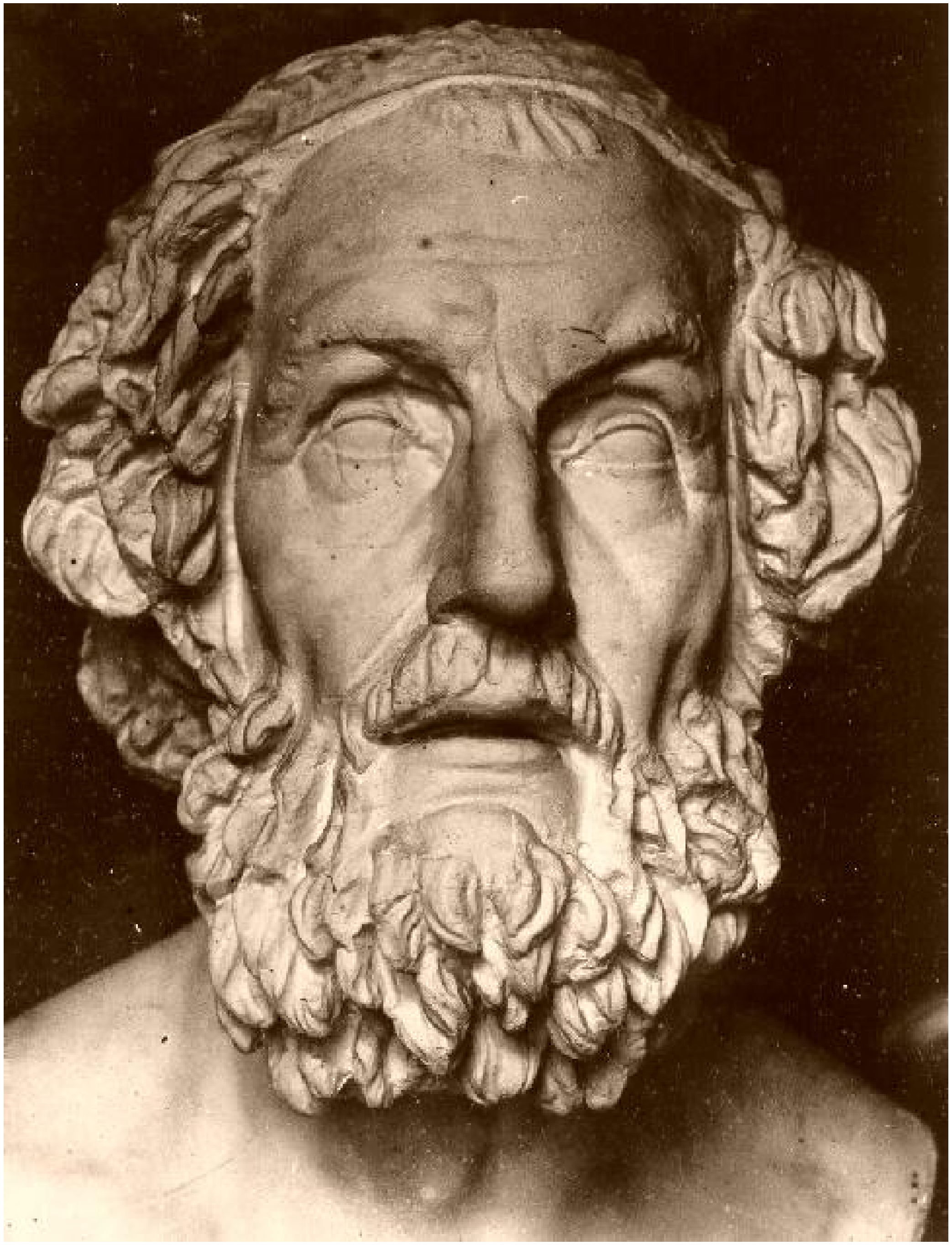
Sociable numbers

Carl Pomerance, Dartmouth College

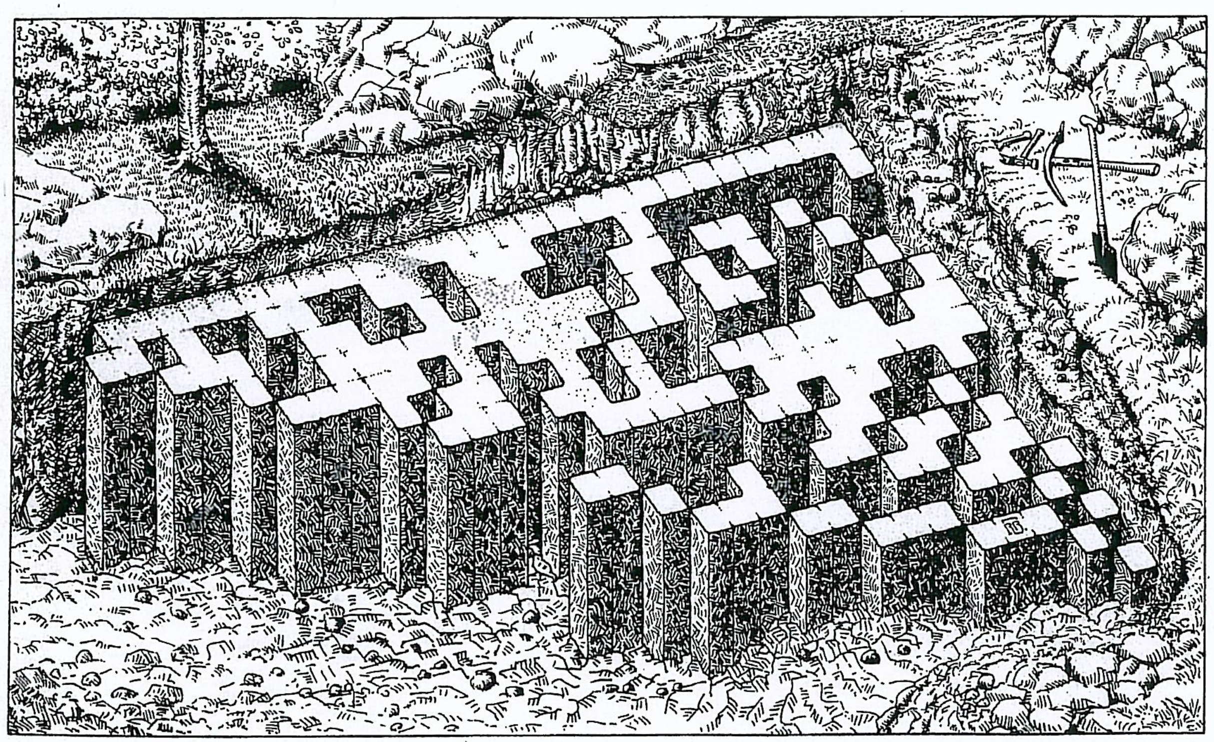
with

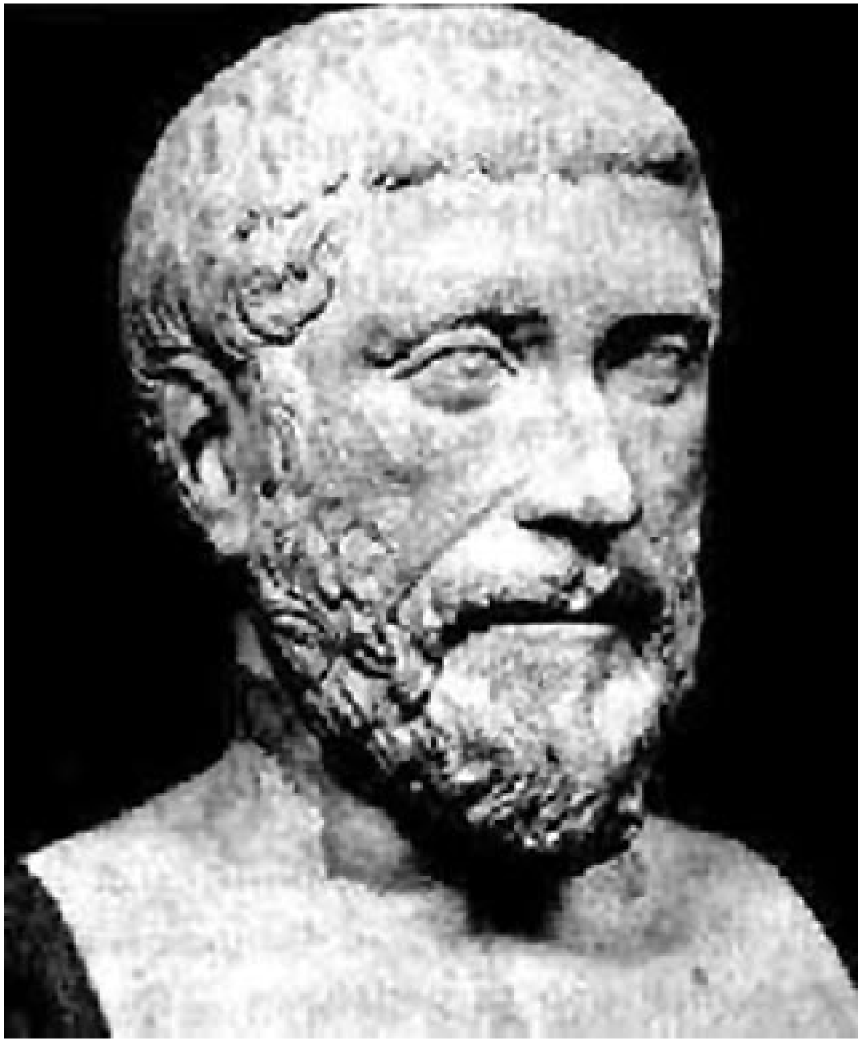
Mitsuo Kobayashi, Dartmouth College

Paul Pollack, University of Illinois, Urbana



Homer





Pythagoras

Sum of proper divisors

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

Thus, $s(n) = \sigma(n) - n$, 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.

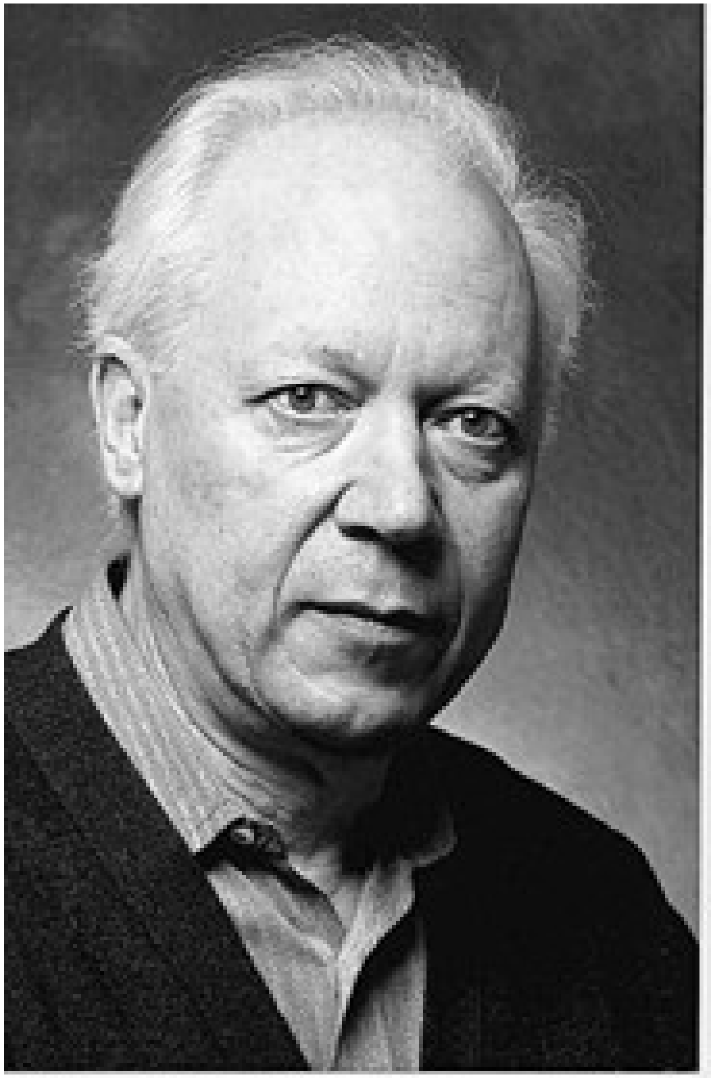
Pythagoras:

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

and 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.)



Enrico Bombieri

In 1976, 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

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.

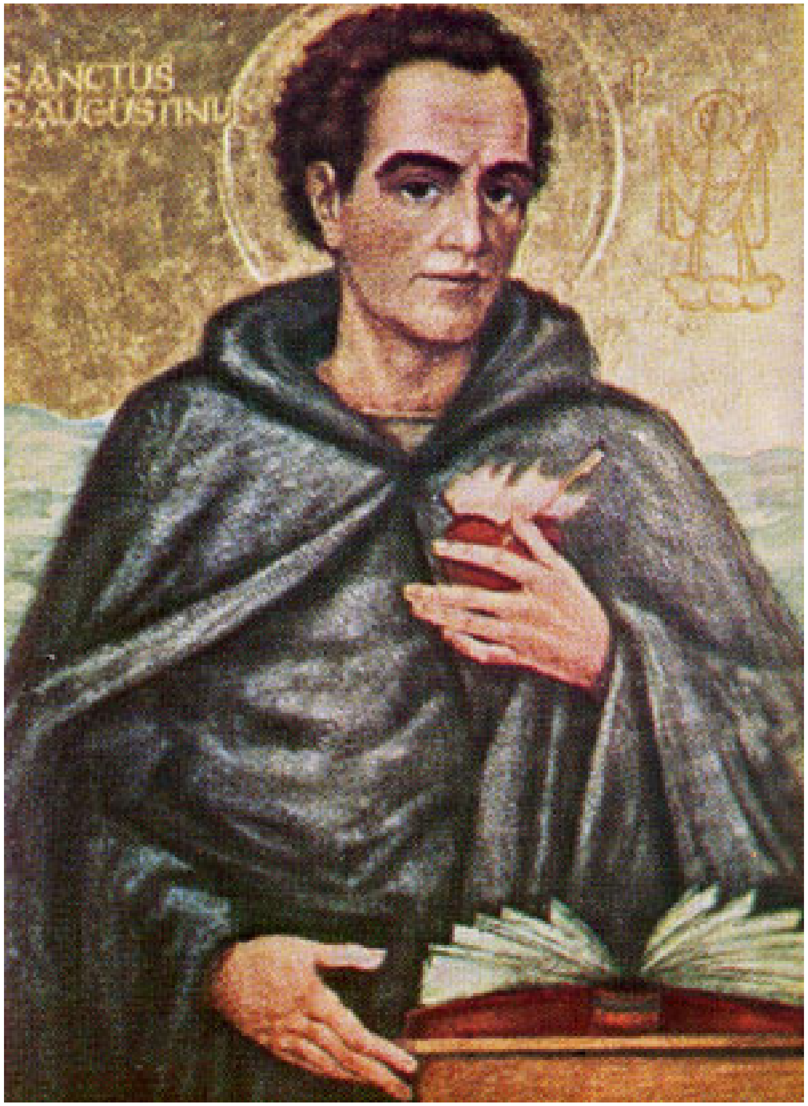
The good problem: Why do the planets wander through the constellations in the night sky?

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

Historically, perfect numbers, amicable numbers, and topics like these (figurate numbers, e.g.) were important to the development of elementary number theory. So, perhaps it could be argued that they were “good” problems, in the sense of Hoyle.

Sadly, I must agree with Bombieri that these topics are perhaps not of great interest *now* to the advancement of number theory. Yet, they and their brethren continue to fascinate. Let us throw mathematical propriety out the window and revel a bit in this quite unfashionable subject!

For they are fascinating to more than just number theorists. . .



St. Augustine

In the bible?

St. Augustine, ca. 1600 years ago in "City of God":

" 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."

It was also noted that 28, the second perfect number, is the number of days in a lunar month. A coincidence? Numerologists thought not.

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 . . .)


Euclid teaching

Euclid, ca. 2300 years ago:

"If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect."

For example: $1 + 2 + 4 = 7$ is prime, so $7 \times 4 = 28$ is perfect.

That is, if $1 + 2 + \cdots + 2^k = 2^{k+1} - 1$ is prime, then $2^k(2^{k+1} - 1)$ is perfect.

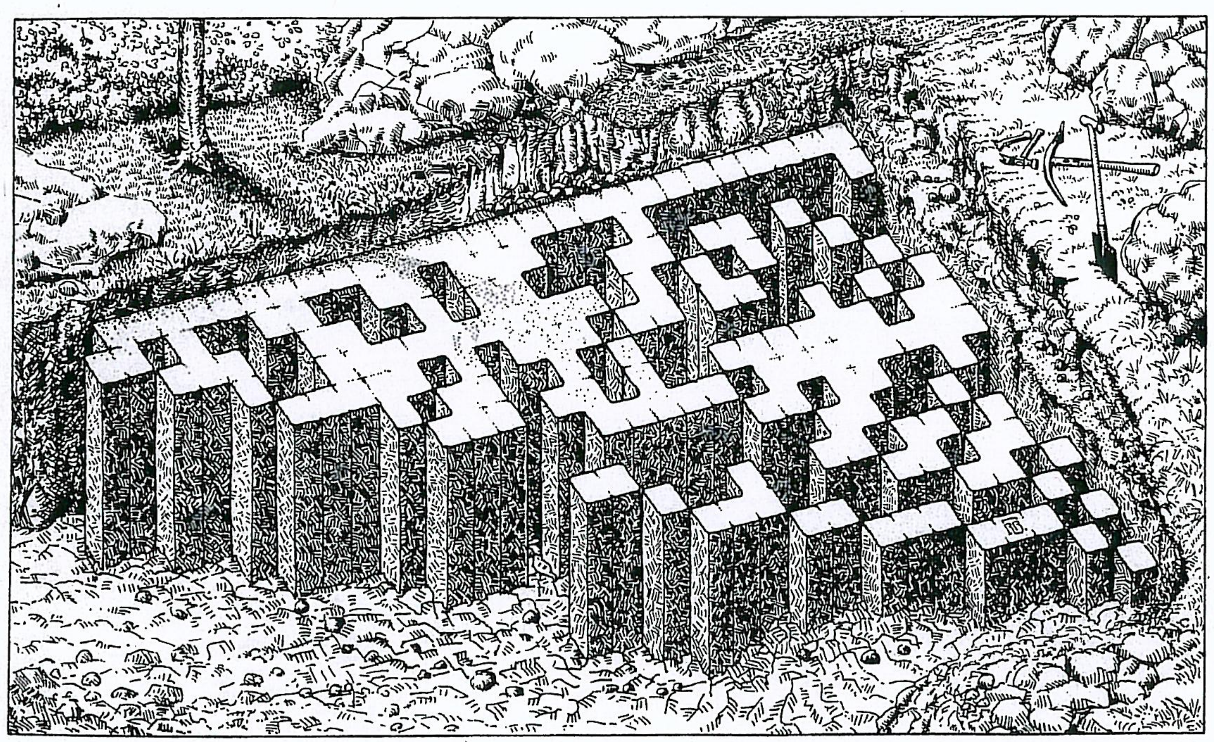
For example, take $k = 43{,}112{,}608$.

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

If $2^{k+1} - 1$ is prime, so too is $k + 1$, but not always conversely.

Exponents p with $2^p - 1$ prime:

2, 3, 5, 7, 13, 19, 31, 61, ..., 43,112,609, ...



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."

Abundant numbers are like an animal with *"ten mouths, or nine lips, and provided with three lines of teeth; or with a hundred arms, or having too many fingers on one of its hands..."* while with deficient numbers, *"a single eye,..., or if he does not have a tongue."*

Actually, Nicomachus only defined deficient and abundant for even numbers, since he likely thought all odd numbers are deficient. However, 945 is abundant; it is the smallest odd abundant number.

Nicomachus conjectured that there are infinitely many perfect numbers and that they are all given by the Euclid formula. Euler, ca. 250 years ago, showed that all *even* perfect numbers are given by the formula. We still don't know if there are infinitely many, or if there are any odd perfect numbers.

Euler

Eugène Catalan

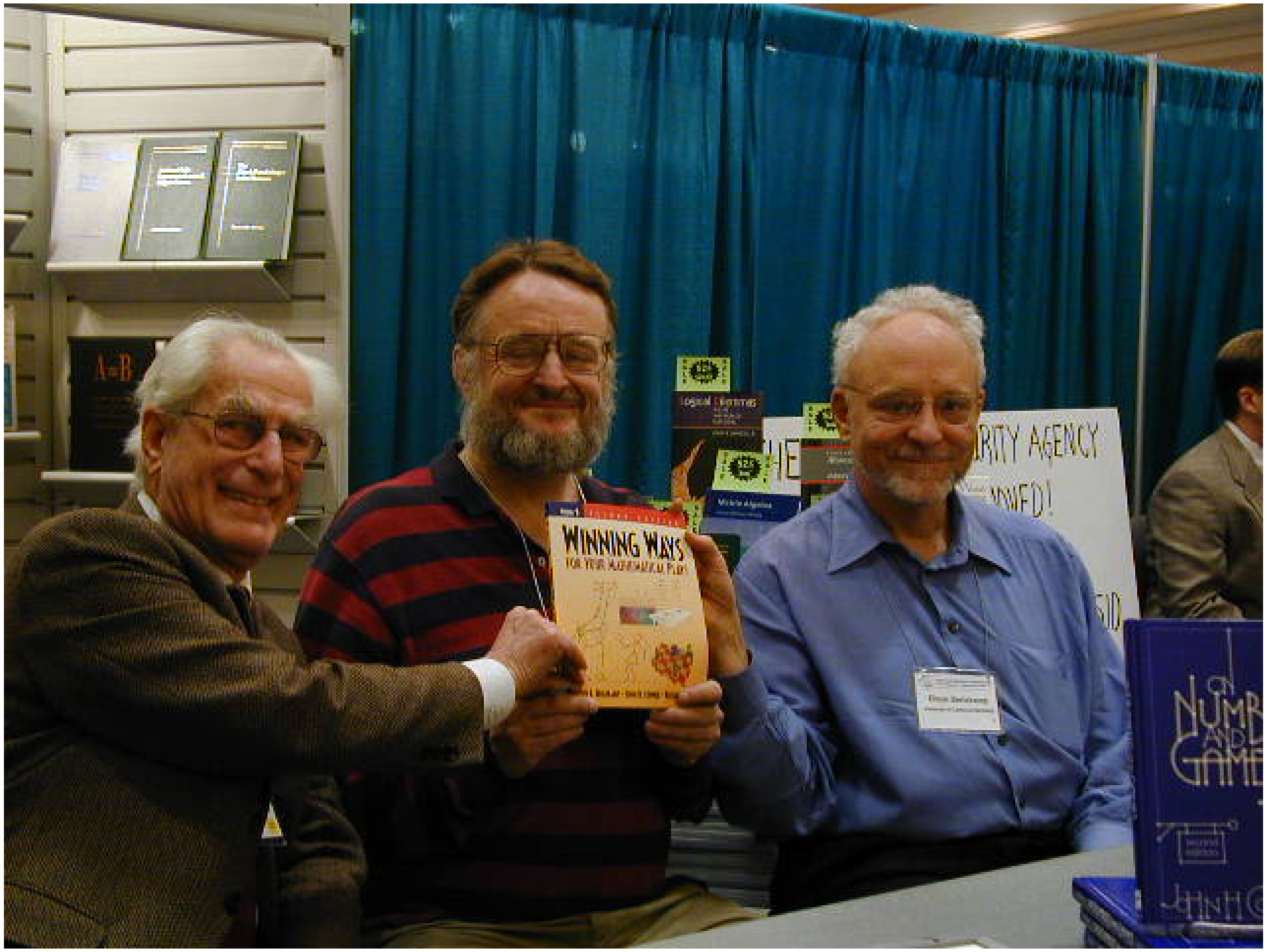

Leonard Dickson

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

$$s(n_1) = n_2, \quad s(n_2) = n_3, \quad \dots \ , \quad s(n_k) = n_1,$$

where $n_1, n_2, \dots, n_k$ are distinct. We say these numbers form a *sociable* cycle of length k, and that they are *sociable* numbers 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; it is 1,264,460.)

We know 46 perfect numbers and about 12 million amicable pairs.

A modern perspective on these problems: what can we say about their distribution in the natural numbers, in particular, do they have density 0?

What do you think is the density of the sociable numbers?

Up to 100 the only sociable numbers are the perfect numbers 6 and 28, so $N(100) = 2$ and $N(100)/100 = 0.02$.

Up to 1000 we pick up the perfect number 496 and the Pythagorean amicables 220 and 284. So $N(1000) = 5$ and $N(1000)/1000 = 0.005$.

Up to 10,000 we pick up the perfect number 8128 and the amicable pairs

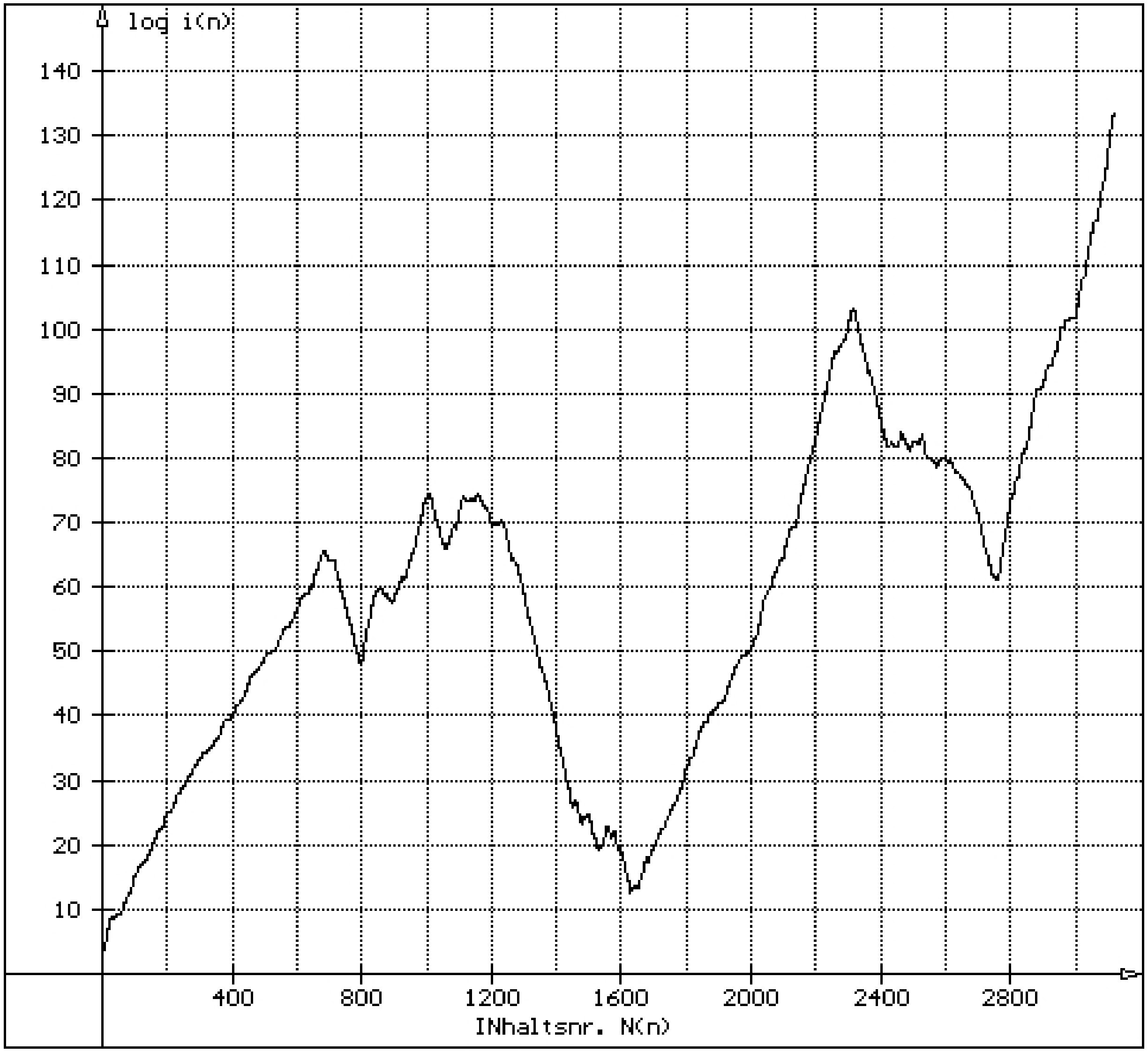
$$1184,\ 1210;\quad 2620,\ 2924;\quad 5020,\ 5564;\quad 6232,\ 6368.$$

(The first was found by Paganini in 1860, the others by Euler.) So $N(10{,}000) = 14$ and $N(10{,}000)/10{,}000 = 0.0014$.

Are we sure we have the counts right? These are the correct counts for perfects and amicables, and also for sociables of order at most 600.

In fact, there are 81 starting numbers below 10,000 where we have iterated $s(n)$ over 600 times, and it is not yet clear what is happening. Some of these are known *not* to be sociable, for example the least number in doubt, 276. (It is not sociable because it is not in the range of the function s.) But some of them might end up being sociable after travelling a very long distance through its s-chain. The least such possibility is 564.

So, we are having trouble even computing $N(1000)$ much less showing the sociable numbers have density 0.



564 iteration

How are we able to get as far as we have? One can see in the chart that more than 100 numbers with more than 100 digits have been factored, and the largest few have more than 120 digits.

These numbers have presumably not been given to us by an adversary who wants to make life especially difficult. They might be called *natural* natural numbers.

And, the workhorse algorithm for such numbers, which exploits the number of points on varieties, is the Elliptic Curve Method of Lenstra.

Hendrik Lenstra

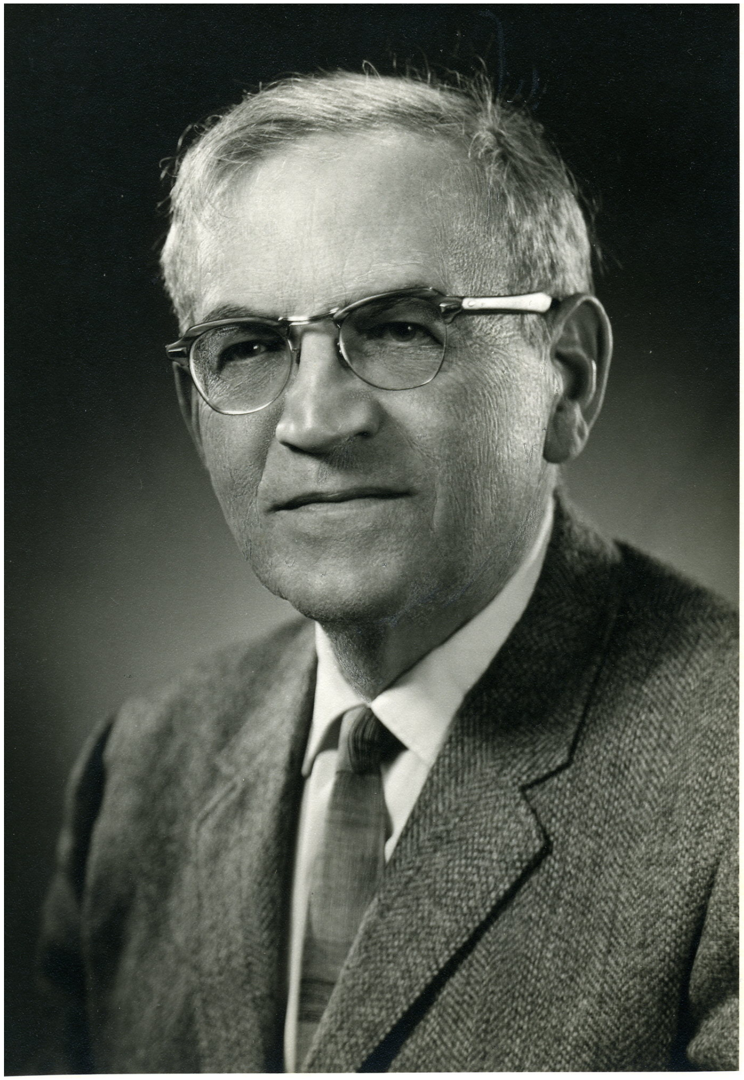
From work of Descartes and Euler, it is not hard to see that perfect numbers are sparsely distributed within the natural numbers; that is, they have density 0. It is instructive though to look at a result of Davenport from 1933 that implies the same.

For each real number $u > 0$, let $\mathcal{D}_s(u)$ denote the set of natural numbers n with $s(n)/n \le u$. Davenport proved that $\mathcal{D}_s(u)$ has a positive density $D_s(u)$ within the natural numbers; properties for the function $D_s(u)$ include

$$\text{continuous}, \quad \text{strictly increasing}, \quad D_s(0+) = 0, \quad D_s(+\infty) = 1.$$

Note that continuity implies that the perfect numbers have density 0.

Harold Davenport



I. J. Schoenberg

Davenport was preceded by Schoenberg in 1928 who had analogous results for Euler's function. Later, Erdős and Wintner considered general multiplicative functions. This (and the Turán proof of the Hardy–Ramanujan theorem) was the dawn of the field of *probabilistic number theory*.

The Davenport distribution result also implies that the deficient numbers ($s(n)/n < 1$) and the abundant numbers ($s(n)/n > 1$) have positive densities. From the very start, people were interested in computing these densities, especially since it seemed that the even numbers are about equally split between abundant and deficient. After work of Behrend in the 1930's, Wall et al. in the 1970's, Deléglise in the 1990's, and now Kobayashi, we know that the density of the abundant numbers is ≈ 0.2476.

Mitsuo Kobayashi

Herman te Riele

But what of the density of amicable numbers or more generally, sociable numbers?

In January 1973, te Riele published an example of a number n such that the sequence $n, s(n), s(s(n)), \ldots$ is strictly increasing for more than 5092 steps. At the end he remarks that Lenstra communicated a proof to him that for every k there is some number n, with the sequence $n, s(n), s(s(n)), \ldots$ strictly increasing for at least k steps. I believe this is the earliest citation of a result of Lenstra.

In 1975, Lenstra published this assertion as a problem in the *American Mathematics Monthly*. Here is his solution from the *Monthly* in 1977.

Lemma. *Suppose* $n = abm$ *where* a, b, m *are pairwise coprime and* $a^2 \mid \sigma(b)$*. Then* $s(n) = am'$*, where* a, m' *are coprime.*

Proof. We have $a^2 \mid \sigma(n)$ and $a, n/a$ are coprime. Thus $a \mid \sigma(n) - n = s(n)$, and $s(n)/a$ is coprime to a. $\square$

Say we apply this to $a = 12$ and a number b coprime to 12 and such that $12^2 \mid \sigma(b)$. For example, choose b as a prime $\equiv -1 \mod 12^2$, or more easily, choose $b = 5^{47}$ (since $\sigma(5^{47}) = (5^{48} - 1)/4$). Then, for every number m coprime to ab, we have $abm = n < s(n) < s(s(n))$, since $12 \mid n$ and $12 \mid s(n)$.

This can be continued to the next step as follows. Choose c coprime to ab with $(ab)^2 \mid \sigma(c)$. (So, c could be a prime that's $-1 \mod (ab)^2$, or an appropriate power of 7, or something else.) Then let $n = abcm$, where m is coprime to abc.

By the lemma, $s(n) = abm'$ where m' is coprime to ab, so $s(n)$ begins a climb of length at least 2. But $a = 12$ divides n, so $n < s(n)$.

Next, choose d coprime to abc with $(abc)^2 \mid \sigma(d)$ and consider numbers $n = abcdm$ with m coprime to $abcd$.

And so on.

Let $s_1(n) = s(n)$, and for all positive integers k, n, if $s_k(n)$ is defined and not 0, let $s_{k+1}(n) = s(s_k(n))$.

From Lenstra's proof we have for each k, the set of numbers n where $n < s_1(n) < \cdots < s_k(n)$ contains a set of positive asymptotic density.

The Lenstra problem and solution inspired Erdős to prove a remarkable and at first counter-intuitive theorem: *Let C_k be the set of integers n such that $n < s_1(n) < \cdots < s_k(n)$. Then each set C_k has the same asymptotic density as the set C_1, the set of abundant numbers.* That is, if $n < s(n)$, then almost surely, $s(n) < s(s(n)) < \ldots$ for $k - 1$ more steps.

Now, if you have a sociable k-cycle with $k \geq 2$, then it contains an abundant number n not in C_k. Thus, for each fixed k, the sociable numbers of order at most k have density 0.

The Erdős argument springs from the observation that if a is any fixed positive integer, then $a^2 \mid \sigma(n)$ for a set of integers n of asymptotic density 1. (Basically, since the primes that are $-1 \mod a^2$ have positive density, n is almost surely divisible by one of these primes to exactly the first power.)

Erdős actually proved the still stronger result that for each positive integer k and real number $\epsilon > 0$, the set of integers n with

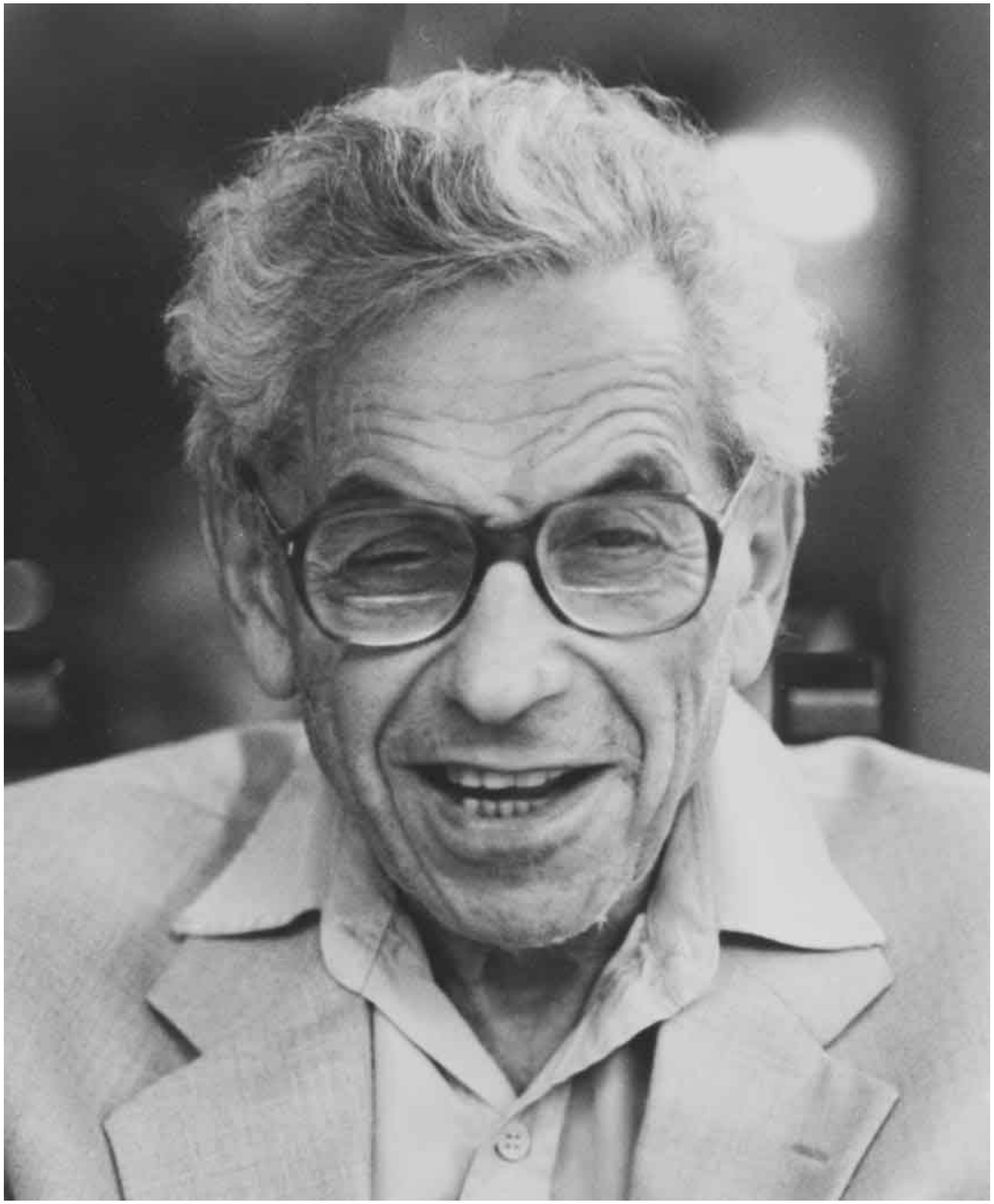
$$s_j(n) > (s(n)/n - \epsilon)^j n, \quad j = 1, 2, \dots, k$$

has asymptotic density 1.

He asserted in the paper that the same argument would show that

$$s_j(n) < (s(n)/n + \epsilon)^j n, \quad j = 1, 2, \dots, k.$$

In 1981, Lenstra told me he didn't understand this, and I enthusiastically offered to explain it to him. I realized then that I also didn't understand the proof. I later challenged Erdős who also realized his idea didn't work, and so this assertion was later retracted by him.



Paul Erdős

Any given natural number is either sociable or it is not sociable.

I ask again: Does the set of sociable numbers have density 0? We think the answer is yes, but we have no heuristic for this. (Despite the fact that Cohen and Lenstra have worked in this subject, I don't think the Cohen–Lenstra heuristics apply.)

As mentioned, one thing that makes this a hard question is that we don't have a simple algorithm that can test membership in the set of sociable numbers. For example, is 564 sociable?

Kobayashi, Pollack, P (2009):
But for a set of density 0, all sociable numbers are contained within the odd abundant numbers.

Further, the density of all odd abundant numbers is $\approx 1/500$.

One helpful tool in the proof was to essentially prove the Erdős upper bound assertion in the context of sociable numbers. So, in particular, if one has a deficient sociable number n, the sequence $n, s_1(n), s_2(n), \ldots$ usually decays exponentially for a long way, and so n is associated to a very small sociable number in its cycle.

We'd like to the same for abundant numbers, but by backing up to earlier members of the cycle. For even abundants, this idea works fine, but not for odd abundants.

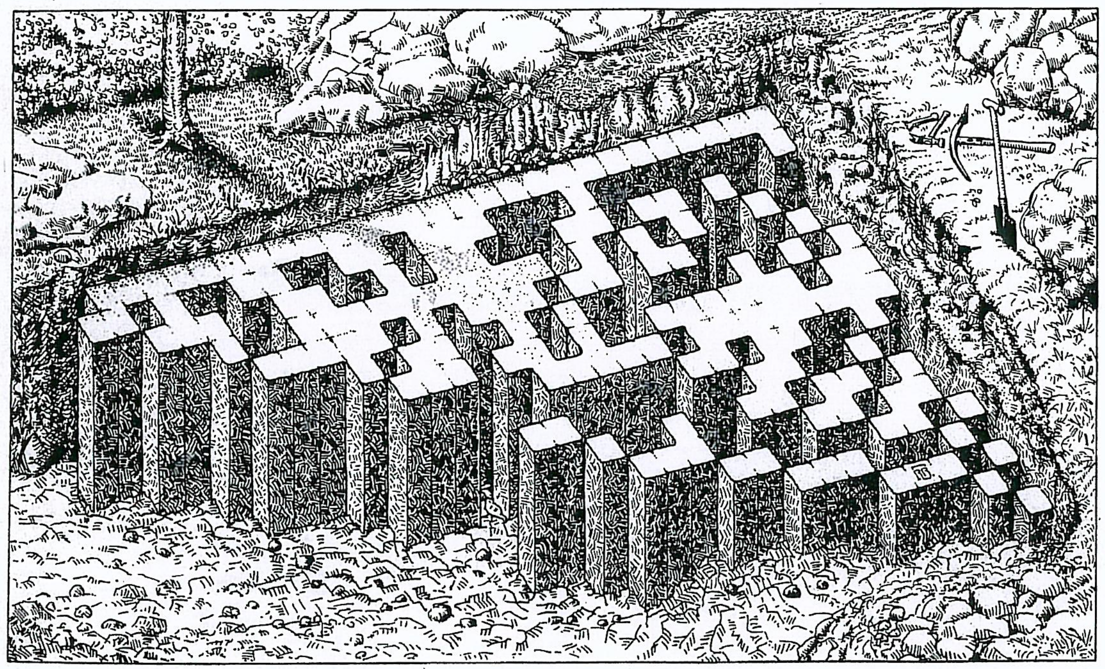
Which one is Paul Pollack? 

Call a sociable number n *special* if

- n is odd abundant,
- the number preceding n in its cycle exceeds

$$n \exp\left(\tfrac{1}{2}\sqrt{\log\log\log n \, \log\log\log\log n}\right).$$

We prove that if the special sociable numbers have density 0, then so too do all sociable numbers have density 0. Further, we prove that the special sociable numbers have upper density at most $\approx 1/6000$.



These are the famous digs at Mersennechus.

W. Creyaufmueller, `www.aliquot.de/aliquot.htm/`

M. Deléglise, *Bounds for the density of abundant integers*, Experimental Math. **7** (1998), 137–143.

P. Erdős, *On asymptotic properties of aliquot sequences*, Math. Comp. **30** (1976), 641–645,

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, pp. 165–204 in Analytic number theory, Progr. Math. vol. 85, Birkhäuser, Boston, 1990.

M. Kobayashi, P. Pollack, and C. Pomerance, *On the distribution of sociable numbers*, J. Number Theory, to appear.

(The last two papers and these slides are available at `www.dartmouth.edu/~carlp` .)

$2 = 10$

$3 = 11$

$5 = 101$

$7 = 111$

$13 = 1101$

$\ldots$