The ranges of some familiar arithmetic functions

Carl Pomerance
Dartmouth College, emeritus
University of Georgia, emeritus

based on joint work with
K. Ford, F. Luca, and P. Pollack
and T. Freiburg, N. McNew, and H.-S. Yang

Elementary number theory has many basic functions, like:

- $\sigma(n)$, the sum of the postive divisors of n,
- $s(n) = \sigma(n) - n$, the sum of the "proper" divisors of n,
- $\tau(n)$, the number of positive divisors of n,
- $\omega(n)$, the number of primes dividing n,
- $\varphi(n)$, the number of integers in $[1, n]$ coprime to n,

and many more.

When one has a function, one can ask various statistical questions about it.

For example: How big can it be? How small? What is it on average? Normally? How are its values distributed? How close is it to being one-to-one? What is its set of values?

This talk is aimed at the last question, the set of values of an arithmetic function.

And to get started, we note that $\tau(n)$, the number of divisors of n, can take any positive integral value, merely note that $\tau(2^k) = k + 1$. And $\omega(n)$, the number of primes dividing n, can take any nonnegative integral value.

The other functions mentioned at the start, namely σ (sum-of-divisors function), s (sum-of-proper-divisors function), and φ (Euler's function), are a bit trickier.

We introduce one more function that has some interest:

$\lambda(n)$, the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^*$.

Note that this group, which has order $\varphi(n)$, is the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$. The exponent of a group is the least positive integer k such every element has order dividing k. In a finite abelian group, this is just the maximal order of an element. We always have $\lambda(n) \mid \varphi(n)$, and when the group is cyclic, they are equal, for example, when n is prime.

The oldest of σ, s, φ, and λ is $s(n) = \sigma(n) - n$, going back to Pythagoras. He was interested in fixed points ($s(n) = n$) and 2-cycles ($s(n) = m$, $s(m) = n$) in the dynamical system given by iterating s.

Very little is known after millennia of study, but we do know that the number of $n \le x$ with $s(n) = n$ is at most x^ϵ (Hornfeck & Wirsing, 1957) and that the number of $n \le x$ with n in a 2-cycle is at most $x/\exp((\log x)^{1/2})$ for x large (P, 2014).

The study of the comparison of $s(n)$ to n led to the theorems of Schoenberg, Davenport, and Erdős & Wintner. And the dawn of probabilistic number theory.

Erdős was the first to consider the set of values of $s(n)$. Note that if $p \neq q$ are primes, then $s(pq) = p + q + 1$, so that:

If: *All even integers at least* 8 *are the sum of* 2 *unequal primes*,

Then: *All odd numbers at least 9 are values of* s.

Also, $s(2) = 1$, $s(4) = 3$, and $s(8) = 7$, so presumably the only odd number that's not an s-value is 5. It's known that this slightly stronger form of Goldbach is almost true in that the set of evens not so representable as $p + q$ has density 0.

Thus: *the image of* s *contains almost all odd numbers.*

But what of even numbers?

Erdős (1973): *There is a positive proportion of even numbers missing from the image of* s.

But what of even numbers?

Erdős (1973): *There is a positive proportion of even numbers missing from the image of* s.

Chen & Zhao (2011): *At least* $(0.06 + o(1))x$ *even numbers in* $[1, x]$ *are not of the form* $s(n)$.

But what of even numbers?

Erdős (1973): *There is a positive proportion of even numbers missing from the image of* s.

Chen & Zhao (2011): *At least* $(0.06 + o(1))x$ *even numbers in* $[1, x]$ *are not of the form* $s(n)$.

P & Yang (2014): Computationally it is appearing that about $\frac{1}{6}x$ even numbers to x are not of the form $s(n)$.

But what of even numbers?
Erdős (1973): *There is a positive proportion of even numbers missing from the image of* s.

Chen & Zhao (2011): *At least* $(0.06+o(1))x$ *even numbers in* $[1,x]$ *are not of the form* $s(n)$.

P & Yang (2014): Computationally it is appearing that about $\frac{1}{6}x$ even numbers to x are not of the form $s(n)$.

Pollack & P (2015): Heuristically, the density of numbers not of the form $s(n)$ is

$$\lim_{y\to\infty}\frac{1}{\log y}\sum_{\substack{a\le y\\ 2|a}}\frac{1}{a}e^{-1/s(a)}\approx 0.172.$$

Can it at least be proved that the image of s has a positive proportion of even numbers?

Yes, it can.

Luca & P (2015): *In any residue class $a \pmod{m}$, there is a positive proportion of members of the form $s(n)$.*

The details are worked out only in the case of 0 (mod 2). We load things in our favor by taking “normal” even numbers n which have a fairly large prime factor, and a few other properties designed to help out with the proof. We need to show that for our restricted set we don’t have too many values that arise in more than one way. This involves studying the equation

$$s(mp) = s(m'p'), \quad (\text{so } ps(m) + \sigma(m) = p's(m') + \sigma(m'))$$

where p, p' are the largest prime factors of the respective numbers. We then fix m, m' and use a sieve to upper bound the number of choices of m, m'. The proof gets messy. If there's time, a few details will be given at the end of the talk.

Unsolved: *Prove that if $\mathcal{A}$ contains a positive proportion of natural numbers, so does $s(\mathcal{A})$.* This is a conjecture of Erdős, Granville, P, and Spiro.

This conjecture would imply a conjecture of Erdős: *But for a set of asymptotic density* 0*, if $n > s(n)$, then $n > s(n) > s_2(n) > \cdots > s_k(n)$, where s_k denotes the k-fold iteration.* It is a theorem of Erdős that this holds for increasing aliquot sequences.

The set of values of φ was first considered by Pillai (1929): *The number $V_\varphi(x)$ of φ-values in $[1, x]$ is $O(x/(\log x)^c)$, where* $c = \frac{1}{e} \log 2 = 0.254 \ldots$.

Pillai's idea: There are not many values $\varphi(n)$ when n has few prime factors, and if n has more than a few prime factors, then $\varphi(n)$ is divisible by a high power of 2.

The set of values of φ was first considered by Pillai (1929): *The number $V_\varphi(x)$ of φ-values in $[1, x]$ is $O(x/(\log x)^c)$, where* $c = \frac{1}{e}\log 2 = 0.254\dots$.

Pillai's idea: There are not many values $\varphi(n)$ when n has few prime factors, and if n has more than a few prime factors, then $\varphi(n)$ is divisible by a high power of 2.

Erdős (1935): $V_\varphi(x) = x/(\log x)^{1+o(1)}$.

Erdős's idea: Deal with $\Omega(\varphi(n))$ (the total number of prime factors of $\varphi(n)$, with multiplicity). This paper was seminal for the various ideas introduced. For example, the proof of the infinitude of Carmichael numbers owes much to this paper.

Again: $V_\varphi(x) = x/(\log x)^{1+o(1)}$.
But: A great deal of info may be lurking in that "$o(1)$".

After work of Erdős & Hall, Maier & P, and Ford, we now know that $V_\varphi(x)$ is of magnitude

$$\frac{x}{\log x}\exp\left(A(\log_3 x - \log_4 x)^2 + B\log_3 x + C\log_4 x\right),$$

where $\log_k$ is the k-fold iterated log, and A, B, C are explicit constants.

Unsolved: Is there an asymptotic formula for $V_\varphi(x)$?
Do we have $V_\varphi(2x) \sim 2V_\varphi(x)$?

The same results and unsolved problems pertain as well for the image of σ.

In 1959, Erdős conjectured that the image of σ and the image of φ has an infinite intersection; that is, there are infinitely many pairs m, n with

$$\sigma(m) = \varphi(n).$$

It is amazing how many famous conjectures imply that the answer is yes!

Yes, if there are infinitely many twin primes:

If p, $p+2$ are both prime, then

$$\varphi(p+2) = p+1 = \sigma(p).$$

Yes, if there are infinitely many twin primes:

If p, $p+2$ are both prime, then

$$\varphi(p+2) = p+1 = \sigma(p).$$

Yes, if there are infinitely many Mersenne primes:

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

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

Yes, if there are infinitely many twin primes:

If p, $p+2$ are both prime, then

$$\varphi(p+2) = p+1 = \sigma(p).$$

Yes, if there are infinitely many Mersenne primes:

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

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

Yes, if the Extended Riemann Hypothesis holds.

It would seem to be promising to prove that there are at most finitely many solutions to $\sigma(m) = \varphi(n)$; it has some amazing and unexpected corollaries!

However, Ford, Luca, & P (2010): There are indeed infinitely many solutions to $\sigma(m) = \varphi(n)$.

We gave several proofs, but one proof uses a conditional result of Heath-Brown: *If there are infinitely many Siegel zeros, then there are infinitely many twin primes.*

Some further results:

Garaev (2011): *For each fixed number a, the number $V_{\varphi,\sigma}(x)$ of common values of φ and σ in $[1, x]$ exceeds* $\exp\left((\log\log x)^a\right)$ *for x sufficiently large.*

Ford & Pollack (2011): *Assuming a strong form of the prime k-tuples conjecture, $V_{\varphi,\sigma}(x) = x/(\log x)^{1+o(1)}$.*

Ford & Pollack (2012): *Most values of φ are not values of σ and vice versa.*

The situation for Carmichael's function λ has only recently become clearer. Recall that $\lambda(p^a) = \varphi(p^a)$ unless $p = 2, a \geq 3$, when $\lambda(2^a) = 2^{a-2}$, and that

$$\lambda(\mathrm{lcm}[m, n]) = \mathrm{lcm}[\lambda(m), \lambda(n)].$$

It is easy to see that the image of φ has density 0, just playing with powers of 2 as did Pillai. But what can be done with λ? It's not even obvious that λ-values that are 2 mod 4 have density 0.

The solution lies in the "anatomy of integers" and in particular of shifted primes. It is known (Erdős & Wagstaff) that most numbers do not have a large divisor of the form $p - 1$ with p prime. But a λ-value has such a large divisor or it is "smooth", so in either case, there are not many of them.

Using these thoughts, Erdős, P, & Schmutz (1991): *There is a positive constant c such that $V_\lambda(x)$, the number of λ-values in $[1,x]$, is $O(x/(\log x)^c)$.*

Using these thoughts, Erdős, P, & Schmutz (1991): *There is a positive constant* c *such that* $V_\lambda(x)$*, the number of* λ*-values in* $[1,x]$*, is* $O(x/(\log x)^c)$*.*

Friedlander & Luca (2007): *A valid choice for* c *is* $1-\frac{e}{2}\log 2 = 0.057\dots$ *.*

Using these thoughts, Erdős, P, & Schmutz (1991): *There is a positive constant c such that $V_\lambda(x)$, the number of λ-values in $[1, x]$, is $O(x/(\log x)^c)$.*

Friedlander & Luca (2007): *A valid choice for c is* $1 - \frac{e}{2}\log 2 = 0.057\ldots$.

Banks, Friedlander, Luca, Pappalardi, & Shparlinski (2006): $V_\lambda(x) \geq \frac{x}{\log x}\exp\Big((A + o(1))(\log_3 x)^2\Big)$.

So, $V_\lambda(x)$ is somewhere between $x/(\log x)^{1+o(1)}$ and $x/(\log x)^c$, where $c = 1 - \frac{e}{2}\log 2$.

Recently, Luca & P (2013): $V_\lambda(x) \le x/(\log x)^{\eta+o(1)}$, *where* $\eta = 1 - (1+\log\log 2)/\log 2 = 0.086\ldots$.
Further, $V_\lambda(x) \ge x/(\log x)^{0.36}$ *for all large* x.

More recently:
(Ford, Luca, & P, 2014). The "correct" exponent is η

The constant η actually pops up in some other problems:

Erdős (1960): *The number of distinct entries in the* $N \times N$ *multiplication table is* $N^2/(\log N)^{\eta+o(1)}$.

The asymptotic density of integers with a divisor in the interval $[N, 2N]$ *is* $1/(\log N)^{\eta+o(1)}$. This result has its own history beginning with Besicovitch in 1934, some of the other players being Erdős, Hooley, Tenenbaum, and Ford.

The constant $\eta = 1 - (1 + \log\log 2)/\log 2 = 0.86\ldots$ has even shown up in a very new result on torsion subgroups of elliptic curves:

Let $T(d)$ denote the maximal size of a torsion group for an elliptic curve over a number field of degree d over the rationals. After Merel, we know that $T(d) < \infty$, that is, there is some bound on the torsion that depends only on the degree d of the field. This bound is very large, but for CM-curves we know more. Let $T_{\mathsf{CM}}(d)$ denote the torsion bound for CM-curves. In a paper from earlier this year, Clark & Pollack showed that $T_{\mathsf{CM}}(d) \ll d \log\log d$ for $d \ge 3$.

McNew, Pollack, & P (2015): For $3 \le y \le x^{1-\epsilon}$, the number of degrees $d \le x$ with $T_{\mathsf{CM}}(d) > y$ is $x/(\log y)^{\eta + o(1)}$, as $x \to \infty$.

The proof is based on the lemma (due to Bourdon, Clark, & Pollack, 2015) that if $T_{\mathsf{CM}}(d) > y$, then d is divisible by some $\ell - 1$ for ℓ a prime with $\ell > y^{1-\epsilon}$. So, it becomes a problem in the "anatomy of integers".

Square values

Banks, Friedlander, P, & Shparlinski (2004): *There are more than* $x^{0.7}$ *integers* $n \le x$ *with* $\varphi(n)$ *a square. The same goes for* σ *and* λ*.*

Square values

Banks, Friedlander, P, & Shparlinski (2004): *There are more than $x^{0.7}$ integers $n \le x$ with $\varphi(n)$ a square. The same goes for σ and λ.*

Remark. There are only $x^{0.5}$ squares below x. (!)

Square values

Banks, Friedlander, P, & Shparlinski (2004): *There are more than $x^{0.7}$ integers $n \le x$ with $\varphi(n)$ a square. The same goes for σ and λ.*

Remark. There are only $x^{0.5}$ squares below x. (!)

Might there be a positive proportion of integers n with n^2 a value of φ?

Pollack & P (2014): No, the number of $n \le x$ with n^2 a φ-value is $O(x/(\log x)^{0.0063})$. The same goes for σ.

Unsolved: Could possibly almost all even squares be λ-values??

The exponent 0.0063 in my result with Pollack is not sharp. The best lower bound we have is:
Pollack & P (2014): The number of $n \le x$ with n^2 a φ-value is $\gg x/(\log x \log\log x)^2$.

So, the "correct" exponent on $\log x$ is somewhere between 0.0063 and 2.

But, we do know the order of magnitude of the number of pairs of primes $p, q \le x$ with $\varphi(pq)$ a square.
Freiburg & P (2015): It is $x/\log x$.

(So the number of $n \le x$ of the form pq with $\varphi(pq)$ a square is at least of order $\sqrt{x}/\log x$.)

Idea of the proof that a positive proportion of even numbers are values of $s(n) = \sigma(n) - n$ (Luca & P, 2014):

Consider even numbers n with several constraints:

- n is deficient (means that $s(n) < n$);

- $n = pqrk \in [\frac{1}{2}x, x]$ with $p > q > r > k$ and p, q, r primes;

- $k \le x^{1/60}, \quad r \in [x^{1/15}, x^{1/12}], \quad q \in [x^{7/20}, x^{11/30}]$;

- n is "normal".

If n satisfies these conditions, then $s(n) \le x$ is even.

Let $r(s)$ denote the number of representations of s as $s(n)$ from such numbers n.

We have $\sum_{s \le x} r(s) \gg x$.

The trick then is to show that $\sum_s r(s)^2 \ll x$. And for this, the sieve is useful.

In trying to generalize the proof to prove the conjecture of Erdős, Granville, P, & Spiro, the biggest stumbling block seems to be relaxing the condition that the largest prime p in n is very large. In particular, if $\mathcal{A}$ is the set of even numbers n with largest prime factor $< \sqrt{n}$, we don't know how to prove that $s(\mathcal{A})$ has positive lower density.

There is a very similar function to $s(n) = \sigma(n) - n$, namely

$$s_\varphi(n) = n - \varphi(n),$$

also known as the "cototient function". The proof that s hits almost all odd numbers works too for s_φ, and also the proof that s hits a positive proportion of numbers in any residue class works too for s_φ.

However, it is unsolved whether s_φ misses a postive proportion of evens. Pollack & P have a heuristic argument that it does, and even an estimate for the density missed, namely $\approx$ 0.09.

In any event, there's more work to do!

MERCI & THANK YOU