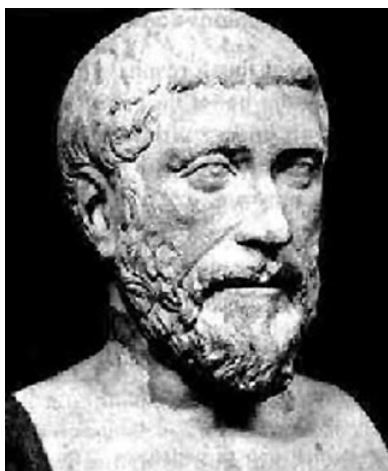# The first dynamical system

Carl Pomerance

Dartmouth College (emeritus)

University of Georgia (emeritus)

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**.

The sum-of-proper-divisors function

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 amazingly, he noticed that

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

By iterating s, Pythagoras was looking at the first dynamical system!

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.

Some problems

- Are there infinitely many perfect numbers?, amicable pairs? What can we say about their distribution?

- What can we say about the s-dynamical system?

- What can we say about the distribution of the fractions $s(n)/n$?

- What numbers are of the form $s(n)$?

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.

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:

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

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 49 Mersenne primes, the largest having exponent 74,207,281 (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 $a_0 = 4$, $a_1 = 14$, $a_2 = 194$, ..., where the rule is $a_k = a_{k-1}^2 - 2 \pmod{M_p}$. Then, for $p > 2$, M_p is prime if and only if $a_{p-2} = 0$.

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 $s(n)$ (mod n) as "random", where the event that n is perfect implies $s(n) \equiv 0$ (mod 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 $O(\log m)$ possibilities for p, once m is given. Once one of these p's is chosen, we will have $s(pm^2) \equiv 0$ (mod p), so there remains at best a $1/m^2$ chance that pm^2 will be perfect. Since $\sum (\log m)/m^2$ 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.

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.

In the 9th century, **Thābit ibn Qurra** 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. For example, the heuristic argument mentioned earlier for odd perfect numbers can be fashioned into a proof that the number of perfect numbers to x is $O(\sqrt{x} \log x)$.

13

There are much better upper bounds for the distribution of perfect numbers. The champion result is due to **Hornfeck** and **Wirsing**: the number of perfect numbers in $[1, x]$ is at most $x^{o(1)}$. (The "$o(1)$" is of the shape $c/\log\log x$.)

But amicables form a larger set, maybe much larger.

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

His insight: the smaller member of an amicable pair is *abundant* (meaning $s(n) > n$), the larger is *deficient* (meaning $s(m) < m$). Thus, we have an abundant number with the sum of its proper divisors being deficient.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

P (2014): $\mathcal{A}(x) \leq x/\exp((\log x)^{1/2})$, 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 A satisfies

$$A > 0.0119841556\ldots.$$

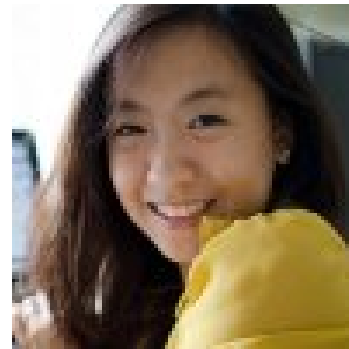So, what is this sum of reciprocals? Using a complete roster of all amicables to 10^{14} we can show the reciprocal sum A satisfies

$$A > 0.0119841556\dots.$$

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

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

$$A > 0.0119841556\ldots.$$

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

Nguyen (2014): $A < 4084$

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:

$10 \rightarrow 8 \rightarrow 7 \rightarrow 1$

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

$14 \rightarrow 10 \ldots$

$18 \rightarrow 21 \rightarrow 11 \rightarrow 1$

$20 \rightarrow 22 \rightarrow 14 \ldots$

$24 \rightarrow 36 \rightarrow 55 \rightarrow 17 \rightarrow 1$

$25 \rightarrow 6 \rightarrow 6$

$26 \rightarrow 16 \ldots$

$28 \rightarrow 28$

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

$\vdots$

If p, q are different primes and $n = p + q + 1$, then $n = s(pq)$ is a value of s. A slightly stronger form of **Goldbach**'s conjecture implies that every even number starting with 8 is the sum of two different odd primes p, q, so this conjecture implies that starting from any odd number $n \geq 9$ there is an infinite sequence $n = n_0 < n_1 < n_2 < \ldots$, where $s(n_i) = n_{i-1}$.

In 1990, Erdős, Granville, P, & Spiro showed that this argument works for "almost all" odd numbers n. In particular there are arbitrarily long decreasing "aliquot" sequences.

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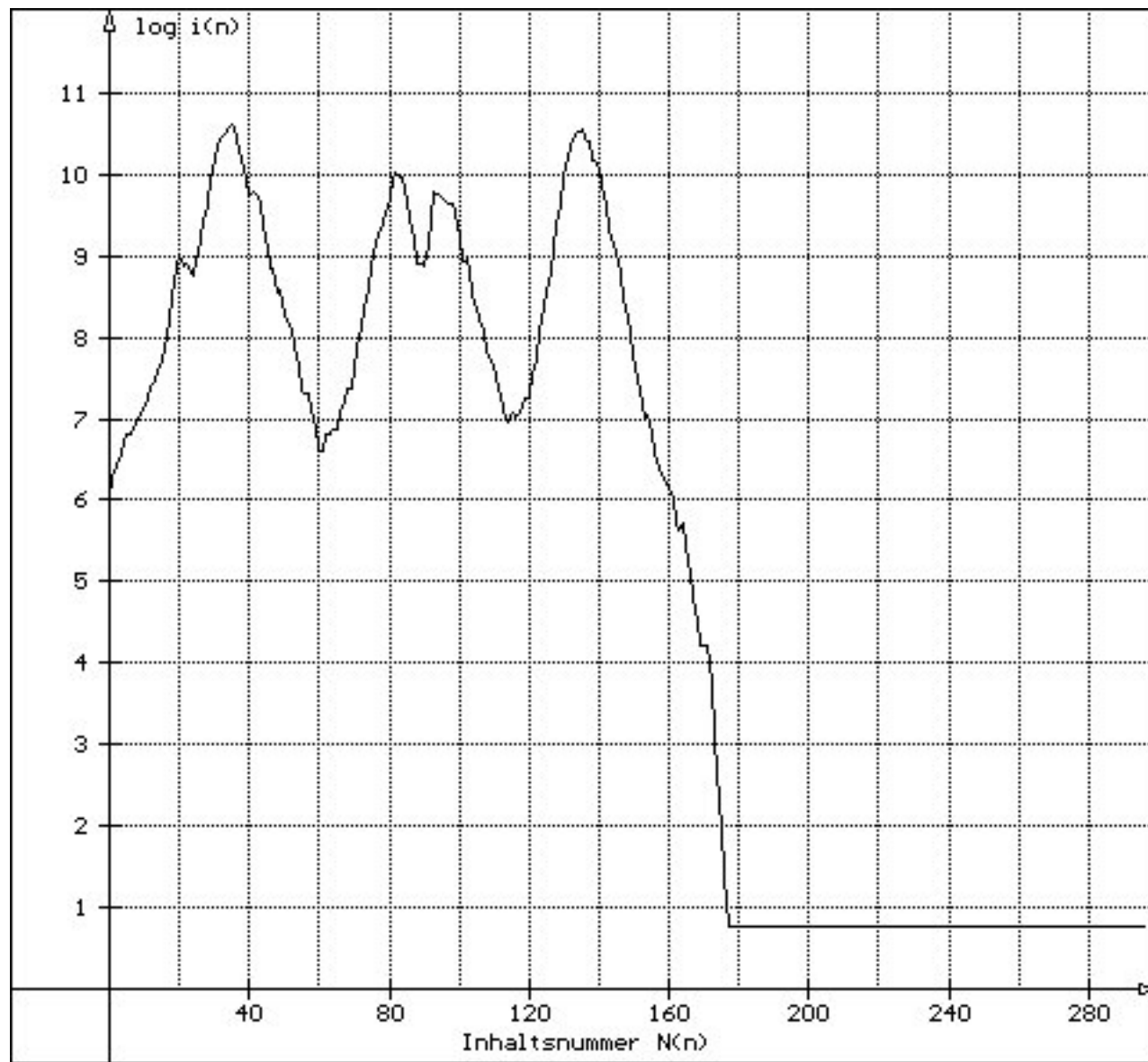
Nevertheless, we have the **Catalan–Dickson conjecture:**
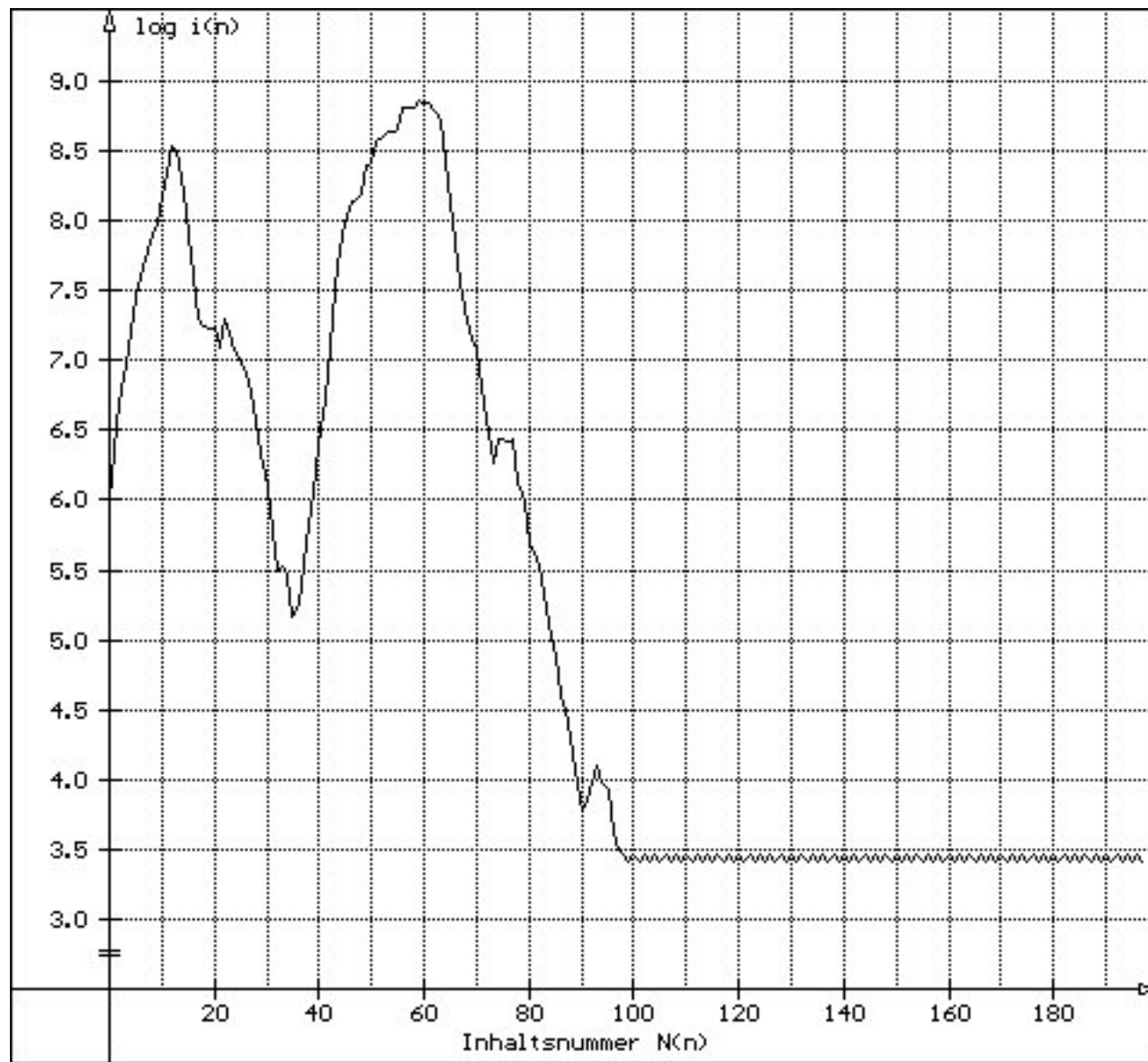*Every aliquot sequence is bounded.*

Some of the extensive calculations in computing orbits are summed up in these graphs taken from `aliquot.de` maintained by **Wolfgang Creyaufmüller**.
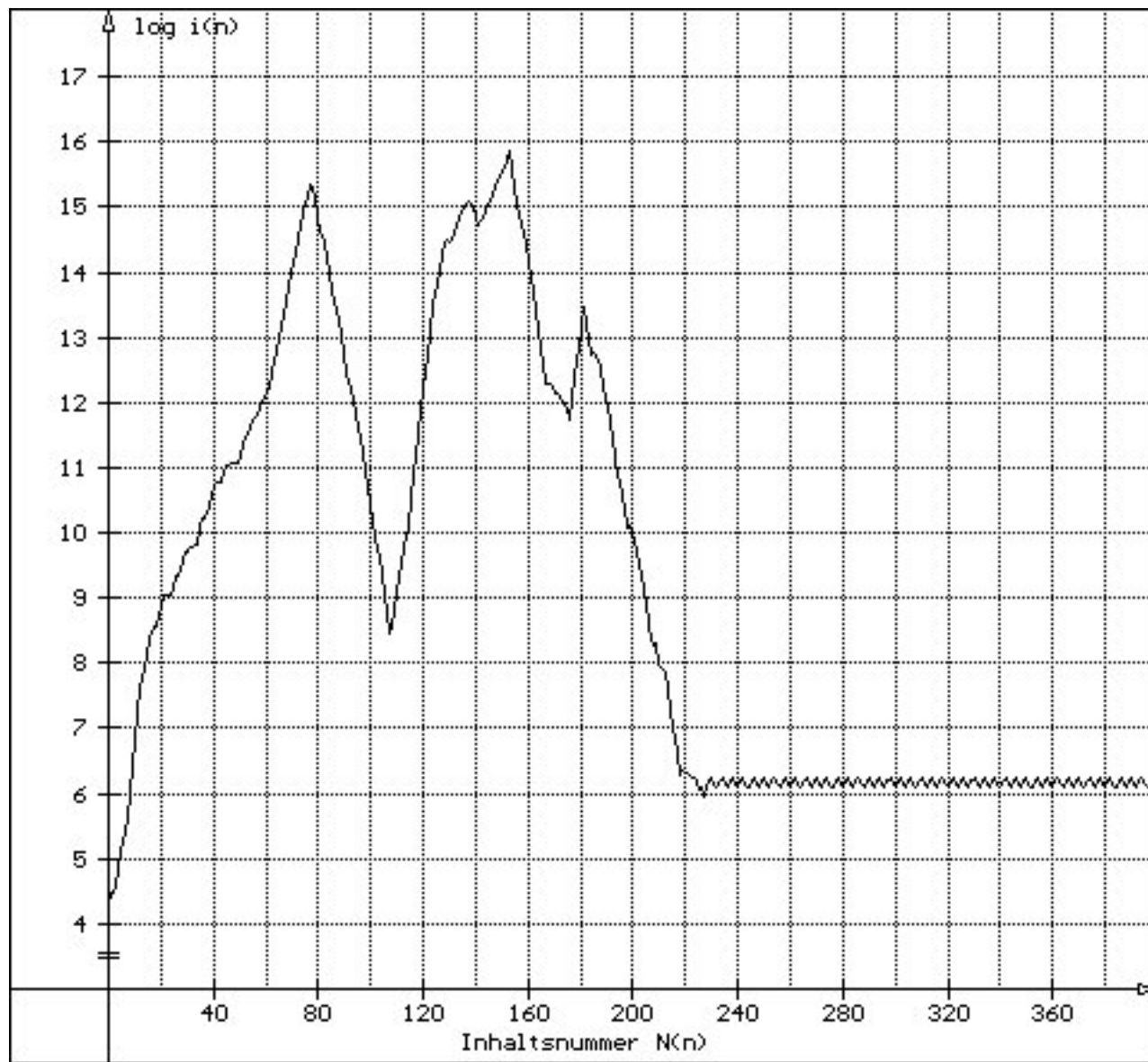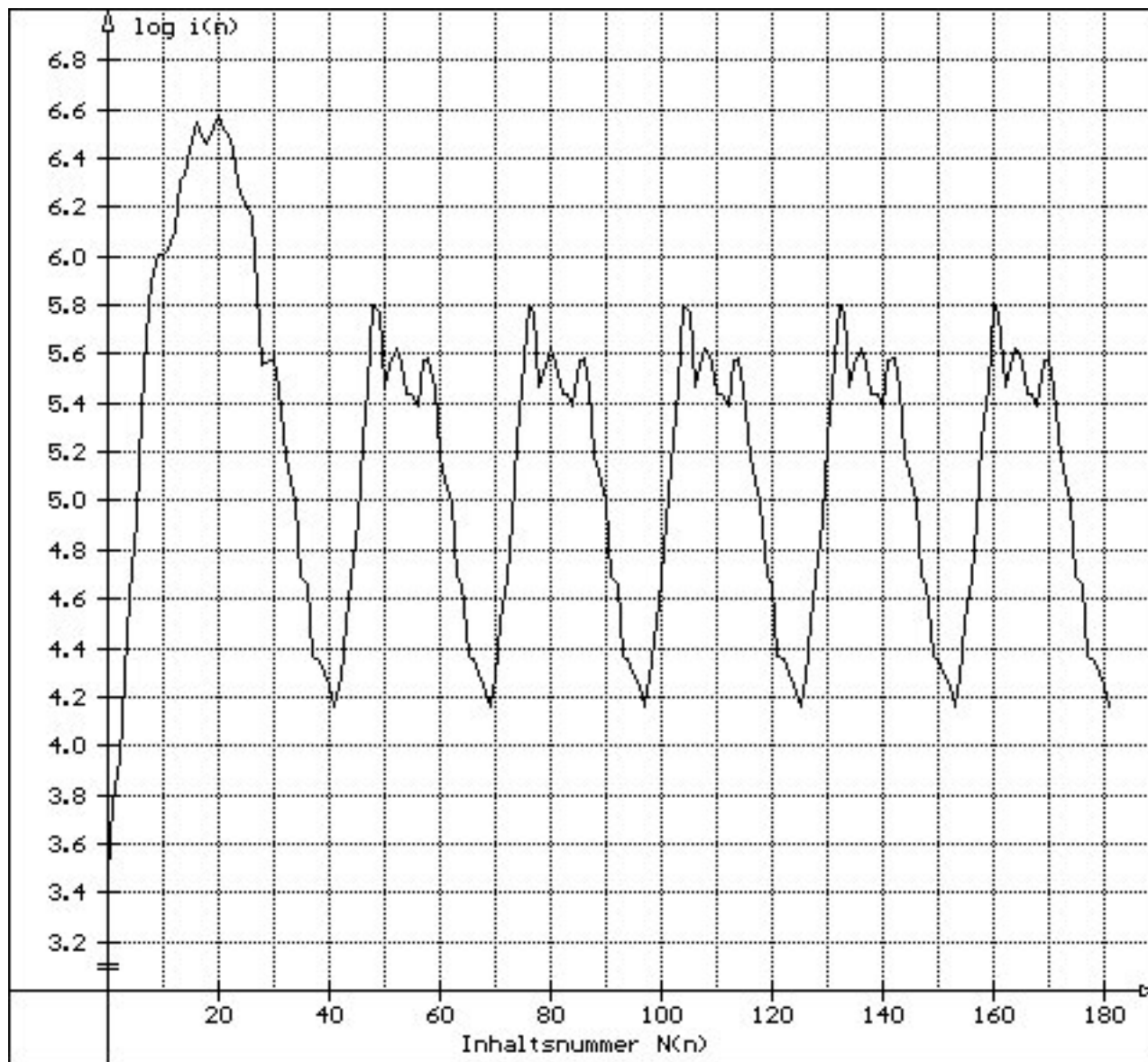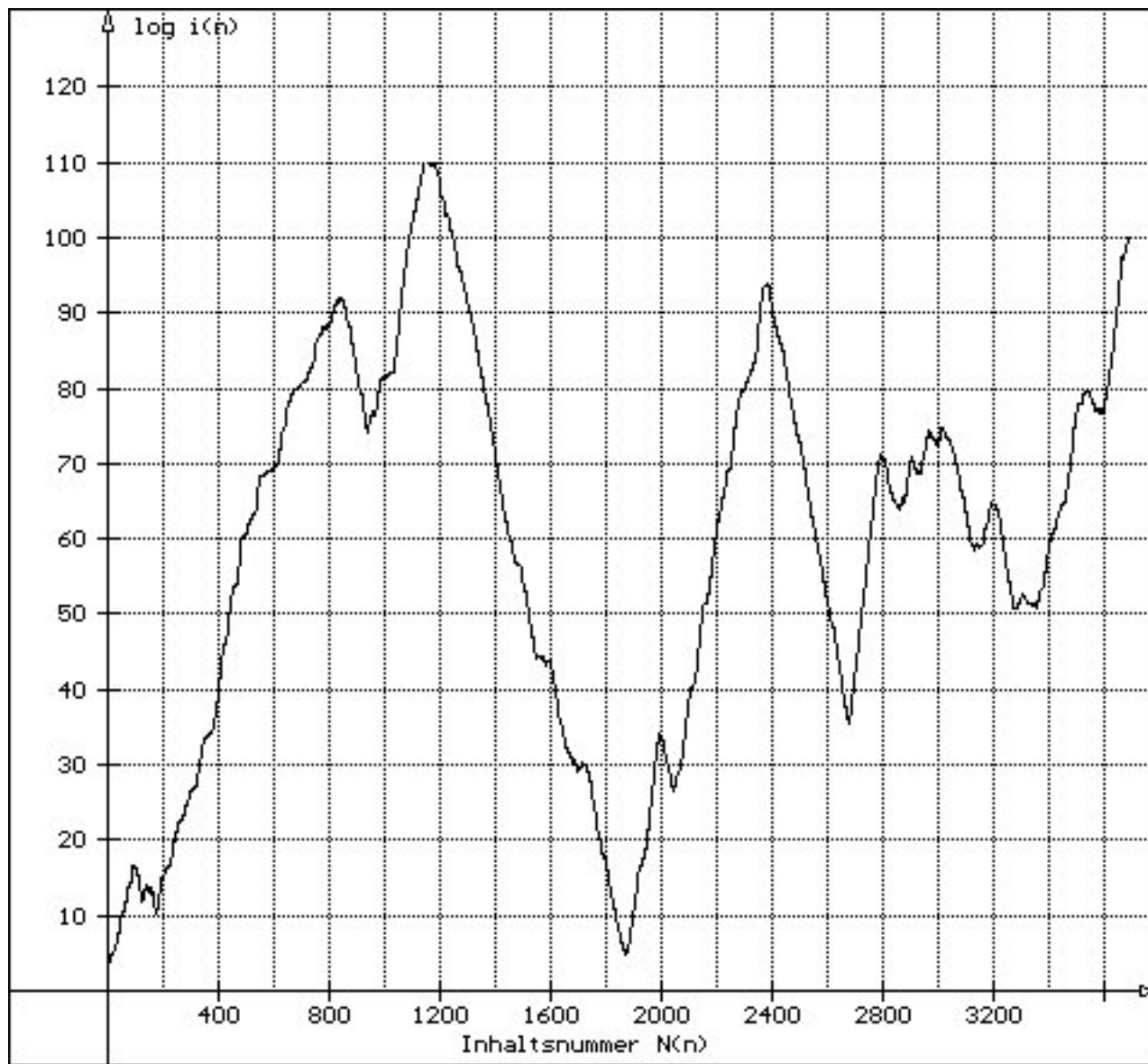
840

976950

980460

31

17490

32

2856

1578

34

276
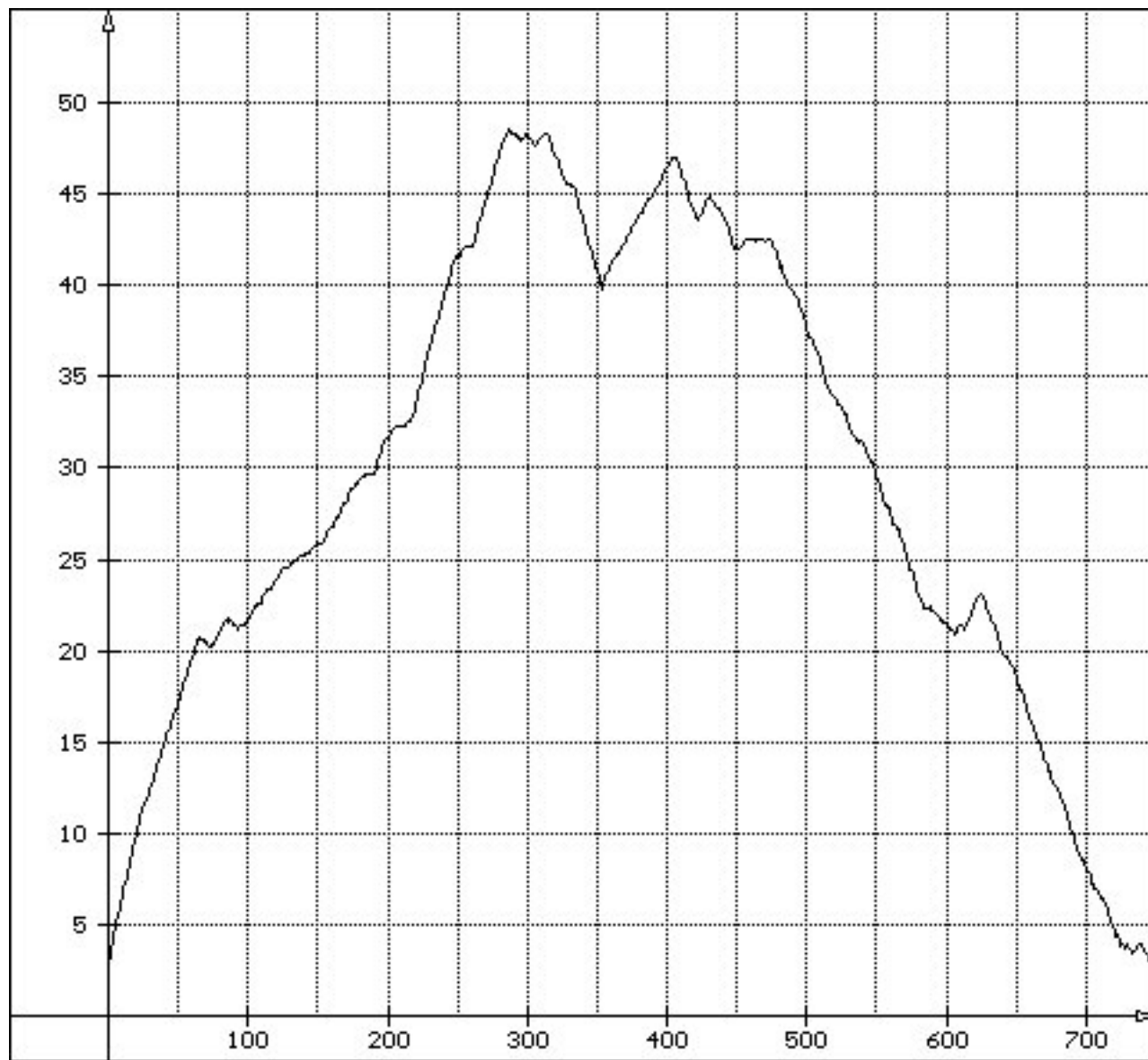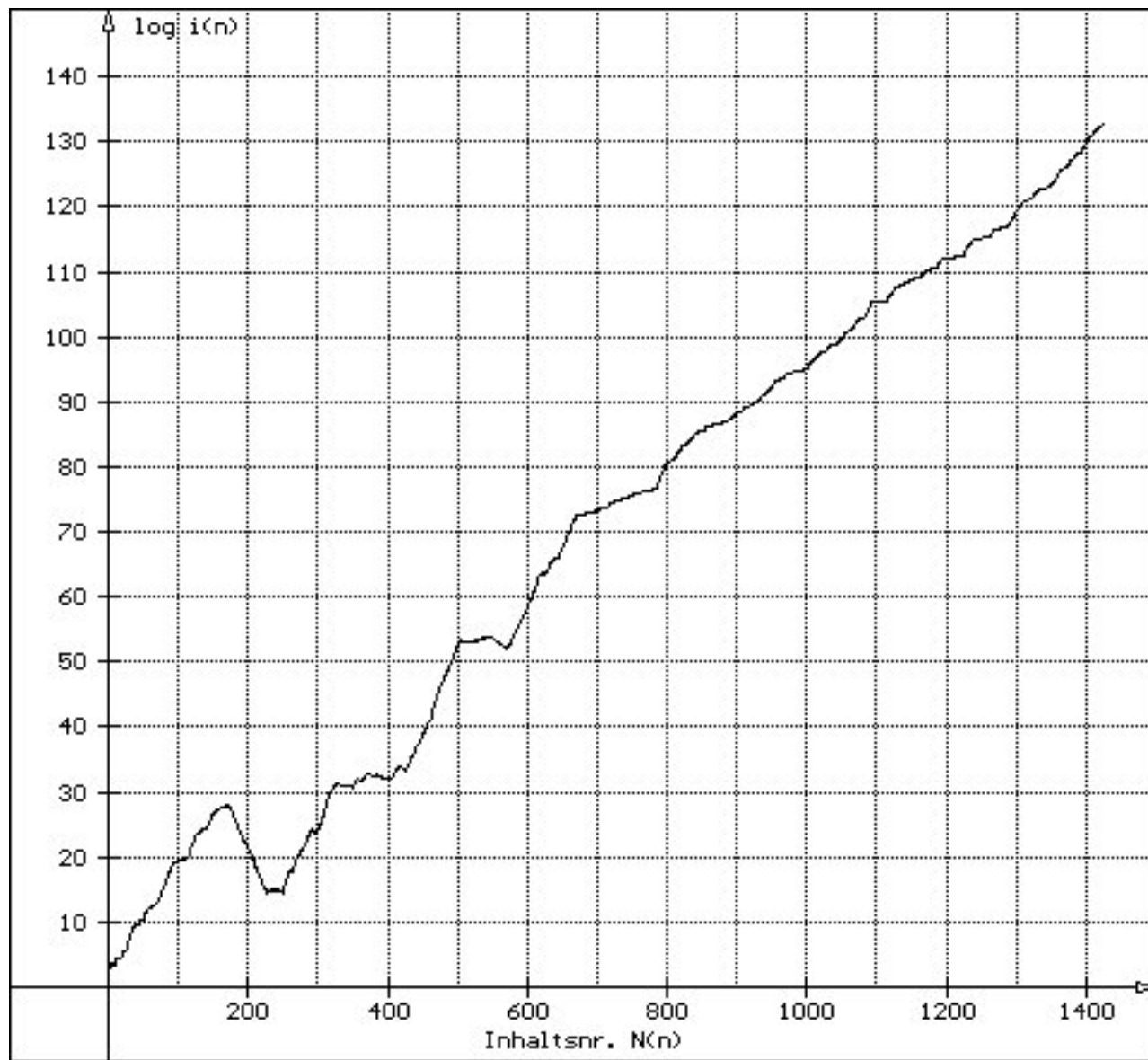
There are 5 orbits starting below 1000 where it's not clear what's happening:

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

known as the "**Lehmer** five".

The Guy & Selfridge counter conjecture:
For almost all even n, the aliquot sequence starting with n is unbounded.

D. H. Lehmer
(1905–1991)

R. K. Guy
(1916–)

J. L. Selfridge
(1927–2010)

Recently **Bosma** did a statistical study of aliquot sequences with starting numbers below 10^6. About one-third of the even starters are still open and running beyond 10^{99}. Evidence for **Guy–Selfridge**? But: he and **Kane** found the geometric mean of the ratios $s(2n)/2n$ asymptotically, finding it slightly below 1. Evidence for **Catalan–Dickson**?

P, 2016:

- *The asymptotic geometric mean of the ratios $s(s(2n))/s(2n)$ is the same as for $s(2n)/2n$.*

- *Assuming a conjecture of **Erdős, Granville, P, & Spiro**, for each fixed k, there is a set A_k of asymptotic density 1 such that the asymptotic geometric mean of $s_k(2n)/s_{k-1}(2n)$ on A_k is the same as for $s(2n)/2n$ on all n.*

The conjecture mentioned:

If E has asymptotic density 0, so does $s^{-1}(E)$.

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-cycles, 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? The **Erdős** result on increasing aliquot sequences shows this if one restricts to cycles of bounded length. Recently, **Kobayashi, Pollack, & P** showed that apart possibly from sociable numbers that are odd and abundant, they have density 0. Further, we computed that the density of odd abundant numbers, whether or not they are sociable, is about 0.002.

Earlier we met *abundant* numbers $(s(n) > n)$ and *deficient* numbers $(s(n) < n)$. These terms were defined by **Nicomachus** in the 1st century. More generally, one can ask about

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

for each nonnegative real number u. Does this set have an asymptotic density? If so, how does it vary as u varies?

The question was first posed for $u = 1$ by **Erich Bessel-Hagen** in 1929.

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

Bessel-Hagen   Schoenberg   Davenport

42
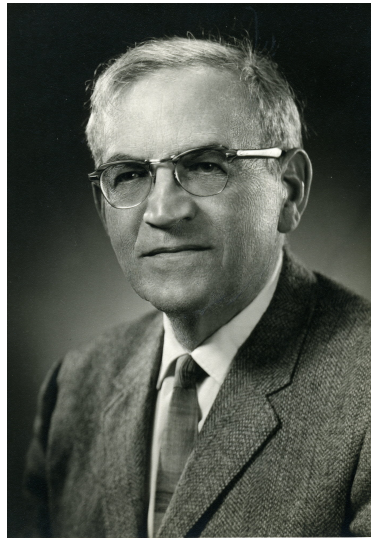
A number of people have estimated $D(1)$, the density of the abundant numbers; recently we learned it to 4 decimal places: $0.2476\ldots$
(**Mitsuo Kobayashi**, 2011).

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 great theorem that would unite and generalize the work on Euler's function and s, and also to look for an elementary method.

This culminated in the **Erdős–Wintner** theorem in 1939 (with echoes from **Kolmogorov**):

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

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

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

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 $\omega(n) - \log\log n$.
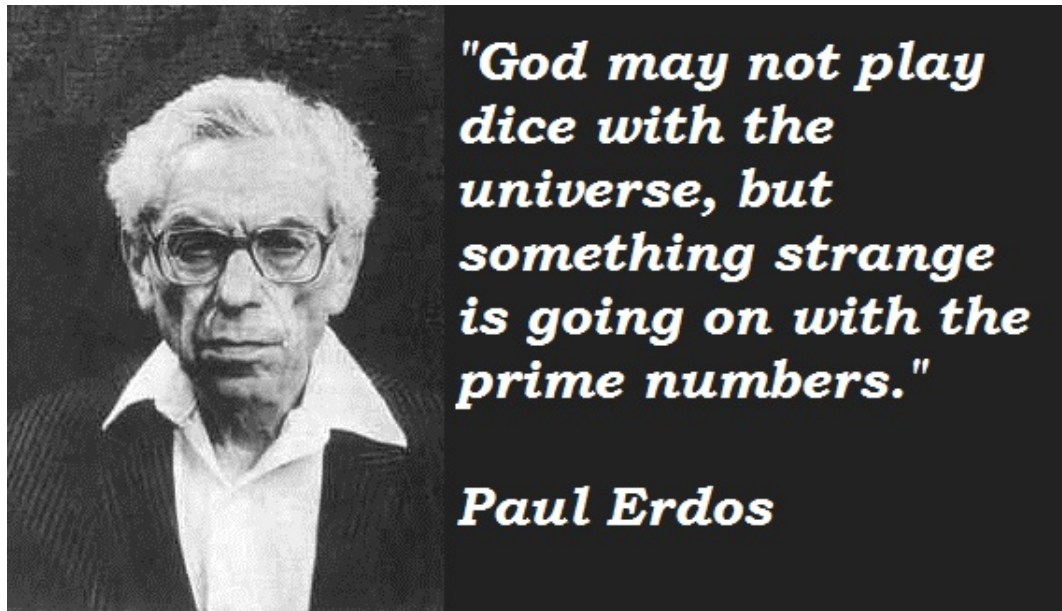
Ramanujan

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!

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

Paul Erdos

(!)

Kac

In 1973, **Erdős** considered the range of $s(n)$: Which integers m are in the form $s(n)$? He showed that

- Almost all odd numbers are of the form $s(n)$. (As mentioned earlier, in 1990, Erdős, et al. showed that almost all odd numbers are values of every iterate of s.)

- There is a positive proportion of even numbers not in the range.

In 2014 **Luca** and **P** showed that a positive proportion of even numbers *are* in the range, and the same goes for any residue class.

Last year, **Pollack** and **P** gave a heuristic argument for the density of the range of s. The heuristic is based on the theorem that for a given positive integer a, we have, apart from a set of density 0, that $a \mid n$ if and only $a \mid s(n)$. Further, the ratio $s(n)/n$ is usually closely determined by the small prime factors of n. Assuming randomness otherwise, we came up with the expression

$$\lim_{y \to \infty} \frac{1}{\log y} \sum_{\substack{a \leq y \\ 2 \mid a}} \frac{1}{a \, e^{a/s(a)}}$$

for the density of integers not in the range of s. This limit is not so easy to compute, but the value of the expression at $y = 2 \cdot 10^{10}$ is about 0.171822, while the frequency of numbers not in the range to 10^{10} is about 0.168187. (**Anton Mosunov** just computed the density at 10^{12}: it's $\approx 0.171128(!)$)

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 studying the Pythagoras function $s(n)$ 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!