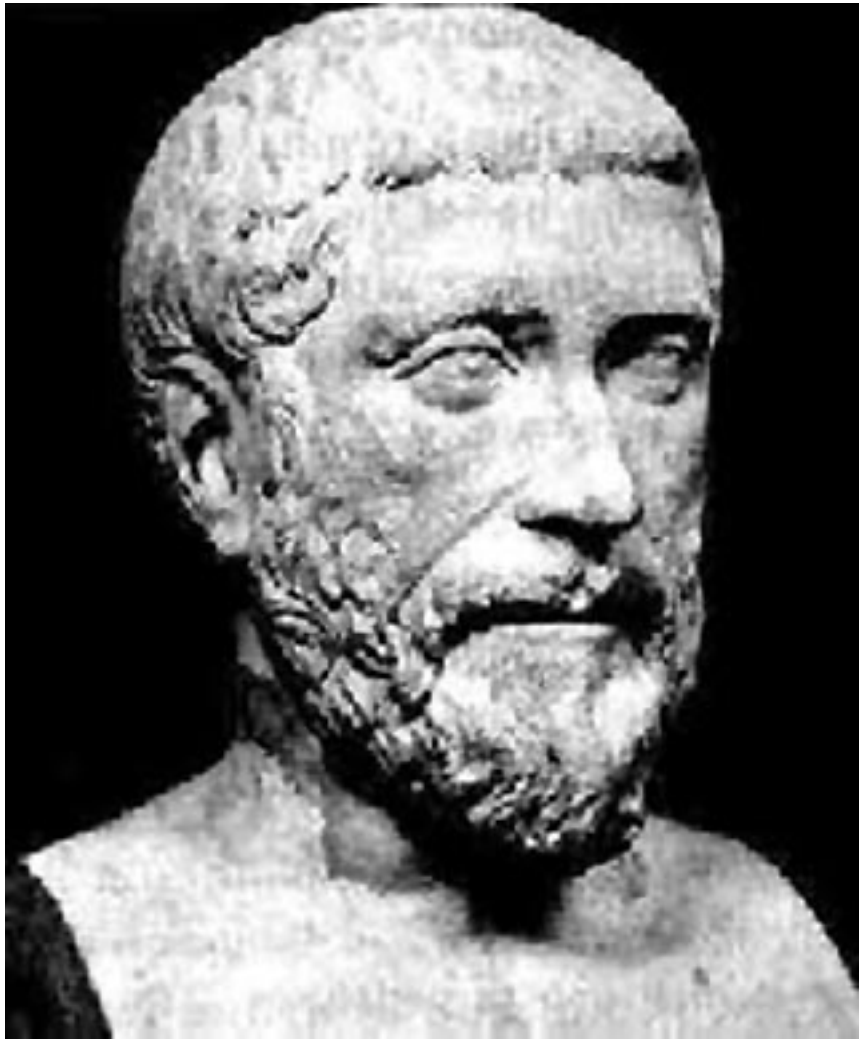
Amicable numbers

Carl Pomerance, Dartmouth College



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:

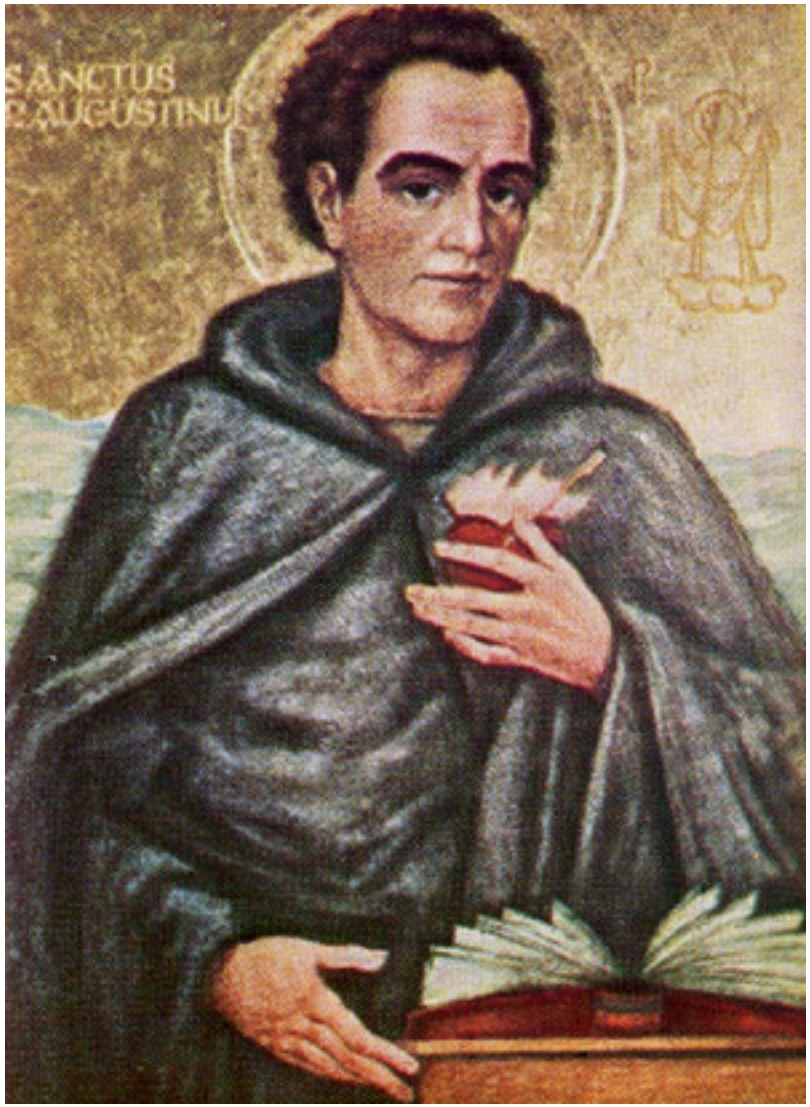
He noticed that $s(6) = 1 + 2 + 3 = 6$.
(If $s(n) = n$, we say n is *perfect*.)

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.)

We have here perhaps the first ever *function* and the first ever *dynamical system*.



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 ... And here's proof that it is indeed applied math:

Available for £9 from mathsgear.co.uk

Let's take a look at the dynamical system suggested by Pythagoras:

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.

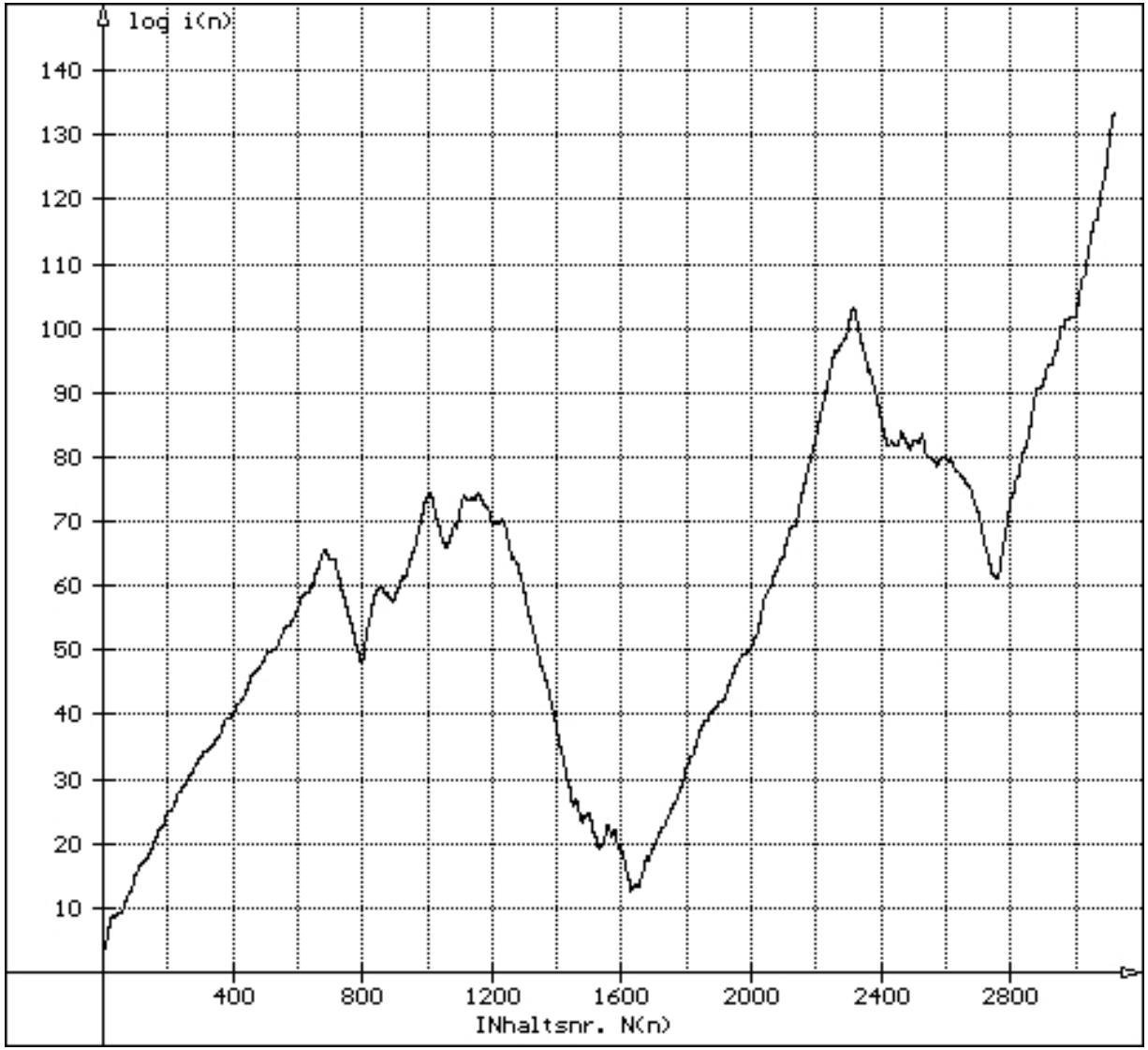
Erdős showed in 1976:
There are arbitrarily long increasing aliquot sequences

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

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 (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".

We currently know about 12 million different cycles, and all, with about 200 exceptions, are amicable pairs. There are 48 known 1-cycles (perfect numbers), and of the cycles of length greater than 2, all but 10 are length 4. There are no known of length 3; the longest cycle known is length 28.

In elementary number theory we learn the formula of Euclid for even perfect numbers:
If $2^p - 1$ *is prime, then* $2^{p-1}(2^p - 1)$ *is perfect.*

In the 9th century, the Iraqi scholar Thâbit ibn Qurra found a similar formula for amicable pairs:
If $p = 3 \cdot 2^n - 1,\ q = 3 \cdot 2^{n-1} - 1,\ r = 9 \cdot 2^{2n-1} - 1$ *are primes, then* $2^n pq,\ 2^n r$ *form an amicable pair.*

For example, $n = 2$ gives the primes 11, 5, 71, giving rise to the pair $2^2 \cdot 5 \cdot 11 = 220$, $2^2 \cdot 71 = 284$.

This formula was rediscoverd by Fermat and Descartes, and Fermat found it also gives a second pair with $n = 4$.

Euler generalized Thâbit's rule:
If $p = (2^{n-m}+1)2^n - 1,\ q = (2^{n-m}+1)2^m - 1,$
$r = (2^{n-m}+1)^2 2^{n+m} - 1$ *are prime, then* $2^n pq,\ 2^n r$ *are an amicable pair.*

He found about 50 pairs, but missed the second smallest: 1184, 1210. It was discovered by a 16-year-old in Italy in the 19th century (Paganini).

After exhaustive searches to 10^{14} (Moews & Moews and others) and generalizations of Euler's rule (Borho, te Riele), we now know about 12 million amicable pairs.

Erdős has a heuristic that there should be infinitely many amicable pairs, in fact, more than $x^{1-\epsilon}$ of them up to x, for each fixed $\epsilon > 0$ and x sufficiently large in terms of ϵ.

There is already a well-known and widely believed heuristic of Erdős that there are infinitely many numbers N with $\sigma(n) = N$ having more than $N^{1-\epsilon}$ solutions n. (This is proved for $\epsilon = \frac{1}{3}$.) So among these solutions n, it should be not that unusual to have two of them with $n + n' = N$, in fact there ought to be about $N^{1-2\epsilon}$ such pairs.

But if $n + n' = \sigma(n) = \sigma(n')$ and $n \neq n'$, one immediately sees that n, n' form an amicable pair.

Nevertheless, we have not proved that there are infinitely many amicable numbers.

Can we prove that amicable numbers are rare among the natural numbers?

This quest was begun by Kanold in 1954, who showed that the number of integers $n \leq x$ that belong to an amicable pair is at most $.204x$ for all sufficiently large values of x.

To fix notation, let $A(x)$ denote the number of integers $n \leq x$ that belong to some amicable pair. Here's what's happened since Kanold:

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): $A(x) = O(x/\log\log\log x)$.

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

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

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

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

Bayless & Klyve (2011): *Let P denote the reciprocal sum of the amicable numbers. Then*

$$0.0119841556\cdots \leq P < 656{,}000{,}000.$$

Nguyen (2014): $P <$??? (Come find out Tuesday May 28, 2:30 pm, 041 Haldeman!)

How do we get a strong upper bound for $A(x)$?

As typical with an Erdős-style argument, one divides the problem into a number of cases, some being routine, some not. But there is an overarching strategy which is sometimes lost in the details.

Here's the strategy. We have n, n' an amicable pair. Write

$$n = pm, \quad n' = p'm',$$

where p, p' are the largest primes in n, n', respectively. Assume that $p > p', \ p \nmid m, \ p' \nmid m'$. (The cases $p = p', \ p \mid m, \ p' \mid m'$ are easily handled.)

We may assume that m, m' are largely squarefree and not too smooth, and they both have some size. That is, p, p' don't dominate. (For $n \leq x$, we have $p < x^{3/4}$, approximately.)

Since m is large, we may assume that r, the largest prime factor of $\sigma(m)$ is large, say $r > L$. (Prove directly or use a recent paper of Banks, Friedlander, P, & Shparlinski.)

We have $r \mid q+1$ for some prime $q \| m$. Since $r \mid \sigma(m) \mid \sigma(n) = \sigma(n')$, we have $r \mid q'+1$ for some prime $q' \| n'$, and $q' \neq q$. Note that

$$q' \mid n' = s(n) = s(pm) = (p+1)s(m) + \sigma(m).$$

Thus, with m, q' given, p is constrained to a residue class modulo q'.

We thus count as follows:

$$\sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \sum_{\substack{m<x \\ q|m}} \sum_{\substack{q'<x \\ r|q'+1}} \sum_{\substack{p\leq x/m \\ p>q' \\ p\equiv a_{m,q'} \pmod{q'}}} 1.$$

We thus count as follows:

$$\sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \sum_{\substack{m<x \\ q|m}} \sum_{\substack{q'<x \\ r|q'+1}} \sum_{\substack{p\leq x/m \\ p>q' \\ p\equiv a_{m,q'} \pmod{q'}}} 1.$$

And we're laughing.

$$\sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \sum_{\substack{m<x \\ q|m}} \sum_{\substack{q'<x \\ r|q'+1}} \sum_{\substack{p\le x/m \\ p>q' \\ p\equiv a_{m,q'} \pmod{q'}}} 1.$$

The inner sum can be replaced with $\frac{x}{mq'}$:

$$x \sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \sum_{\substack{m<x \\ q|m}} \sum_{\substack{q'<x \\ r|q'+1}} \frac{1}{mq'}.$$

The new inner sum can be replaced with $\frac{\log x}{mr}$:

$$x \log x \sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \sum_{\substack{m<x \\ q|m}} \frac{1}{mr}.$$

The new inner sum can be replaced with $\frac{\log x}{qr}$:

$$x(\log x)^2 \sum_{r>L} \sum_{\substack{q<x \\ r|q+1}} \frac{1}{qr}$$

The new inner sum can be replaced with $\frac{\log x}{r^2}$:

$$x(\log x)^3 \sum_{r>L} \frac{1}{r^2}.$$

And this sum is smaller than $1/L$, so we have the estimate $x(\log x)^3/L$. By choosing L as large as possible so that the various assumptions may be justified, we have our result. And in fact we can choose L a tad larger than $\exp(\sqrt{\log x})$.

My earlier result with $x/\exp((\log x)^{1/3})$ did not get such a good lower bound on m, m' so that it was difficult to show that $\sigma(m), \sigma(m')$ had large prime factors.

Beyond showing there are few amicable numbers, it should be true that there are few *sociable* numbers.

Definition: Say a number n with $s_k(n) = n$ for some k is sociable.

That is, sociable numbers are the numbers involved in a cycle in the dynamical system introduced by Pythagoras.

Here is what we know about the distribution of sociable numbers.

From the 1976 Erdős result that if $n < s(n)$, then almost surely the sequence continues to increase for k terms, one can show that the sociable numbers that belong to a cycle of any fixed length have asymptotic density 0.

In Kobayashi, Pollack, & P (2009), we showed that

- The even sociable numbers have asymptotic density 0.
- The odd sociable numbers n with $n > s(n)$ have asymptotic density 0.

This would leave the odd sociables n with $n < s(n)$. The odd numbers n with $n < s(n)$ have an asymptotic density of about 1/500, so we're talking about a fairly sparse set to begin with. But the problem of showing the sociable numbers in this set have density 0 is still open.

Here are some other unsolved problems in connection with the function $s(n)$.

Show that there is a positive proportion of even numbers in the range of s. We know (Erdős) that there is a positive proportion of even numbers *not* in the range of s. We also know that almost all odd numbers are in the range of s.

Show that if $n > s(n)$, then almost surely the sequence continues to decrease for another k steps (or terminates). This is known for $k = 1$ (Erdős, Granville, P, Spiro).

Thank You!