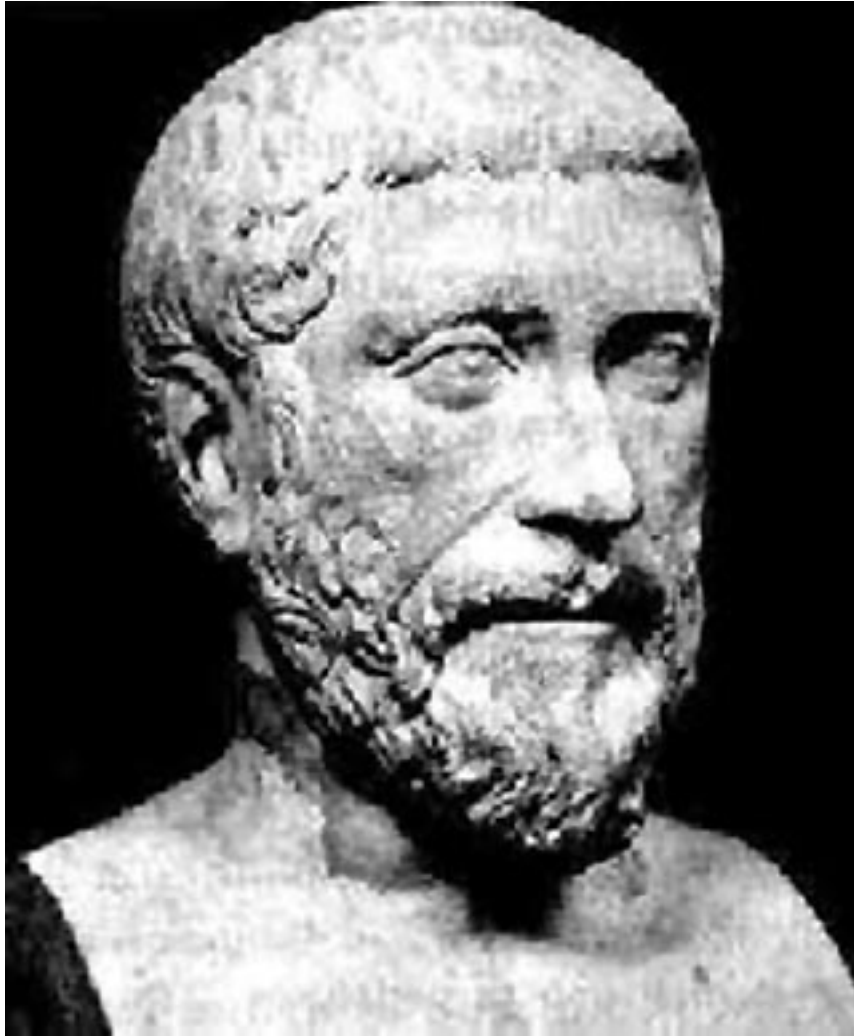


# Amicable numbers

The Memorial Conference for  
Felice and Paul Bateman and Heini Halberstam  
University of Illinois, June 5–7, 2014

**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*.

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 another application:



Available for £9 from [mathsgear.co.uk](http://mathsgear.co.uk)

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

Many orbits end at 1, while others cycle:

10 → 8 → 7 → 1

12 → 16 → 15 → 9 → 4 → 3 → 1

14 → 10...

18 → 21 → 11 → 1

20 → 22 → 14...

24 → 36 → 55 → 17 → 1

25 → 6 → 6

26 → 16...

28 → 28

30 → 42 → 54 → 66 → 78 → 90 → 144 → 259 → 45 → 33 → 15...



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

$$25 \rightarrow 6 \rightarrow 6.$$

It can be preceded by 95:

$$95 \rightarrow 25 \rightarrow 6 \rightarrow 6.$$

And again preceded by 445:

$$445 \rightarrow 95 \rightarrow 25 \rightarrow 6 \rightarrow 6.$$

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*

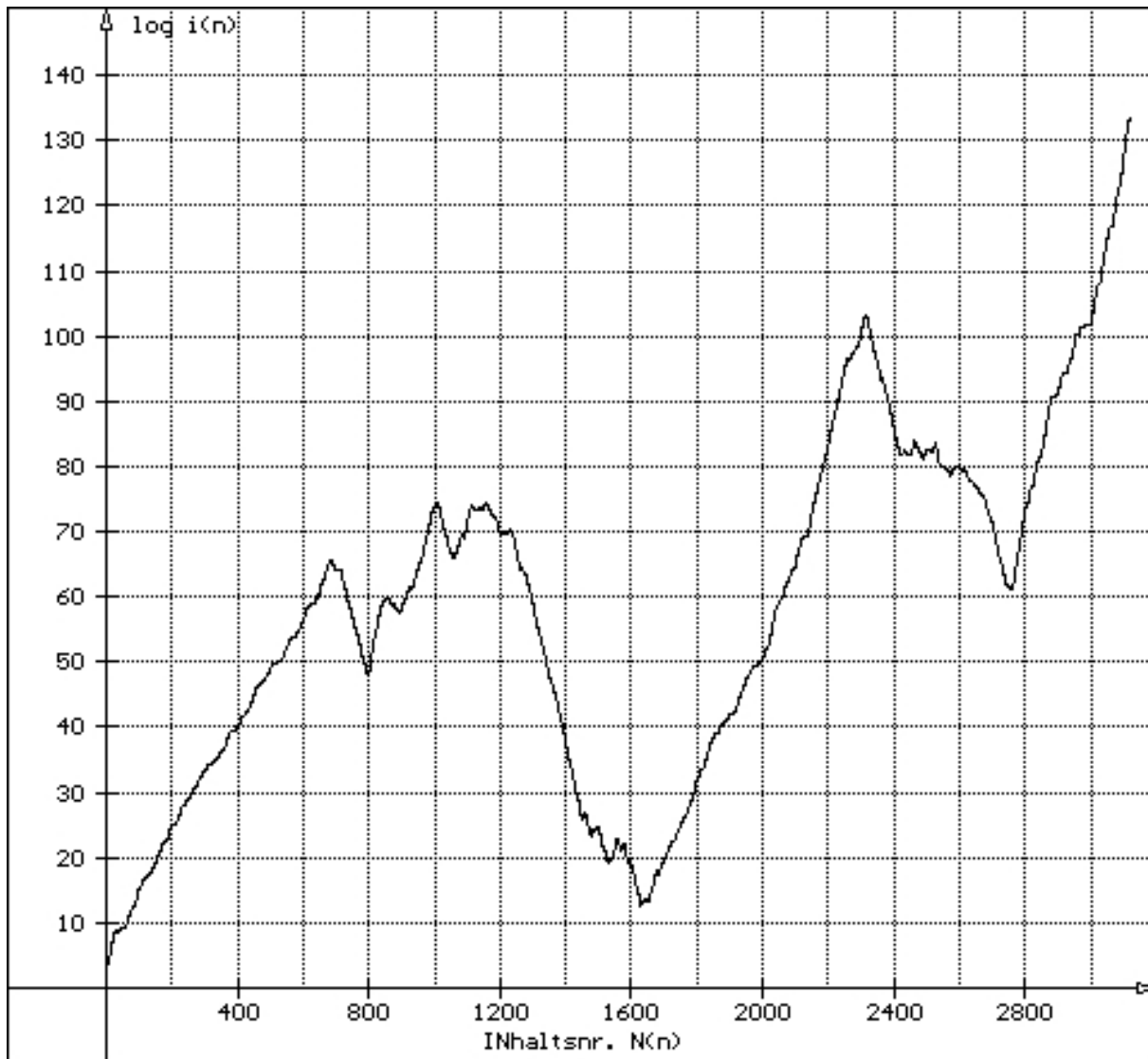
$$n < s(n) < s(s(n)) < \cdots < s_k(n).$$

[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](http://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, 552, 564, 660, 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.

[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  $\epsilon$ .

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 follows from the [Elliott–Halberstam](#) conjecture, and 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  $x \rightarrow \infty$ . Said his method would give  $A(x) = O(x / \log \log \log x)$ .



Erdős (1955):  $A(x) = o(x)$  as  $x \rightarrow \infty$ . 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 (1955):  $A(x) = o(x)$  as  $x \rightarrow \infty$ . 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  $x \rightarrow \infty$ . 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.

Erdős (1955):  $A(x) = o(x)$  as  $x \rightarrow \infty$ . 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.

Erdős (1955):  $A(x) = o(x)$  as  $x \rightarrow \infty$ . 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 finite.

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

$$P > 0.0119841556\dots$$

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

$$P > 0.0119841556 \dots$$

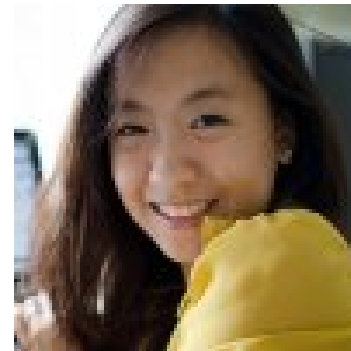
Bayless & Klyve (2011):  $P < 656,000,000$ .

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

$$P > 0.0119841556 \dots$$

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

Nguyen (2014):  $P < 4084$





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  $q \parallel m$ . Since  $r \mid \sigma(m) \mid \sigma(n) = \sigma(n')$ , we have  $r \mid q' + 1$  for some prime  $q' \parallel n'$ , 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.

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

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 (*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  $s$ . (Maybe Florian Luca and I have a proof.)

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).

This paper of Erdős, Granville, P, & Spiro appeared in the Bateman Proceedings from the Allerton Park Conference in 1990. A conjecture from that paper:

*If  $\mathcal{A} \subset \mathbb{N}$  has density 0, then  $s^{-1}(\mathcal{A})$  has density 0.*

(This conjecture implies the two problems just mentioned.)

Finally, note that there is a set  $\mathcal{A}$  of density 0 such that  $s(\mathcal{A})$  has density  $\frac{1}{2}$ , namely the set  $\{pq : p, q \text{ prime}\}$ .

**Thank You**