Florian Luca
*Instituto de Matemáticas*
*Universidad Nacional Autónoma de México*
*C.P. 58089, Morelia, Michoacán*
*México*
*fluca@matmor.unam.mx*

Herman te Riele
*Centrum Wiskunde & Informatica*
*Postbus 94079*
*1090 GB Amsterdam*
*Herman.te.Riele@cwi.nl*

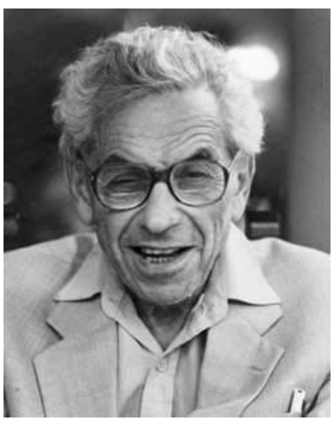
**Research**

# $\phi$ and $\sigma$: from Euler to Erdős

This paper bij Florian Luca and Herman te Riele is an extended version of the 10th biennial Beeger Lecture, presented by Florian Luca on April 23, 2010 during the *Nederlands Mathematisch Congres* in Utrecht. Florian Luca (born 1969 in Romania) is full professor at the Instituto de Matemáticas, UNAM, Morelia, México. His research interests are abstract algebra, algebraic number theory, and Diophantine equations. He obtained a Young Researcher Award from UNAM in 2008, a Guggenheim Fellowship in 2006, and an Alexander von Humboldt Fellowship in 1998–1999.

Euler's $\phi$ function, which counts the number of positive integers relative prime to and smaller than its argument, as well as the sum of divisors function $\sigma$, play an important role in number theory and its applications. In this paper we survey various old and new results related to the distribution of the values of these two functions, their popular values, their champions, and the distribution of those positive integers satisfying certain equations involving such function, like the perfect numbers and the amicable numbers. In the second part of this paper, we discuss some of the ideas which are used in the proof of a recent result of Ford, Luca, and Pomerance which says that there are infinitely many common values in the ranges of these two functions. This settles a $50$ year old question of Erdős.

Leonard Euler



Paul Erdős

## Perfect and multiperfect numbers

Let $n$ be a positive integer. We write $\sigma(n)$ for the sum of all divisors of $n$, and $s(n)$ for the sum of the proper divisors of $n$. So,

$$\sigma(n) = \sum_{d|n} d \quad \text{and} \quad s(n) = \sigma(n) - n.$$

A number $n$ is called *perfect* if $n = s(n)$ and *multiperfect* if $n \mid s(n)$. Examples of (multi-)perfect numbers are: $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$. Some other multiperfect numbers: 120 (with $s(n) = 240 = 2 \cdot n$) and 30240 (with $s(n) = 90720 = 3 \cdot n$). Let $\mathcal{P}$ be the set of perfect numbers. Then

$$\mathcal{P} = \{6, 28, 496, 8128, 33550336, 8589869056, 137438691328, \ldots\}.$$

This is sequence A000396 in [39]. All these numbers seem to be even. Is there a rule to generate them? The answer is yes and is given by the following result.

**Theorem 1** (Euclid, Euler). *The number $n$ is even and perfect if and only if*

$$n = 2^k(2^{k+1} - 1),$$

*where the number $P = 2^{k+1} - 1$ is prime.*

*Proof.*
– Say $P = 2^{k+1} - 1$ is prime. Then Euclid observed that the sum of the

divisors of $n = 2^k P$ is

$$\sigma(n) = 1 + 2 + \cdots + 2^k + P + 2P + \cdots + 2^k P = (1+P)(1+2+\cdots+2^k) = 2^{k+1}P = 2n.$$

– Euler observed that, conversely, if $n = 2^k M$ is perfect with odd $M$, then

$$2n = 2^{k+1}M = \sigma(n) = \sigma(2^k)\sigma(M) = (1+2+\cdots+2^k)\sigma(M).$$

This implies that $P = 2^{k+1} - 1$ is a divisor of $M$. Say $M = PL$. Then $n = 2^k PL$ has at least the divisors

$$L, 2L, \ldots, 2^k L, PL, 2PL, \ldots, 2^k PL$$

already summing up to $2n$, so it cannot have other divisors. Thus, $L = 1$ and $P$ is prime. □

**Theorem 2** (H.W. Lenstra [17]). *There are no perfect squares.*

*Proof* (without using Theorem 1).
– If $n = m^2$ is odd, then

$$\sigma(n) = \sum_{d|m^2,\, d<m} \left(d + \frac{m^2}{d}\right) + m$$

is odd.
– If $n$ is even and square, then $n = 2^{2k}m^2$ with $m$ odd, so

$$\sigma(n) = \sum_{d|n\,:\,d \text{ even}} d + \sum_{d|m^2} d$$

is also odd by the previous argument. □

Concerning *odd* perfect numbers, Pomerance proved in 1973 that every odd perfect number must have at least 7 distinct prime factors [34]. The current record holder for this type of result is Nielsen who was able to replace 7 by 9 in 2007 [29]. In 2001, Brent performed extensive computations to show that any odd perfect number must exceed $10^{300}$ [5]. This was recently extended (but not yet published) to $10^{1500}$ by Ochem and Rao (see [31]). They also obtained that the largest prime power in an odd perfect number exceeds $10^{62}$ and that the number of prime factors, counting multiplicities, is at least 97.

Concerning the occurrence of perfect numbers in various sequences, in 2000 Luca [26] proved that there is no perfect number among the Fibonacci numbers $\{F_n\}_{n\geq 1}$, where $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n$ for all $n = 1, 2, \ldots$. In 2009, Pollack [33] used similar arguments to show that the only perfect number which is a repdigit in base 10, i.e., whose base 10 representation is of the form

$$n = \underbrace{\overline{ddd\ldots d}}_{m \text{ times}} = d\left(\frac{10^m - 1}{9}\right), \qquad \text{with } d \in \{1, \ldots, 9\},$$

is $n = 6$. Also in 2009, Broughan et al. [6] extended the above-mentioned result by proving that there is no Fibonacci number $F_n > 1$ which is multiperfect.

Numbers of the form $P = 2^m - 1$ are called Mersenne numbers. If $P$ is prime, then $m$ must be prime, but the converse is not true, since $2^{11} - 1 = 2047 = 23 \times 89$. In 1953, 12 Mersenne primes — and thus even perfect numbers — were known. Now, in 2010, 47 Mersenne primes are known, the largest one being

$$2^{43{,}112{,}609} - 1, \text{ with 12,978,189 decimal digits.}$$

It is predicted that there are about $\sim c \log x$ primes $p \leq x$ such that $2^p - 1$ is prime, where $c = e^{-\gamma}/\log 2$ and $\gamma = 0.5572\ldots$ is Euler's constant.

**Theorem 3** (Luca [25]). *There are no consecutive perfect numbers.*

*Proof.* If $m$ is odd perfect, then $m = p \times$ odd square, with prime $p \equiv 1 \pmod 4$ (Euler). Since even perfect numbers $> 6$ are multiples of 4, we get that if $n$ and $n+1$ are perfect, then $n$ is even. So, $n = 2^{p-1}(2^p - 1)$ for some prime $p > 2$. Thus, $n \equiv 1 \pmod 3$, and

$$\sigma(n+1) = \sum_{d|n+1,\, d<\sqrt{n+1}} \left(d + \frac{n+1}{d}\right) \equiv 0 \pmod 3,$$

a contradiction. □

A similar argument shows that there are no two perfect numbers which differ by 2, or by 3, or by 4. One would like to say: *and so on*, but one quickly gets stuck. At least at $22 = 28 - 6$, although quite likely much sooner. The following problem looks innocent:

*Assume that the sequence $\mathcal{P}$ of perfect numbers is infinite and arrange them in increasing order $n_1 < n_2 < \cdots$. Is it then true that*

$$n_{k+1} - n_k \to \infty?$$

In 2009, Pomerance and Luca [28] almost confirmed this conditionally.

**Theorem 4**. *Assume the $ABC$ conjecture. Then*

$$n_{k+2} - n_k \to \infty.$$

The $ABC$ conjecture [30] is the following statement.

**Conjecture**. *For all $\varepsilon > 0$, there exists some absolute constant $C_\varepsilon$ such that if $a$ and $b$ are coprime positive integers then*

$$a + b < C_\varepsilon \left(\prod_{p|ab(a+b)} p\right)^{1+\varepsilon}.$$

The truth of the ABC conjecture implies the truth of Fermat's Last Theorem up to (possibly) finitely many exceptions. Luckily, this has been proved in a different way by Wiles, and Wiles and Taylor.

**Iterating $s$**
What happens if we start with $n$ and iterate $s$? Then some numbers go to 0 after a while, like $\{12, 16, 15, 9, 4, 3, 1, 0\}$ and some numbers get

trapped in a loop, like $\{220, 280, 220, \ldots\}$; that is, for some $n$ there exist $k$ such that if we put

$$n_1 = n, n_2 = s(n_1), \ldots, n_{k+1} = s(n_k),$$

then $n_{k+1} = n_1$. Sequences obtained by iterating $s$ are called *aliquot sequences*. Numbers which get trapped in a loop are called *sociable*. Their distribution was investigated recently by Kobayashi et al. [22]. An old conjecture of Catalan and Dickson states that all aliquot sequences are bounded [9–10]. In 1975, Lenstra [24] proved that for every positive integer $k$, there exist infinitely many positive integers $n$ such that

$$n < s^{(1)}(n) < \cdots < s^{(k)}(n).$$

Here is a modified question: Given $k \geq 2$ and any permutation $i_0, \ldots, i_k$ of $\{0, 1, \ldots, k\}$, do there exist positive integers $n$ such that

$$s^{(i_0)}(n) < s^{(i_1)}(n) < \cdots < s^{(i_k)}(n)?$$

Guy and Selfridge have made the counter-conjecture to that of Catalan and Dickson that in fact *unbounded* aliquot sequences are fairly common [20].

Loops with $k = 2$ are called *amicable numbers* [18, 32]. In 1955, Erdős proved that amicable numbers have zero density [12]. Pomerance worked on the counting function of amicable numbers [35–36]. As a byproduct of his work, he deduced that the series

$$P = \sum_{n \text{ amicable}} \frac{1}{n}$$

is finite, although it is not known whether the number of amicable numbers is finite or infinite! In 2009, Bayless and Klyve [3] showed that

$$0.0119841556 < P < 7 \times 10^8.$$

The lower bound follows from the known amicable pairs [32].

**Euler's totient function and related numbers**

Let $\phi(n)$ be Euler's totient function which counts the number of positive integers $m \leq n$ which are coprime to $n$. If finding $n$ such that $n \mid \sigma(n)$ is hard, it turns out that finding $n$ such that $\phi(n) \mid n$ is easy! They are all of the form $n = 2^a \cdot 3^b$ with arbitrary $a \geq 0$ and $b \geq 0$ except that if $b > 0$ then also $a > 0$. Observe that if $n$ is prime, then $\phi(n) = n - 1$. In particular, $\phi(n) \mid n - 1$. Lehmer asked the innocent looking question whether $\phi(n) \mid n - 1$ and $n > 1$ implies that $n$ is prime. One typical result is that such $n$ should have at least 14 different prime factors (see [19, Problem B37]). Let us call a composite $n$ such that $\phi(n) \mid n - 1$ a *Lehmer-*$\phi$ number and let $\mathcal{L}(x)$ be the set of Lehmer-$\phi$ numbers $\leq x$. In 1977, Pomerance [37] showed that $\mathcal{L}(x) \ll x^{1/2}(\log x)^{4/3}$. The best current bound on $\mathcal{L}(x)$ is due to Pomerance and Luca: $\mathcal{L}(x) \leq x^{1/2}(\log x)^{-1/2+o(1)}$ as $x \to \infty$.

**Theorem 5** (Luca [27]). *There is no Fibonacci number which is a Lehmer-*$\phi$ *number.*

In other words, if $\phi(n) \mid n-1$ and $n > 1$ is a Fibonacci number, then $n$ is prime. Can this be used as a primality test for Fibonacci numbers? It is not known if there are infinitely many Fibonacci primes, although a heuristic similar to the heuristic for the Mersenne primes can be made.

By Euler's theorem, we have that $a^{\phi(n)} \equiv 1 \pmod{n}$ whenever $a$ is an integer coprime to $n$. In particular, if $n$ is Lehmer-$\phi$, we have that

$$a^n \equiv a \pmod{n} \tag{1}$$

and $n$ is composite. Composite numbers $n$ satisfying (1) for some fixed $a$ are called *base* $a$*-pseudoprimes*. There is a large literature on pseudoprimes. See, for example, [19, Problem A12]. In 1951, Beeger [4] proved that there exist infinitely many even positive integers $n$ such that $n \mid 2^n - 2$. In 1910, Carmichael [8] observed that $n = 561$ is a composite positive integer which satisfies $a^n \equiv a \pmod{n}$ for *all* positive integers $a$. Such numbers are now called *Carmichael numbers*. In 1994, Alford, Granville and Pomerance [1] proved that there are infinitely many of them.

Call $m$ a *totient* if $m$ is in the range of the Euler $\phi$-function. There are many interesting questions and results involving totients.

**Theorem 6** (Gauss). *The regular polygon with* $n \geq 3$ *sides can be constructed with the ruler and the compass if and only if* $\phi(n) = 2^k$ *for some* $k > 0$.

Numbers $n$ satisfying $\phi(n) = 2^k$ for some positive integer $k$ have a constrained multiplicative structure. They must be of the form $2^a p_1 p_2 \cdots p_b$, where the $p_i$ are distinct primes of the form $2^{m_i} + 1$ for $i = 1, \ldots, b$. If $2^m + 1$ is a prime, then $m$ must be a power of 2. Fermat thought that $2^{2^n} + 1$ is always prime. However, no $n > 4$ is known for which $2^{2^n} + 1$ is prime! The numbers $2^{2^n} + 1$ are called *Fermat numbers* and a lot of information about them can be found in [23]. Here are some fun facts about Fermat numbers:

- The largest Fibonacci number whose Euler function is a power of 2 is $F_9 = 34$.
- A Fermat number is never perfect or part of an amicable pair.
- A Fermat number is never a nontrivial binomial coefficient $\binom{n}{k}$ for some $n \geq 2k \geq 4$.

In 1907, Carmichael [7] thought he had a proof of the following statement: *For each* $n$*, there is some* $m \neq n$ *such that* $\phi(m) = \phi(n)$. To this day, this has not yet been proved, neither disproved. It is called the *Carmichael* conjecture. The best partial results concerning this conjecture are due to Ford. Put $\mathcal{V}(x) = \#\{\phi(n) \leq x\}$, and for any given $k \geq 1$, let $\mathcal{V}_k(x) = \#\{m \leq x \, : \, \#\phi^{-1}(\{m\}) = k\}$. Then, Ford [14] showed that the following hold:

- $\mathcal{V}_k(x) > 0$ for all $k \geq 2$ when $x$ is large enough;
- if $k$ is fixed and $\mathcal{V}_k(x) > 0$ for some $x$, then

$$\lim_{x \to \infty} \frac{\mathcal{V}_k(x)}{\mathcal{V}(x)} > 0;$$

- the Carmichael conjecture is true for all $n < 10^{10^{10}}$.

Here are some thoughts about popular totients. Can you find $n$ such that $\phi(n) = \square$? You will say: this is easy! Take $n = 2^{2k+1}$, and then $\phi(n) = n/2 = 2^{2k}$. So, let's make it harder. Can you find $n$ such that $\phi(n) = \square$ and $n$ is squarefree? Here is a hint. Look at the following table:

| | | |
|---|---|---|
| $\phi(2) = \square$ | $\phi(3) = 2 \times \square$ | $\phi(5) = \square$ |
| $\phi(7) = 2 \times 3 \times \square$ | $\phi(11) = 2 \times 5 \times \square$ | $\phi(13) = 3 \times \square$ |
| $\phi(17) = \square$ | $\phi(19) = 2 \times \square$ | $\phi(23) = 2 \times 11 \times \square$ |
| $\phi(29) = 7 \times \square$ | $\phi(31) = 2 \times 3 \times 5 \times \square$ | $\phi(37) = \square$ |

From this, it should be easy to find examples. Like

$$2, \quad 5, \quad 7\times 19\times 13, \quad 3\times 7\times 11\times 31.$$

Can we really find infinitely many examples in this way? Yes! Here is why. Let $x$ be large and $p$ be a prime with $p \le x$. Write

$$\phi(p) = p - 1 = a_p\Box,$$

where $a_p$ is square-free. Then the largest prime factor of $a_p$ is $< x/2$. Put $\pi(y) = \#\{p \le y : p \text{ prime}\}$. Identify $a_p$ with the vector $v_p$ in the vector space

$$V = \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{\pi(x/2)\text{ times}},$$

obtained by putting a 1 or a 0 in the appropriate coordinate according to whether the corresponding prime $q < x/2$ divides $a_p$ or not. There are $\pi(x)$ values of $v_p$, all living together in the $\mathbb{Z}_2$-vector space $V$ of dimension $\pi(x/2)$. So, there must be at least $\pi(x) - \pi(x/2)$ linear combinations of them which are equal to 0. All you have to recall is that $\pi(x) - \pi(x/2) > 0$. This is called *the Bertrand postulate* and was proved by Chebyshev in 1850. Actually, $\pi(x) - \pi(x/2)$ is not only positive but actually quite large for large values of $x$, so we get many $n$ with $\phi(n) = \Box$. Was this really better? Yes! Here are some reasons. First of all, it works not only for $\phi(n)$ but also for $\sigma(n)$: just replace $p - 1$ with $p + 1$ for all primes $p$. It also works for $\phi(n)\sigma(n)$. Secondly, and most importantly, it is open to *refinements*. Let's see one. An improvement comes from considering primes $p$ such that $p - 1$ does not have a very large prime factor. Write $P(m)$ for the maximal prime factor of $m$. If $y$ is much smaller than $x/2$ and we work only with primes $p$ such that $P(p - 1) \le y$, then $v_p$ can be regarded as an element in the much smaller vector space

$$V_y = \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{\pi(y)\text{ times}}.$$

If we have many such primes, then in this vector space we will have many zero linear combinations involving $v_p$ for such primes $p$. Hence, many $n$'s with $\phi(n) = \Box$.

All this can be turned around into a very specific statement that says something like this:

*If $\delta > 0$ is such that*

$$\#\{p \le x : P(p-1) < x^{\delta}\} > c_\delta \pi(x) \tag{2}$$

*for large $x$ ($c_\delta > 0$ some constant), then*

$$\#\{n \le x : \phi(n) = \Box\} \ge x^{1-\delta+o(1)} \quad \textit{as} \quad x \to \infty.$$

Erdős [11] proved in 1935 that there exists $\delta < 1$ such that (2) holds. It is believed that (2) holds with *any* $\delta > 0$ but this has not been proved yet.

Pomerance was the first to find a specific value for $\delta < 1/2$ such that (2) holds. Many people (such as R. Baker, Balog, Harman and Friedlander, to mention only a few) worked on finding smaller and smaller values of $\delta$ such that (2) holds. State of the art: estimate (2) is known with $\delta = 1/3.3772$, with corresponding $1 - \delta = 0.7038$. Thus,

$$\#\{n \le x : \phi(n) = \Box\} > x^{0.7038}. \tag{3}$$

In this form it was proved in 2004 by Banks, Friedlander, Pomerance and Shparlinski [2]. There are $x^{1/2}$ squares $m \le x$. So, in a fair world, there should be only about $x^{1/2}$ values for $n \le x$ such that $\phi(n) = \Box$, whereas estimate (3) tells us that there are considerably more such values for $n$. Thus, *squares are popular among totients*! Erdős showed in the same paper [11] in 1935 that for some $\delta < 1$ there are infinitely many $m$ such that

$$\#\{n : \phi(n) = m\} > m^{1-\delta}.$$

In fact, his proof shows that we can take $\delta$ such that (2) holds. Such values of $m$ are also *popular*. Of course, the same applies to $\sigma$.

Here is a heuristic due to Erdős concerning $\sigma$-values and amicable numbers. Say (2) holds with all $\delta > 0$. Put $\delta = \varepsilon > 0$, some very small positive number. Then for large $x$ there is some $m < x$ such that if we put

$$\mathcal{A} = \{n \le x : \sigma(n) = m\} \quad \text{then} \quad \#\mathcal{A} > x^{1-\varepsilon}.$$

The number of solutions of the equation

$$n_1 + n_2 = m \quad \text{with} \quad n_1,\ n_2 \in \mathcal{A}$$

should be $x^{1-2\varepsilon}$. Each such solution leads to

$$n_2 = m - n_1 = \sigma(n_1) - n_1 = s(n_1)$$

and vice versa, so $(n_1, n_2)$ is an amicable pair. *Conclusion: There should be $x^{1+o(1)}$ amicable numbers $n \le x$ as $x \to \infty$.* (Let $a(x)$ be the number of amicable pairs $(n_1, n_2)$, $n_1 < n_2$. This number is known for all values of $x \le 10^{14}$ [32]. The 4-decimal values of $(\log a(x))/(\log x)$ for $x = 10^j$, $j = 5, \ldots, 14$, are 0.2228, 0.2705, 0.2905, 0.2966, 0.3075, 0.3154, 0.3203, 0.3236, 0.3264, 0.3282. The data would seem to suggest that the ratio $(\log a(x))/(\log x)$ may converge somewhere close to $1/3$.)

This procedure of Erdős was tried out by te Riele in [38]. He proposed an algorithm to solve the equation $\sigma(n) = m$ recursively by finding a divisor $\sigma(p^e)$ of $m$ for some prime power $p^e$ and then solve the equation $\sigma(k) = m/\sigma(p^e)$: $n = p^e k$ then solves $\sigma(n) = m$. One may expect the equation $\sigma(n) = m$ to have many solutions if $m$ has many divisors, i.e., if $m$ is *smooth*. If that number of solutions is about $\sqrt{m}$, the number of *pairs of solutions* is about $\frac{1}{2}m$, so then there is a good chance that there are pairs of solutions which sum up to $m$ (provided that the solutions behave like randomly distributed numbers). By carrying out this algorithm for many smooth numbers $m$, including factorials, te Riele found more than 700 new amicable pairs. For example, for $m = 16!$ he found 2183888 solutions $n$ of $\sigma(n) = m$ (with $2183888 \approx 0.4774\sqrt{16!}$), and among these there are four pairs which sum up to $m$, giving four amicable pairs.

### $\phi$ and $\sigma$

Starting with about 50 years ago, Erdős [13] asked whether one can prove that the equation

$$\phi(m) = \sigma(n) \tag{4}$$

has infinitely many positive integer solutions $(m, n)$. If $p$ and $p + 2$ are both primes then

$$\phi(p+2) = p+1 = \sigma(p). \tag{5}$$

If $2^p - 1$ is prime, then

$$\phi(2^{p+1}) = 2^p = \sigma(2^p - 1).$$

Observe that

$$n! = \prod_{p\le n}(p-1)\prod_{p\le n} p^{e_p} = \phi(m),$$

where $m = \prod_{p\le n} p^{e_p+1}$. Maybe it is true that $n!$ is also a value of $\sigma$ infinitely often.

**Theorem 7** (Ford, Luca, Pomerance [16]). *There exists a constant $a > 0$ such that for large $x$, the number of common values of $\phi(n)$ and $\sigma(m)$ which are at most $x$ is $> \exp((\log\log x)^a)$.*

Here are some of the things that go into the proof of Theorem 7. There is an easy criterion for producing totients. Namely, if

$$\prod_{p|n}(p-1) \mid n \quad \text{then} \quad n = \phi(m) \quad \text{for some } m. \tag{6}$$

We start with a $\sigma$-value and use (6) to see that it is a $\phi$-value. Let

$$n = \prod_{p\in\mathcal{S}}(p+1), \tag{7}$$

where $\mathcal{S}$ is a large set of primes $p \le x$ such that $P(p+1) \le y$, where $y = x^{1/2-\eta}$ with some small $\eta$. The number in (7) is a product of small primes $p \le y$ each at some hopefully large power. To exploit implication (6) we need to know something about the distribution of the primes in $\mathcal{S}$ modulo $p \le y$. This is governed by zeros of *$L$-functions*. The $L$-functions, used by Dirichlet in his proof about primes in progressions modulo $m$ are like the Riemann zeta function

$$\zeta(s) = \sum_{n\ge1}\frac{1}{n^s},$$

but twisted by some character modulo $m$. $L$-functions might have some badly behaved zeros called *Siegel zeros*, which are zeros whose real part is very close to 1. They have profound implications on the distribution of primes in arithmetic progressions with the appropriate modulus and most proofs try to avoid this issue. It turns out that in the case of the proof of Theorem 7 Siegel zeros were quite helpful because of the following result.

**Theorem 8** (Heath-Brown [21]). *If $\chi$ is a primitive character modulo $m$ and $L(s,\chi) = 0$ for $s = 1 - \lambda(\log m)^{-1}$, then for $m^{300} < z \le m^{500}$, the number of primes $p \le z$ with $p+2$ prime is*

$$C\frac{z}{\log^2 z} + O\left(\frac{\lambda z}{\log^2 z}\right) \quad \textit{with} \quad C = 2\prod_{p>2}(1-(p-1)^{-2}) = 1.32\ldots.$$

So Siegel zeros imply twin primes! Thus, one could deal with the possible existence of Siegel zeros thanks to the fact that they imply the presence of twin primes, hence to solutions of equation (5). Still there might be some other bad zeros creating irregularities in the distribution of primes in progressions which have to be handled in a different way. Furthermore, something interesting happens, say if $q \le y$ is a prime that does not divide the number shown at (7), but for which we would like to apply (6). Namely,

$$q \nmid n \Rightarrow p \nmid n \quad \text{for all primes} \quad p \equiv 1 \pmod q. \tag{8}$$

Say $p_1 \equiv 1 \pmod q$, and $p_1 \nmid n$. By (8), we have

$$p_1 \nmid n \Rightarrow p \nmid n \quad \text{for all primes} \quad p \equiv 1 \pmod{p_1}.$$

Iterating, we get that $n$ is free of all primes $p$ such that there is a chain of primes

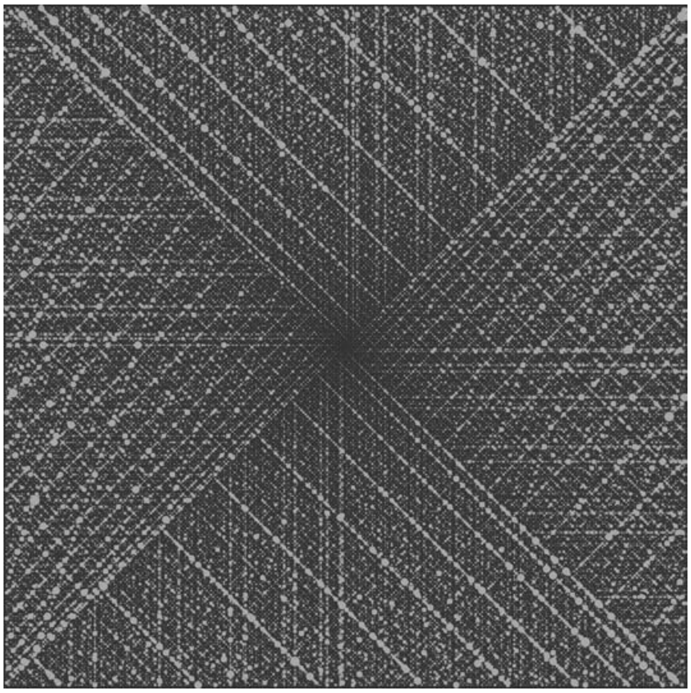
$$q \prec p_1 \prec p_2 \prec \cdots \prec p_k = p, \tag{9}$$

where $a \prec b$ means that $b \equiv 1 \pmod a$, and $q$ is any prime not dividing $m$. To deal with this issue, one needs a bound for the counting function $N(q;x)$ of the number of *prime chains* of the form (9) with $p \le x$. Luckily, this was done previously in a joint work of Ford et al. [15]. Namely, they proved the following result.

**Theorem 9** (Ford et al. [15]). *For every $\varepsilon > 0$, there exists a contant $C_\varepsilon$ such that uniformly for $q \le x$ we have*

$$N(q;x) \le C_\varepsilon\left(\frac{x}{q}\right)^{1+\varepsilon}.$$

Putting everything together and using some combinatorial arguments for the counting, one does get that equation (4) has infinitely many solutions even in the effective form claimed by Theorem 7.



In this graphic the natural numbers are arranged as in the Ulam spiral and a disk of size proportional to the number of divisors is drawn for each number: this yields an intriguing, yet not fully understood pattern.

There are many other nice problems dealing with equations involving the functions $\phi$ and $\sigma$ which are still open. We close this paper by recalling the following one proposed in [16].

**Problem**. *Show that there are infinitely many solutions* $(m, n)$ *to the equation* $\phi(m) = \sigma(n)$ *with* $m$ *square-free.*

## References


1 W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math. (2)* **139** (1994) 703–722.

2 W.D. Banks, J.B. Friedlander, C. Pomerance, and I.E. Shparlinski, Multiplicative structure of values of the Euler function, pp. 29–47 in: Alf van der Poorten and Andreas Stein (eds.), *High Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams*, Fields Inst. Comm. **41** AMS, 2004.

3 J. Bayless and D. Klyve, On the sum of reciprocals of amicable numbers, *Integers*, to appear.

4 N.G.W.H. Beeger, On even numbers $m$ dividing $2^m - 2$, *Amer. Math. Monthly* **58** (1951) 553–555.

5 R.P. Brent, G. L. Cohen, and H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Math. Comp.* **57** (1991) 857–868.

6 K. Broughan, M. González, R. Lewis, F. Luca, J. Mejía, A. Togbé, There are no multiply perfect Fibonacci numbers, *Integers*, to appear.

7 R.D. Carmichael, On Euler's $\phi$–function, *Bull. Amer. Math. Soc.* **13** (1907) 241–243.

8 R.D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–1910) 232–238.

9 E. Catalan, Propositions et questions diverses, *Bull. Soc. Math. France* **16** (1888) 128–129.

10 L. Dickson, Theorems and tables on the sum of the divisors of a number, *Quart. J. Math.* **44** (1913) 264–296.

11 P. Erdős, On the normal number of prime factors of $p - 1$ and some other related problems concerning Euler's $\phi$ function, *Quart. J. Math. (Oxford Ser.)* **6** (1935) 205–213. 38

12 P. Erdős, On amicable numbers, *Publ. Math. Debrecen* **4** (1955) 108–111.

13 P. Erdős, Remarks on number theory, II. Some problems on the $\sigma$ function, *Acta Arith.* **5** (1959) 171 – 177.

14 K. Ford, The number of solutions of $\phi(x) = m$, *Ann. Math.* **150** (1999) 283–311.

15 K. Ford, F. Luca and S. Konyagin, Prime chains and Pratt trees, *GAFA*, to appear.

16 K. Ford, F. Luca and C. Pomerance, Common values of the arithmetic functions $\phi$ and $\sigma$, *Bull. London Math. Soc.* **42** (2010) 478–488.

17 D. Gale, Mathematical Entertainments, *The Mathematical Intelligencer* **13** (1991) 40.

18 M. García, J. M. Pedersen, and H. J. J. te Riele, Amicable numbers – a Survey, pp. 179–197 in: Alf van der Poorten and Andreas Stein (eds.), *High primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams*, Fields Institute Communications **41**, AMS, 2004.

19 R.K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, Third Edition, 2004.

20 R.K. Guy and J. L. Selfridge, What drives an aliquot sequence?, *Math. Comp.* **29** (1975) 101–107; erratum in **34** (1980) 319–321, collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

21 D.R. Heath-Brown, Prime twins and Siegel zeros, *Proc. London Math. Soc. (3)* **47** (1983) 193–224.

22 M. Kobayashi, P. Pollack, and C. Pomerance, On the distribution of sociable numbers, *J. Number Theory* **129** (2009) 1990–2009.

23 M. Křížek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers*, CMS Books in Mathematics, Springer, 2002.

24 H.W. Lenstra, Problem 6064, *Amer. Math. Monthly* **82** (1975) 1016.

25 F. Luca, Problem 10711, *Amer. Math. Monthly* **106** (1999) 166.

26 F. Luca, Perfect Fibonacci and Lucas numbers, *Rend. Circ. Mat. Palermo*, Ser II **49** (2000) 313–318.

27 F. Luca, Fibonacci numbers with the Lehmer property, *Bull. Pol. Acad. Sci. Math.* **55** (2007) 7–15.

28 F. Luca and C. Pomerance, On the radical of a perfect number, *New York J. Math.* **16** (2010) 23–30.

29 P.P. Nielsen, Odd perfect numbers have at least nine distinct prime factors. *Math. Comp.* **76** (2007) 2109–2126.

30 A. Nitaj, *The ABC conjecture home page*, http://www.math.unicaen.fr/~nitaj/abc.html

31 P. Ochem, http://www.lri.fr/~ochem/opn

32 J. M. Pedersen, *Known Amicable Pairs*, http://amicable.homepage.dk/knwnap.htm

33 P. Pollack, Perfect numbers with identical digits, *Integers*, to appear.

34 C. Pomerance, Odd perfect numbers are divisible by at least seven distinct primes, *Acta Arithm.* **25** (1973/74) 265–300.

35 C. Pomerance, On the distribution of amicable numbers, *J. reine angew. Math.* **293/294** (1977) 217–222.

36 C. Pomerance, On the distribution of amicable numbers, II, *J. reine angew. Math.* **325** (1981) 183–188.

37 C. Pomerance, On composite $n$ for which $\phi(n) \mid n-1$, *Acta Arith.* **28** (1976) 387–389; II, *Pacific J. Math* **69** (1977) 177–186; see also *Notices Amer. Math. Soc.* **22** (1975) A542.

38 H.J.J. te Riele, A new method for finding amicable pairs, pp. 577–581 in: Walter Gautschi (ed.), *Mathematics of Computation 1943–1993: a half-century of computational mathematics*, Proc. Symp. Appl. Math. **43** (1994), AMS, Providence, RI.

39 N.J.A. Sloane, *The On-line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences