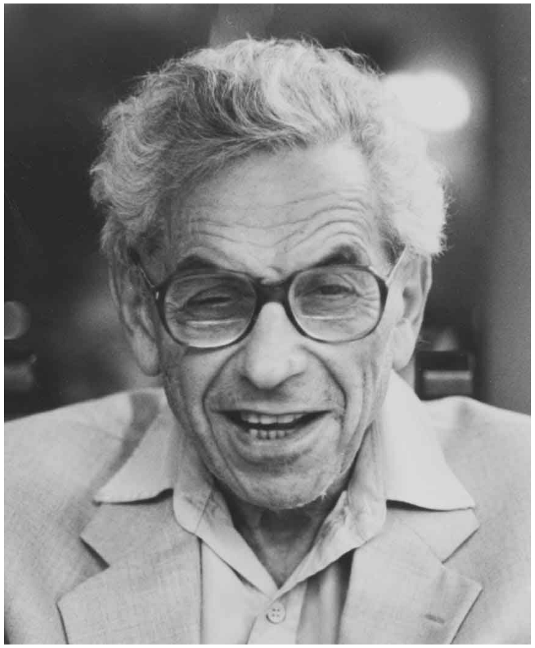
The Erdős–Wintner theorem:

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 $g(p) = \log(1 + \frac{1}{p}) < \frac{1}{p}$.



Erdős

Wintner

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.

The solution is 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. There is a *threshold* function, so one should be studying the difference $\omega(n) - \log\log n$.

Ramanujan

Hardy

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!

Kac

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

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

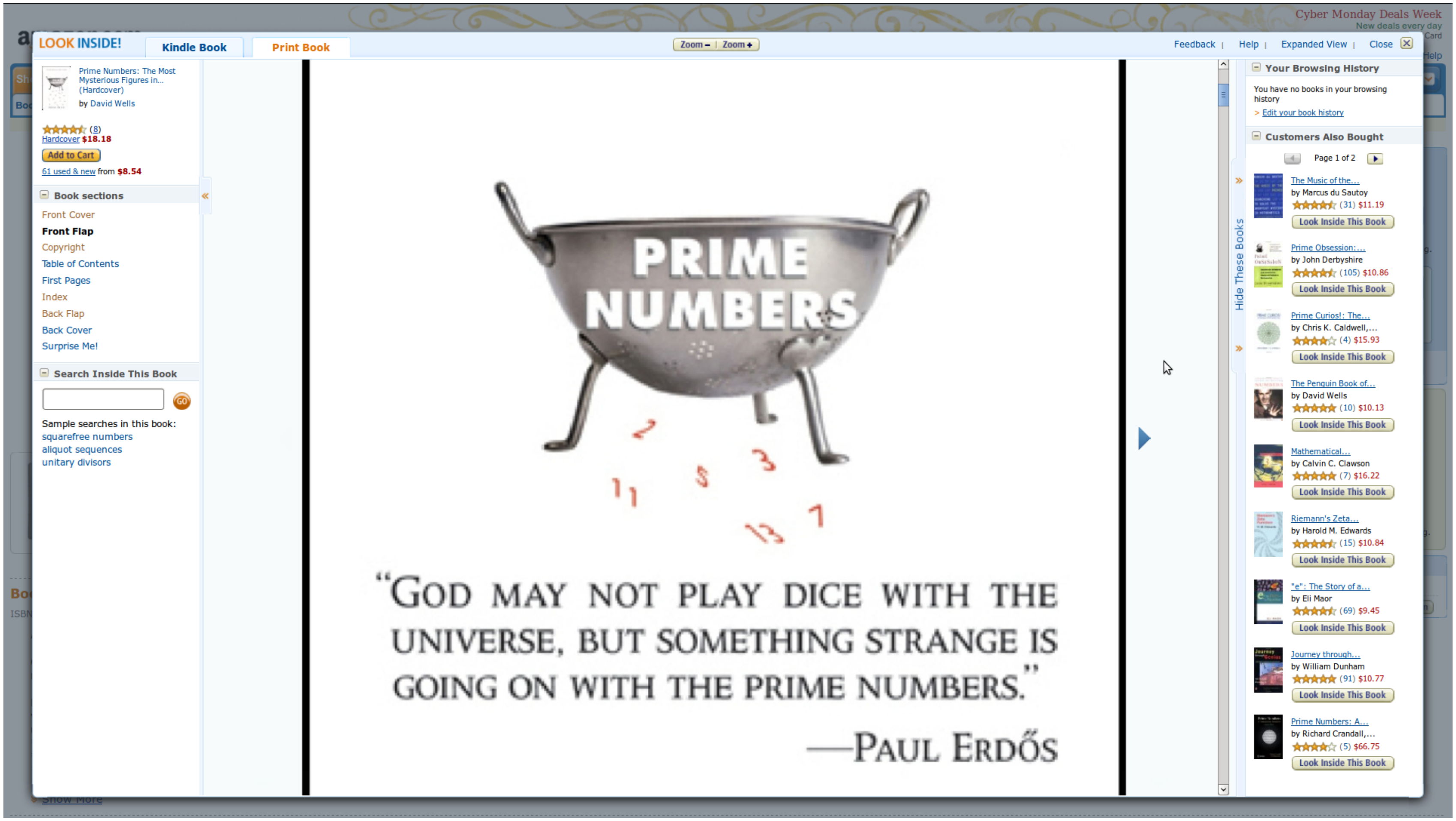
Erdős & Kac: Maybe so but something’s going on with the primes.

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

★★★★½ (8)
Hardcover $18.18

61 used & new from $8.54

Book sections

- Front Cover
- **Front Flap**
- Copyright
- Table of Contents
- First Pages
- Index
- Back Flap
- Back Cover
- Surprise Me!

Search Inside This Book

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

Your Browsing History

You have no books in your browsing history

> Edit your book history

Customers Also Bought

Page 1 of 2

The Music of the...
by Marcus du Sautoy
★★★★½ (31) $11.19

Prime Obsession:...
by John Derbyshire
★★★★½ (105) $10.86

Prime Curios!: The...
by Chris K. Caldwell,...
★★★★☆ (4) $15.93

The Penguin Book of...
by David Wells
★★★★★ (10) $10.13

Mathematical...
by Calvin C. Clawson
★★★★★ (7) $16.22

Riemann's Zeta...
by Harold M. Edwards
★★★★½ (15) $10.84

"e": The Story of a...
by Eli Maor
★★★★½ (69) $9.45

Journey through...
by William Dunham
★★★★★ (91) $10.77

Prime Numbers: A...
by Richard Crandall,...
★★★★☆ (5) $66.75

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 Pythagoras example: 220 and 284.

We have seen that amicable numbers have fascinated people through the intervening centuries. Thābit ibn Kurrah found a formula, similar to Euclid's for even perfect numbers, that gave a few examples. Descartes and Fermat rediscovered Thābit's formula, and Euler generalized it, finding 58 amicable pairs.

His generalized formula missed the second smallest pair, found in 1866 by Paganini at the age of 16: namely 1184 and 1210.

So far we know about twelve million pairs, and probably there are infinitely many, but we have no proof.

Beyond individual examples and possible formulas, how are the amicable numbers distributed within the natural numbers?

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 might be viewed as a subset of 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 form a larger set, maybe much larger.

Erdős (1955) was the first to show $A(x) = o(x)$, 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.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Rieger (1973): $A(x) \le x/(\log\log\log\log x)^{1/2}$, x large.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Rieger (1973): $A(x) \leq x/(\log\log\log\log x)^{1/2}$, x large.

Erdős & Rieger (1975): $A(x) = O(x/\log\log\log x)$.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Rieger (1973): $A(x) \le x/(\log\log\log\log x)^{1/2}$, x large.

Erdős & Rieger (1975): $A(x) = O(x/\log\log\log x)$.

P (1977): $A(x) \le x/\exp((\log\log\log x)^{1/2})$, x large.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Rieger (1973): $A(x) \le x/(\log\log\log\log x)^{1/2}$, x large.

Erdős & Rieger (1975): $A(x) = O(x/\log\log\log x)$.

P (1977): $A(x) \le x/\exp((\log\log\log x)^{1/2})$, x large.

P (1981): $A(x) \le x/\exp((\log x)^{1/3})$, x large.

Erdős (1955): $A(x) = o(x)$ as $x \to \infty$. Said his method would give $A(x) = O(x/\log\log\log x)$.

Rieger (1973): $A(x) \le x/(\log\log\log\log x)^{1/2}$, x large.

Erdős & Rieger (1975): $A(x) = O(x/\log\log\log x)$.

P (1977): $A(x) \le x/\exp((\log\log\log x)^{1/2})$, x large.

P (1981): $A(x) \le x/\exp((\log x)^{1/3})$, x large.

P (2014): $A(x) \le x/\exp((\log x)^{1/2})$, x large.

Note that the last two results imply by a simple calculus argument that the reciprocal sum of the amicable numbers is finite.

So, what is this sum of reciprocals? Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum P satisfies

$$P > 0.0119841556\ldots.$$

So, what is this sum of reciprocals? Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum P satisfies

$$P > 0.0119841556\ldots.$$

Bayless & Klyve (2011): $P < 656{,}000{,}000$.

So, what is this sum of reciprocals? Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum P satisfies

$$P > 0.0119841556\ldots.$$

Bayless & Klyve (2011): $P < 656{,}000{,}000$.

Nguyen (2014): $P < 4084$

Back to Pythagoras:
A number n is perfect if $s(n) = n$.
A number n is amicable if $s(s(n)) = n$, but not perfect.

That is, Pythagoras not only invented the first function, but also the first *dynamical system*.

Let's take a look at this system.

Many orbits end at 1, while others cycle:

$10 \to 8 \to 7 \to 1$

$12 \to 16 \to 15 \to 9 \to 4 \to 3 \to 1$

$14 \to 10 \ldots$

$18 \to 21 \to 11 \to 1$

$20 \to 22 \to 14 \ldots$

$24 \to 36 \to 55 \to 17 \to 1$

$25 \to 6 \to 6$

$26 \to 16 \ldots$

$28 \to 28$

$30 \to 42 \to 54 \to 66 \to 78 \to 90 \to 144 \to 259 \to 45 \to 33 \to 15 \ldots$

Some orbits are likely to be arbitrarily long. For example, consider the orbit

$$25 \to 6 \to 6.$$

It can be preceded by 95:

$$95 \to 25 \to 6 \to 6.$$

And again preceded by 445:

$$445 \to 95 \to 25 \to 6 \to 6.$$

What's happening here: To hit an odd number m, write $m-1$ as the sum of two different primes: $p+q=m-1$. Then $s(pq)=m$. So, Goldbach's conjecture implies one can back up forever.

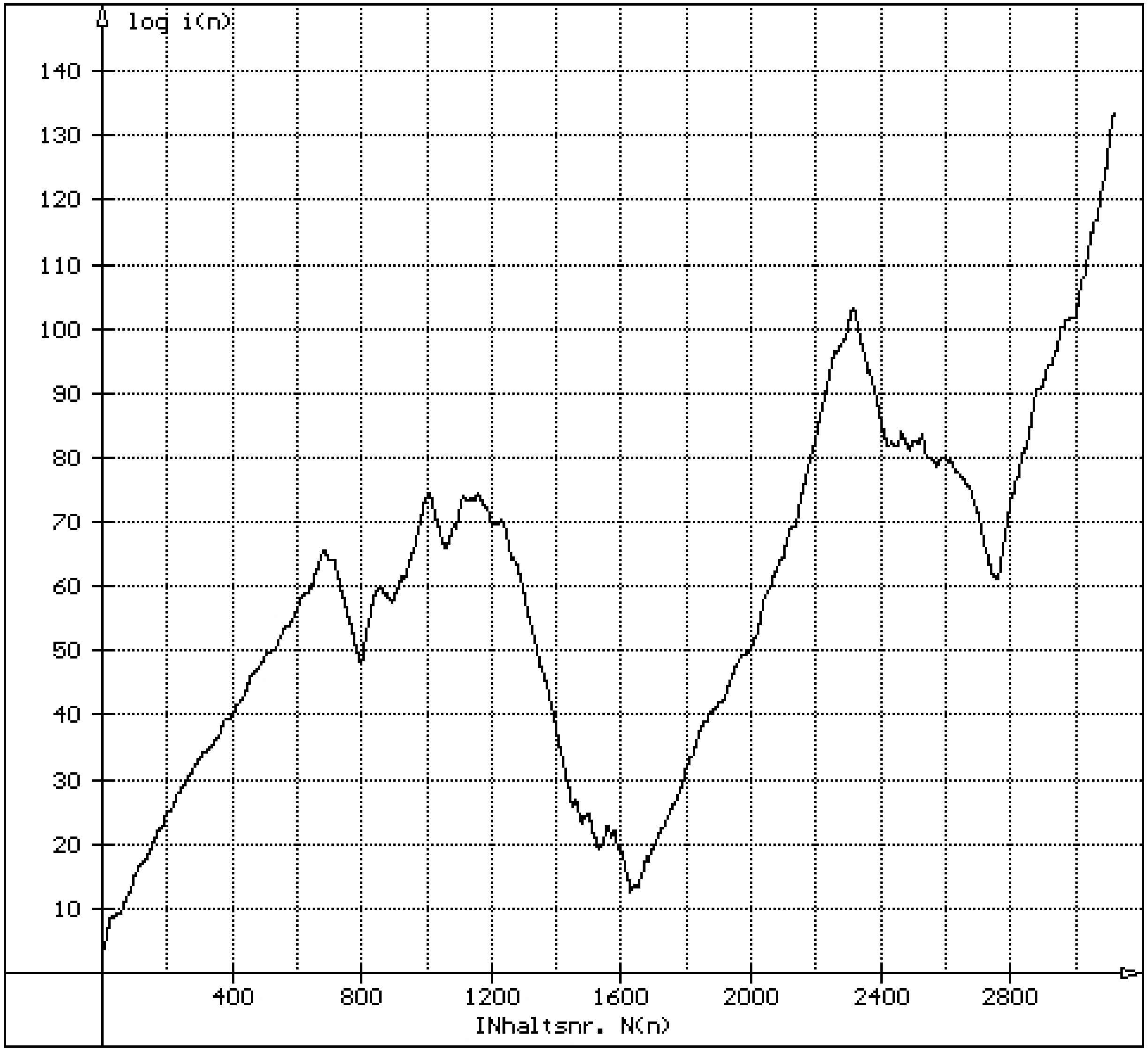
Lenstra (1975):
There are arbitrarily long increasing "aliquot" sequences

$$n < s(n) < s(s(n)) < \cdots < s_k(n).$$

Erdős (1976): *In fact, for each fixed k, if $n < s(n)$, then almost surely the sequence continues to increase for $k - 1$ more steps.*

Nevertheless, we have the **Catalan–Dickson conjecture:**
Every aliquot sequence is bounded.

Here are some data in graphical form for the sequence starting with 564. (The least starting number which is in doubt is 276.) See aliquot.de, maintained by Wolfgang Creyaufmüller.



564 iteration

This has been continued for over 3000 iterations, the numbers that would need to be factored in order to go farther are over 160 decimal digits.

There are 5 numbers below 1000 where it's not clear what's happening:

$$276, \quad 552, \quad 564, \quad 660, \quad 966,$$

known as the "Lehmer five".

The Guy & Selfridge counter conjecture:
For asymptotically all n with $n < s(n)$, the aliquot sequence starting with n is unbounded.

One can also ask about cycles in the s-dynamical system beyond the fixed points (perfect numbers) and 2-cycles (amicable pairs). There are about 12 million cycles known, with all but a few being 2-cylces, and most of the rest being 1-cycles and 4-cycles. There are no known 3-cycles, and the longest known cycle has length 28.

Say a number is *sociable* if it is in some cycle. Do the sociable numbers have density 0? Erdoős showed this is the case if one restricts to cycles of bounded length. Recently, **Pollack, P, & Kobayashi** showed that sociable numbers that are not odd and abundant have density 0. We also computed that the density of odd abundant numbers is about 0.002. There is more work to do!

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?

So, was the study of $s(n)$ a good problem in the sense of Hoyle?

It led us to the study of arithmetic functions and their distribution functions, opening up the entire field of probabilistic number theory.

It led us to the Lucas–Lehmer primality test and essentially all of modern primality testing.

The aliquot sequence problem helped to spur on the quest for fast factoring algorithms.

The study of the distribution of special numbers did not stop with amicables. We have studied prime numbers, and that has led us to analytic number theory and the Riemann Hypothesis.

So, maybe having a little fun along the way was okay!

THANK YOU