The first function

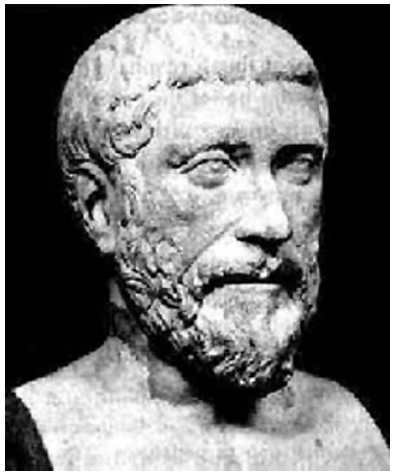
Carl Pomerance, Santa Clara University

Dartmouth College, emeritus

U. Georgia, emeritus

BAMA, Santa Clara University

January 31, 2020



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:

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

(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

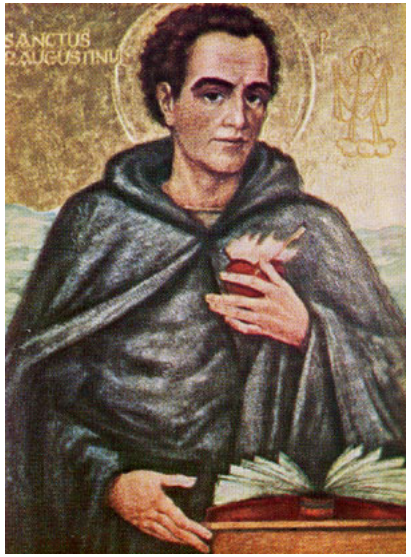
$$s(220) = 284, \quad s(284) = 220.$$

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: *"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."*
(City of God, Part XI, Chapter 30)

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 £11.93 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.*

Euclid gave these examples of perfect numbers:

$$\begin{aligned} 2(2^2 - 1) &= 2 \cdot 3 = 6, \\ 2^2(2^3 - 1) &= 4 \cdot 7 = 28, \\ 2^4(2^5 - 1) &= 16 \cdot 31 = 496, \\ 2^6(2^7 - 1) &= 64 \cdot 127 = 8128. \end{aligned}$$

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

Euclid: If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect.

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. We saw he gave as examples $p = 2, 3, 5, 7$, but not 11, presumably because he knew that $2^{11} - 1$ is composite.

Euler proved that all **even** perfect numbers are given by **Euclid**'s formula. We still don't know if there are infinitely many even perfect numbers.

What about **odd** perfect numbers? Well, there are none known. And we don't know if there are any.

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 51 Mersenne primes, the largest having exponent 82,589,933. We conjecture there are infinitely many of them. We also conjecture there are infinitely many primes p with $2^p - 1$ composite!

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 term* s_k *is the remainder when* $s_{k-1}^2 - 2$ *is divided by* M_p.

Then, for $p > 2$, M_p *is prime if and only if* $s_{p-2} = 0$.

For example, with $p = 5$ and $M_5 = 31$, we have

$$s_0 = 4, \quad s_1 = 14, \quad s_2 = 8, \quad s_3 = 0,$$

so 31 is prime. And with $p = 11$, $M_{11} = 2047$,

$$s_0 = 4,\ s_1 = 14,\ s_2 = 194,\ s_3 = 788,\ s_4 = 701,\ s_5 = 119,$$

$$s_6 = 1877,\ s_7 = 240,\ s_8 = 282,\ s_9 = 1736,$$

so 2047 is composite.

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** 144 years ago.

Probably there are no odd perfect numbers:

It's been known since **Euler** (and easy to prove) that every perfect number n after 6 must be of the form pm^2 where p is a prime divisor of $s(m^2) + m^2$. So given m there are at most about $\ln m$ possible choices for p. For each such choice we will have $s(pm^2)$ a multiple of p, but for pm^2 to be perfect, we need it to be a multiple of m^2 as well. In the case of even perfect numbers, this works out from the formula, but for odd examples it would seem that $s(pm^2)$ is about as likely to be a multiple of m^2 as a random number, namely with probability $1/m^2$. But we have about $\ln m$ lottery tickets p which possibly could bring home a perfect number. However, the infinite sum of $(\ln m)/m^2$ converges to a finite number, suggesting there are no large examples. We already know there are no small examples, so probably 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

$$\{n : s(n) > n\},$$

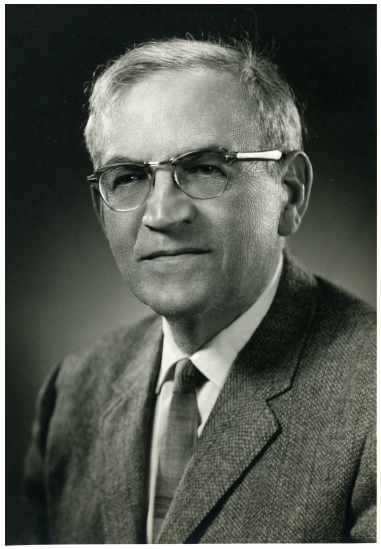
the set of abundant numbers, exists. For example, all the multiples of 6 after 6 itself are abundant, so this brings 1/6 of all numbers to the abundant category. Is there some constant α such that the frequency of abundant numbers tends to α?

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 $D_s(u)$ of those n with $s(n)/n > u$ exists, and $D_s(u)$ is continuous.

Bessel-Hagen



Schoenberg

Davenport

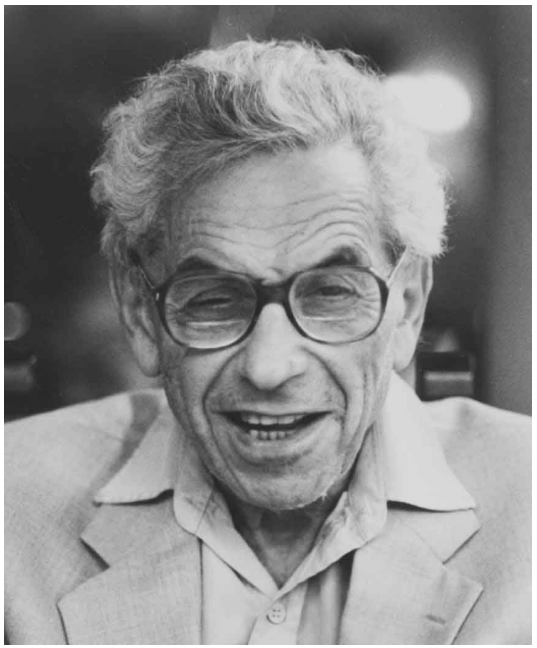
Note: The abundant numbers have density $D_s(2)$. A number of people have estimated this density, recently we learned it to 4 decimal places: 0.2476 . . .
(**Mitsuo Kobayashi**, 2011).

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

Beginning around 1935, **Paul Erdős** began studying this subject, looking for the grand result that would unite and generalize the work on Euler's function and $s(n)$, and also to look for an elementary method.

This culminated in the **Erdős–Wintner** theorem in 1939.

The Erdős–Wintner theorem gives some easily checked conditions for an arithmetic function to behave "like" $s(n)$.



Erdős

Wintner

Surely the wonderful Erdős–Wintner theorem can justify the low origins of the definition of abundant numbers!

However, their theorem does not cover some other familiar arithmetic functions, such as $\omega(n)$, which counts the number of distinct primes that divide n.

For example, $\omega(10) = 2$, $\omega(11) = 1$, $\omega(12) = 2$. What can be said statistically here?

Hardy and **Ramanujan** had shown that $\omega(n)/\ln\ln n \to 1$ as $n \to \infty$ through a set of asymptotic density 1. This is an amazing and unexpected result! What should the double natural logarithm have to do with the number of prime factors of an integer?

The connection is in a theorem of **Euler**:

$$\frac{1}{\ln\ln x} \sum_{\substack{p \le x \\ p \text{ prime}}} \frac{1}{p} \to 1 \text{ as } x \to \infty.$$

Ramanujan

Hardy

But still, if the ratio $\omega(n)/\ln\ln n$ is usually close to 1, what can be said about the difference $\omega(n) - \ln\ln n$?

The Erdős–Kac theorem (1939):

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

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

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

Mark Kac (as quoted by **Peter Elliott** in 1980):

"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."

Einstein: "God does not play dice with the universe."

Einstein: "God does not play dice with the universe."

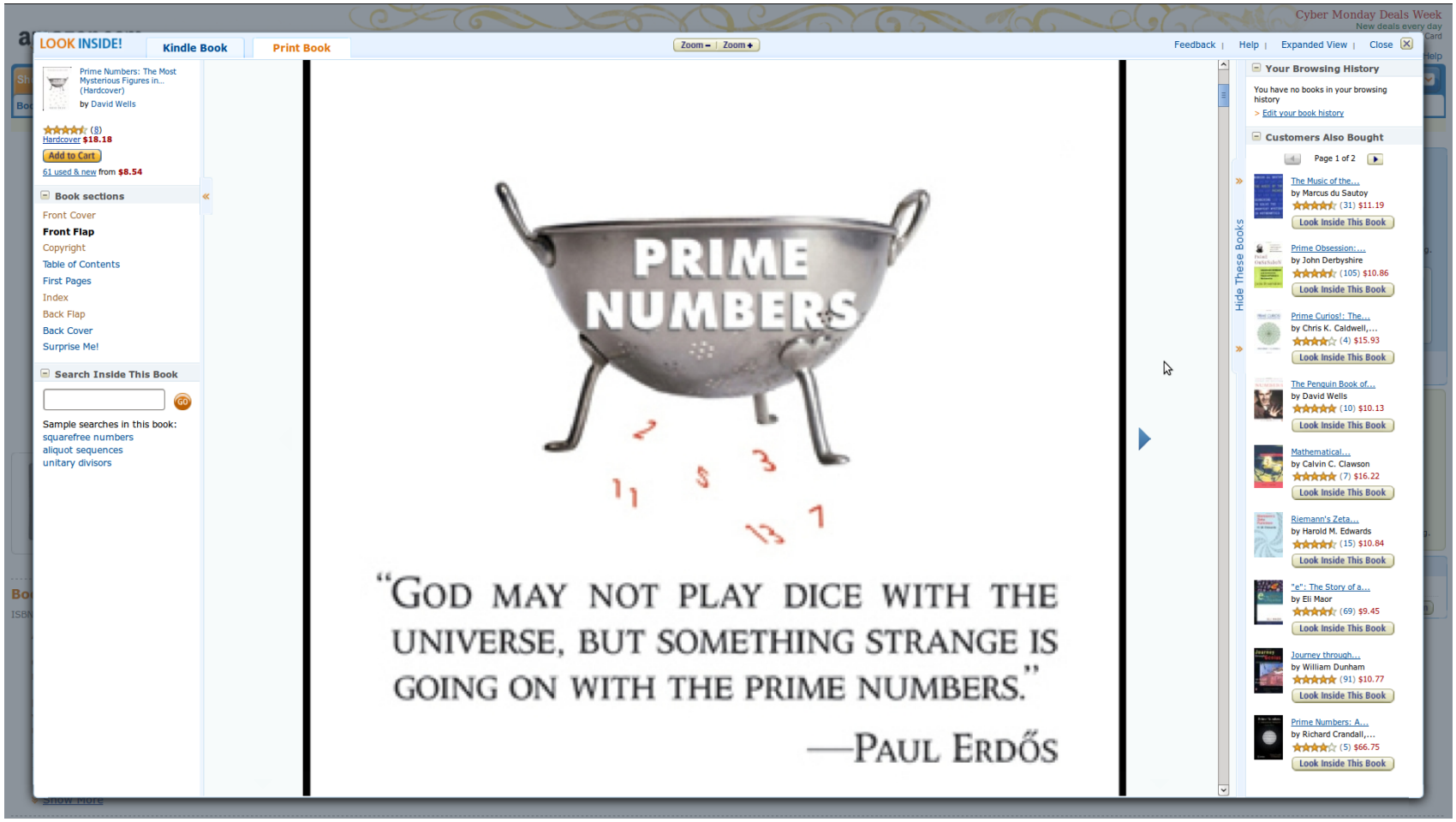
Erdős & Kac: Maybe so but something's going on with the primes.

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**



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 $\mathcal{A}(x)$ denote the number of integers in $[1, x]$ that belong to an amicable pair. We have no good lower bounds for $\mathcal{A}(x)$ 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. As a start, from Euler's result on perfect numbers being of the form pm^2 with p a prime factor of $s(m^2) + m^2$, it follows that the number of perfect numbers up to x is at most $x^{1/2} \ln x$.

However, it is far less clear that the amicable numbers have density 0, that is, if $\mathcal{A}(x)/x \to 0$ as $x \to \infty$.

This was not shown until **Erdős** did this in 1955. Currently I have the best result in this vein:

$$\mathcal{A}(x)/x \leq e^{-\sqrt{\ln x}}$$

for all large values of x.

By a calculus argument, this upper bound for $\mathcal{A}(x)$ can be used to show that the sum of the reciprocals of the amicable numbers does not diverge; that is, it is either a finite sum or a convergent infinite sum.

Let A denote the sum of the reciprocals of all of the amicable numbers.

Can we compute A to a few decimal places?

Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum A satisfies

$$A > 0.0119841556\ldots.$$

Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum A satisfies

$$A > 0.0119841556\ldots.$$

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

Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum A satisfies

$$A > 0.0119841556\ldots.$$

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

Nguyen (2014): $A < 4084$

Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum A satisfies

$$A > 0.0119841556\ldots.$$

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

Nguyen (2014): $A < 4084$

Nguyen & Pomerance (2019): $A < 215$.

Bayless

Klyve

Nguyen

Back to Pythagoras:

$s(n)$ is the sum of the proper divisors of n.

A number n is *perfect* if $s(n) = n$.

A number n is *amicable* if $s(n) = m \neq n$ and $s(m) = n$; that is, $s(s(n)) = n$, but not perfect.

So **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:

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

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

$14 \to 10 \ldots$

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

$20 \to 22 \to 14 \ldots$

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

$25 \to 6 \to 6$

$26 \to 16 \ldots$

$28 \to 28$

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

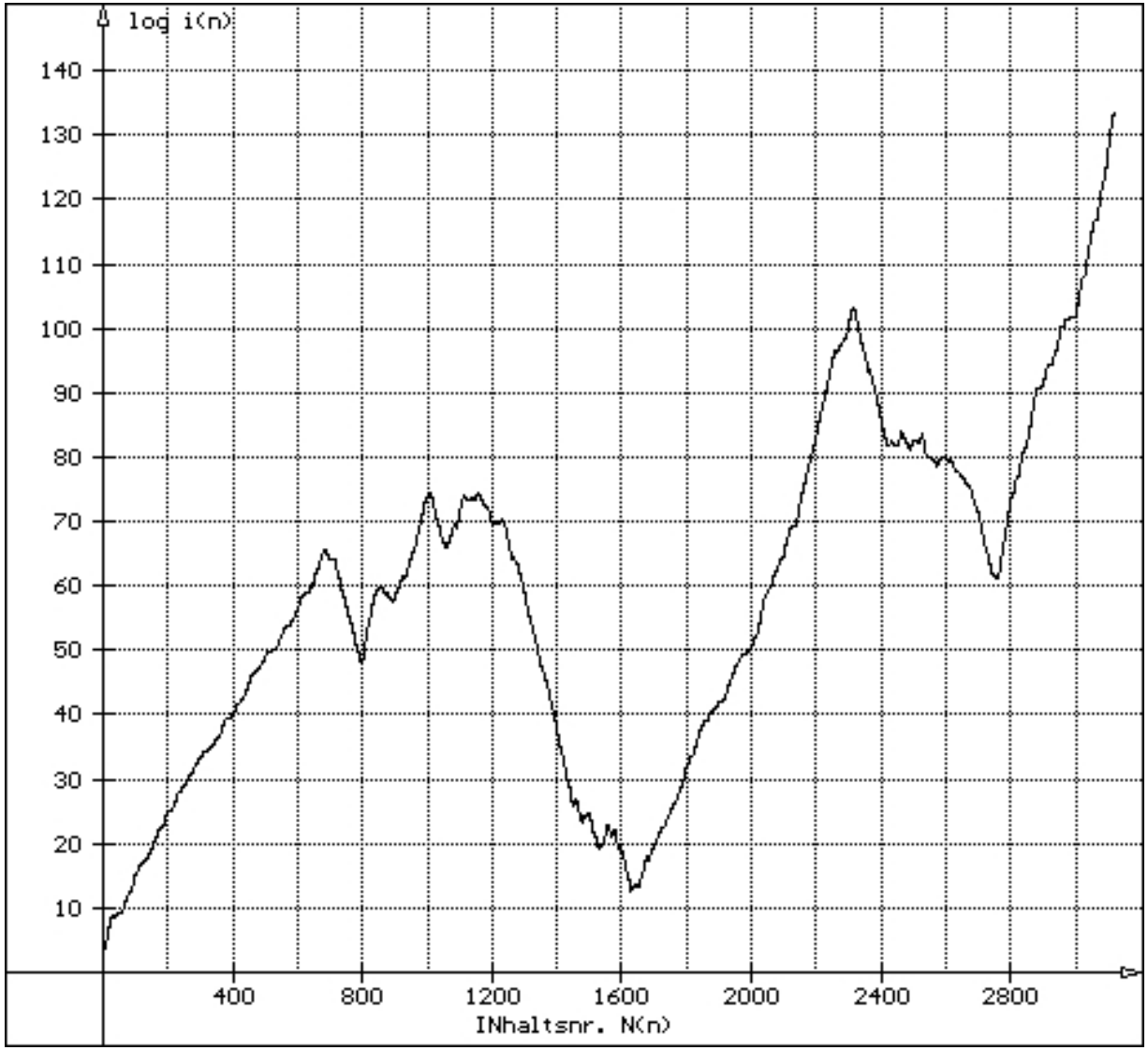
Lenstra (1975):
There are arbitrarily long increasing "aliquot" sequences

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

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.

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 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