# The ranges of some familiar arithmetic functions

Max-Planck-Institut für Mathematik
2 November, 2016

Carl Pomerance, Dartmouth College

Let us introduce our cast of characters: $\varphi, \lambda, \sigma, s$

- Euler's function: $\varphi(n)$ is the cardinality of $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Carmichael's function: $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$.
- $\sigma$: the sum-of-divisors function.
- $s(n) = \sigma(n) - n$: the sum-of-proper-divisors function.

The functions $\varphi$ and $\sigma$ are *multiplicative*, which means that for coprime positive integers $m, n$ we have

$$\varphi(mn) = \varphi(m)\varphi(n), \qquad \sigma(mn) = \sigma(m)\sigma(n).$$

This leads to the formulas, where $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$,

$$\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1), \qquad \sigma(n) = \prod_{i=1}^{k} (p_i^{a_i+1} - 1)/(p_i - 1).$$

Note: For $n$ *squarefree*, that is $n = p_1 p_2 \dots p_k$, we have

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1), \qquad \sigma(n) = \prod_{i=1}^{k} (p_i + 1).$$

Recall that $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, the least positive integer $k$ such that $a^k \equiv 1 \pmod{n}$ for all $a$ coprime to $n$ (or the order of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$).

The function $\lambda$ is not multiplicative, but it also is determined multiplicatively: If $[m,n]$ denotes the lcm of $m,n$, then

$$\lambda([m,n]) = [\lambda(m), \lambda(n)].$$

Moreover, $\lambda(p^a) = \varphi(p^a)$ except when $p = 2$ and $a \geq 3$, and then $\lambda(2^a) = 2^{a-2} = \frac{1}{2}\varphi(2^a)$.

The function $s$, where $s(n) = \sigma(n) - n$ is a bit more awkward, multiplicatively speaking.

All 4 of our functions have the pleasant property that computing them is computationally equivalent to factoring. That is, they are easily computed via the formulas, given the prime factorization of $n$. On the other hand, there is a random, polynomial time algorithm that returns the prime factorization of $n$ given $n$ and $f(n)$, where $f$ is one of the four functions.

But this talk is concerned with the ranges of these functions, that is, the set of values they take.

The oldest of these functions 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 $n$ to $x$ with $s(n) = n$ is at most $x^{\epsilon}$ (Hornfeck & Wirsing, 1957) and that the number of $n$ to $x$ 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 birth 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:

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

implies

*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.*

Note that a set $A$ of positive integers has density $\delta$ if

$$\lim_{x\to\infty} \frac{1}{x} \sum_{\substack{a\in A \\ a\leq x}} 1 = \delta.$$

And when we say the image of $s$ contains "almost all odd numbers" we mean that the set of odd numbers *not* in the image of $s$ has density 0.

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* $s$.

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

P & H.-S. 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* $s$.

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

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

P. Pollack & P (2016): Heuristically the density of even numbers not in the image of $s$ exists and is equal to

$$\lim_{y\to\infty} \frac{1}{\log y} \sum_{\substack{a\le y\\ 2|a}} \frac{1}{a} e^{-a/s(a)} \approx .1718.$$

Note that the proportion to $10^{12}$, computed this year by A. Mosunov is $\approx .1712$.

Can we prove that $s$ actually hits a positive proportion of even numbers?

This had been an open problem until recently Luca & P proved it in 2014. The proof doesn't lend itself to getting a reasonable numerical estimate.

It is still unsolved if the range of $s$ has a density.

Let's look at the range of Euler's function $\varphi$. We'll show this set has density 0.

The values begin as

$$1, 2, 4, 6, 8, 10, 12, \ldots$$

Clearly all the values after 1 are even, so the set of values has density at most 1/2. Maybe it's 1/2?

Let's look at the range of Euler's function $\varphi$. We'll show this set has density 0.

The values begin as

$$1, 2, 4, 6, 8, 10, 12, \ldots$$

However, 14 is missing, and the values then continue

$$16, 18, 20, 22, 24, 28, 30, 32, \ldots.$$

It looks like a few numbers that are 2 mod 4 are missing. In fact, the only values that are 2 mod 4 are numbers $\varphi(p^a) = p^{a-1}(p-1)$ where $p$ is a prime that's 3 mod 4. That is, most 2 mod 4's are missing. So the values have density at most 1/4.

In general, note that if $n$ has at least $k$ odd prime divisors, then $2^k \mid \varphi(n)$, and the number of multiples of $2^k$ at most $x$ is $\leq x/2^k$.

Assume that $n = \varphi(m) \leq x$ and that $m$ has fewer than $k$ odd prime divisors. We have

$$\frac{m}{\varphi(m)} = \prod_{p \mid m} \left(1 - \frac{1}{p}\right)^{-1} = O(\log k),$$

using a 19th century result of Mertens. Since $\varphi(m) \leq x$, we have $m = O(x \log k)$.

So, from the prior slide, if $m$ has fewer than $k$ odd prime divisors and $\varphi(m) \leq x$, then

$$m = O(x \log k).$$

By a result of Hardy & Ramanujan, the number of integers $m \leq z$ with exactly $k$ prime divisors is

$$O\left(\frac{z}{\log z}\frac{(\log\log z + c)^{k-1}}{(k-1)!}\right).$$

Applying this with $z$ being the bound for $m$ just above, shows that for each fixed $k$ there are few $\varphi$ values in this case.

This method can be used to get a concrete upper bound for the number $V_\varphi(x)$ of $\varphi$-values to $x$.

Subbayya Sivasankaranarayana Pillai discovered the above approach and took $k \approx \frac{1}{\mathrm{e}} \log\log x$.

S. S. Pillai(1929): *We have* $V_\varphi(x) = O(x/(\log x)^c)$, *where* $c = \frac{1}{\mathrm{e}} \log 2 = 0.254\ldots$ .

This method can be used to get a concrete upper bound for the number $V_\varphi(x)$ of $\varphi$-values to $x$.

Subbayya Sivasankaranarayana Pillai discovered the above approach and took $k \approx \frac{1}{\mathrm{e}} \log\log x$.

S. S. Pillai(1929): *We have* $V_\varphi(x) = O(x/(\log x)^c)$, *where* $c = \frac{1}{\mathrm{e}} \log 2 = 0.254\ldots$ .

Clearly $V_\varphi(x) \geq (1 + o(1))x/\log x$.

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 $V_\varphi(2x) - V_\varphi(x) \sim V_\varphi(x)$?
(From Ford we have $V_\varphi(2x) - V_\varphi(x) \asymp V_\varphi(x)$.)

The same results and unsolved problems pertain as well for the image of $\sigma$.

In 1959, Erdős conjectured that the image of $\sigma$ and the image of $\varphi$ 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 a promising strategy to prove that there are at most finitely many solutions to $\sigma(m) = \varphi(n)$; it has some fantastic corollaries!

It would seem a promising strategy to prove that there are at most finitely many solutions to $\sigma(m) = \varphi(n)$; it has some fantastic 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 $\varphi$ and $\sigma$ in $[1,x]$ exceeds $\exp((\log\log x)^a)$ 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 $\varphi$ are not values of $\sigma$ and vice versa.*

The situation for Carmichael's function $\lambda$ 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

$$\lambda([m,n]) = [\lambda(m), \lambda(n)].$$

It is easy to see that the image of $\varphi$ has density 0, just playing with powers of 2 as did Pillai. But what can be done with $\lambda$? It's not even obvious that $\lambda$-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 $\lambda$-value has such a large divisor or it is "smooth" (aka "friable"), 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 $\lambda$-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 $\lambda$-values in $[1, x]$, is $O(x/(\log x)^c)$.*

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

Using these thoughts, Erdős, P, & Schmutz (1991): *There is a positive constant $c$ such that $V_\lambda(x)$, the number of $\lambda$-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): $V_\lambda(x) \geq \frac{x}{\log x} \exp\left((A + o(1))(\log_3 x)^2\right)$.

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* $x$.

Actually, the "correct" exponent is $\eta$ (Ford, Luca, & P, 2014).

The constant $\eta$ amazingly pops up in some other problems:

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

Erdős: *The asymptotic density of integers with a divisor in the interval* $[N, 2N]$ *is* $1/(\log N)^{\eta+o(1)}$.

McNew, Pollack, & P (2016): *The number of integers to* $x$ *divisible by some* $p - 1 > y$ *is* $x/(\log y)^{\eta+o(1)}$.

Here is a heuristic argument behind the theorem that $V_\lambda(x) \geq x/(\log x)^{\eta+o(1)}$.

Suppose we consider odd squarefree numbers $n$, say $n = p_1 p_2 \dots p_k$, with $\lambda(n) \leq x$. Now

$$\lambda(n) = [p_1 - 1, p_2 - 1, \dots, p_k - 1].$$

Assume each $p_i - 1 = a_i$ is squarefree. For each prime $p \mid a_1 a_2 \dots a_k$, let $S_p = \{i : p \mid a_i\}$. Then

$$[a_1, a_2, \dots, a_k] = \prod_{\substack{S \subset \{1,2,\dots,k\} \\ S \neq \emptyset}} \prod_{S_p = S} p = \prod_{\substack{S \subset \{1,2,\dots,k\} \\ S \neq \emptyset}} M_S, \quad \text{say,}$$

and the numbers $a_i$ $(= p_i - 1)$ can be retrieved from this factorization via $a_i = \prod_{i \in S} M_S$.

For example, say $n = 3 \cdot 31 \cdot 211$, so that

$$\lambda(n) = [2, 30, 210] = 2 \cdot 3 \cdot 5 \cdot 7.$$

We have

$$S_2 = \{1, 2, 3\}, \quad S_3 = \{2, 3\}, \quad S_5 = \{2, 3\}, \quad S_7 = \{3\}.$$

And for each $S \subset \{1, 2, 3\}$ with $S \neq \emptyset$, we have $M_S = 1$, except

$$M_{\{1,2,3\}} = 2, \quad M_{\{2,3\}} = 15, \quad M_{\{3\}} = 7.$$

Further,

$$\prod_{S \ni 1} M_S = 2, \quad \prod_{S \ni 2} M_S = 30, \quad \prod_{S \ni 3} M_S = 210.$$

Thus, a squarefree number $M$ is of the form $[p_1 - 1, p_2 - 1, \ldots, p_k - 1]$ if and only if $M$ has an ordered factorization into $2^k - 1$ factors $M_S$ indexed by the nonempty $S \subset \{1, 2, \ldots, k\}$, such that for $i \leq k$, the product of all $M_S$ with $i \in S$ is a shifted prime $p_i - 1$, with the $p_i$'s distinct.

What is the chance that a random squarefree $M \leq x$ has such a factorization?

We assume that $M$ is even. Then, for $M/2$, we ask for the product of the factors corresponding to $i$ to be half a shifted prime, $(p_i - 1)/2$.

The number of factorizations of $M/2$ is $(2^k-1)^{\omega(M/2)}$. Thus, the chance that $M=\lambda(n)$ with $\omega(n)=k$, $n$ squarefree, might be close to 1 if $(2^k-1)^{\omega(M/2)} > (\log x)^k$, that is,

$$\omega(M/2) > \frac{k\log\log x}{\log(2^k-1)} \approx \frac{\log\log x}{\log 2},$$

when $k$ is large. But the number of even, squarefree $M \le x$ with

$$\omega(M/2) \ge (1+o(1))\frac{\log\log x}{\log 2}$$

is $x/(\log x)^{\eta+o(1)}$.

This last assertion follows from the Hardy–Ramanujan inequality mentioned earlier (and the fact that it is fairly tight in this range).

**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* $\sigma$ *and* $\lambda$.

**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* $\sigma$ *and* $\lambda$*.*

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 $\sigma$ and $\lambda$.*

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 $\varphi$? To $10^8$, there are 26,094,797, or more than 50% of even numbers. But:

Pollack & P (2013): No, the number of $n \le x$ with $n^2$ a $\varphi$-value is $O(x/(\log x)^{0.0063})$. The same goes for $\sigma$.

Unsolved: Could possibly almost all even squares be $\lambda$-values??

Here's why this may be. Most $n \leq x$ have $\omega(n) > (1-\epsilon)\log\log x$. Thus, most $n \leq x$ have $\tau(n^2) > 3^{(1-\epsilon)\log\log x}$. For each $p^a \| n$, the number of $d \mid n^2/p^{2a}$ with $dp^{2a}+1$ prime might be $> 3^{(1-2\epsilon)\log\log x}/\log x$, and this expression is $> (\log x)^{\epsilon}$. So, most of the time, for each $p^a \| n$, there should be at least one such prime $dp^{2a}+1$. If $m$ is the product of all of the primes $dp^{2a}+1$ so found, we would have that $\lambda(m) = n^2$.

This is very similar to the heuristic for $V_\lambda(x)$. A proof anyone?

THANK YOU