Some new results on λ, φ, and σ

Carl Pomerance, Dartmouth College

The range of the Carmichael function λ

First discussed by Gauss, $\lambda(n)$ is the *exponent* of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. It is the smallest positive integer such that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for all a coprime to n.

So, for coprime m, n, $\lambda(mn) = \mathrm{lcm}[\lambda(m), \lambda(n)]$. And $\lambda(p^j) = \varphi(p^j)$ for prime powers p^j, except when $p = 2, j \geq 3$ in which case $\lambda(2^j) = 2^{j-2}$.

Clearly λ is very similar to Euler's function φ. They are nearly identical on prime powers, and for other numbers, one merely replaces

$$\varphi\left(\prod p_i^{a_i}\right) = \prod \varphi\left(p_i^{a_i}\right) \quad \text{with} \quad \lambda\left(\prod p_i^{a_i}\right) = \mathrm{lcm}\ \lambda\left(p_i^{a_i}\right).$$

Let $V_\varphi(x)$ denote the number of integers in $[1, x]$ that are values of φ, and similarly let $V_\lambda(x)$ denote the corresponding count for λ.

Clearly both $V_\varphi(x) \ge \pi(x)$ and $V_\lambda(x) \ge \pi(x)$, since $\varphi(p) = \lambda(p) = p - 1$ for each prime p.

We've known since 1935 (Erdős) that $V_\varphi(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$. This result was later refined by Erdős & Hall, Pomerance, Maier & Pomerance, and most recently Ford, who was able to find the correct order of $V_\varphi(x)$.

Being so similar to φ, one might expect similar results about the range of λ. But one big headache appears: while $\varphi(n) \le x$ implies $n \ll x \log\log x$ (in fact, the number of n with $\varphi(n) \le x$ is $\sim cx$, a result of Bateman), there can be extraordinarily huge numbers n with $\lambda(n) \le x$.

How huge? Try $\exp(x^{c/\log\log x})$.

In addition, there are $\gg x^{(\log x)^2}$ numbers n with $\lambda(n) \le x$.

So, with so many chances to hit numbers in $[1, x]$, it is not even clear that $V_\lambda(x)$, the number of λ-values in $[1, x]$, is $o(x)$.

But it is true; it follows from a lemma in

Erdős & Wagstaff, **1980**: *Let d_B be the upper density of those numbers n divisible by some $p-1$ with $p > B$ prime. Then $\lim_{B\to\infty} d_B = 0$.*

Note that if $\lambda(n)$ is not divisible by any $p-1$ with $p > B$ prime, then n is not divisible by any prime $p > B$, so $\lambda(n)$ has no prime factors $> B$. So, there are few such integers.

This argument was first outlined by Erdős, Pomerance, & Schmutz (1991) who claimed that $V_\lambda(x) \ll x/(\log x)^c$ for some $c > 0$.

Friedlander & Luca, (2007):

$$V_\lambda(x) \le x/(\log x)^{1-(e/2)\log 2+o(1)},$$

where $1-(e/2)\log 2 = 0.05791\ldots$.

Luca & Pomerance, (2009?):

$$V_\lambda(x) \le x/(\log x)^{1-(1+\log\log 2)/\log 2+o(1)},$$

where $1-(1+\log\log 2)/\log 2 = 0.08607\ldots$.

Towards a lower bound:

As mentioned, $V_\lambda(x) \geq \pi(x)$, so $V_\lambda(x) \gg x/\log x$.

Can we do better?

Banks, Friedlander, Luca, Pappalardi, & Shparlinski, (2006):

$$V_\lambda(x) \gg \frac{x}{\log x} \exp\left(c(\log\log\log x)^2\right).$$

So, what is your instinct? Is 1 the "correct" exponent on $\log x$ as with $V_\varphi(x)$, or is it some number smaller than 1?

Luca & Pomerance, (2009?):

$$V_\lambda(x) \gg \frac{x}{(\log x)^{3/5}}.$$

In fact, we show this for numbers $\lambda(n)$, where $n = pq$ with p, q primes. This seems counter-intuitive, since the number of integers $n = pq \le x$ is $\sim x \log\log x / \log x$. But recall, it is not $n \le x$ that we need, but $\lambda(n) \le x$.

So, let $R(x)$ be the number of triples a, b, d where $abd \le x$, $\gcd(a, b) = 1$, and $p = ad + 1, q = bd + 1$ are both prime. Then $\lambda(pq) = abd$, and except for possible overcounting, we have $V_\lambda(x) \ge R(x)$. But overcounting needs to be considered!

Assume $p \le \exp((\log x)^c)$ with c chosen appropriately. Say $\lambda(pq) = \lambda(p'q')$. If $R_1(x)$ is the number of times this happens with $q = q'$ and $R_2(x)$ is the number of times this happens with $q \ne q'$, then by Cauchy–Schwarz,

$$V_\lambda(x) \ge R(x)^2/(R_1(x) + R_2(x)).$$

In getting upper bounds for $R_1(x), R_2(x)$ we assume further that parameters a, b, d have close to a set number of prime divisors, where the settings are chosen to optimize the final estimate.

We have a heuristic argument (suggested to us by Granville) that our upper bound for $V_\lambda(x)$ is in fact the truth:

$$V_\lambda(x) = x/(\log x)^{c+o(1)}, \quad c = 1-(1+\log\log 2)/\log 2 = 0.08607\ldots.$$

The heuristic generalizes our construction using two primes to one using k primes. It remains to be seen how much can be proved.

The range of φ compared with the range of σ

Results on the range of φ may be carried over with little difficulty to the range of σ, the sum-of-divisors function. Fifty years ago, Erdős proposed the problem of showing there are infinitely many integers that are simultaneously values of both functions.

It is obviously true! For example, it would follow from the conjecture that there are infinitely many Mersenne primes (primes of the form $2^p - 1$), since σ of one of these is a power of 2, and every power of 2 is in the range of φ.

It also follows if there are infinitely many twin primes, since if $p, p+2$ are both primes, then $\sigma(p) = \varphi(p+2)$.

It is easy to see that every factorial number $k!$ is a value of φ, and presumably each of these is also a value of σ (except for $k = 2$). For these reasons, Erdős wrote it was a "very annoying" problem.

Some years ago I came up with a conditional proof on the ERH (Extended Riemann Hypothesis). The idea was to take σ of the product of those primes $p \le x$ where the greatest prime factor of $p - 1$ is below $x^{1/2-\varepsilon}$, and then show using the ERH that this was indeed a φ value. To do this, one need only show that for each prime q dividing the candidate number, we also have $q - 1$ dividing the number.

I used to mention in talks that it would be much more profitable to prove that the intersection of the ranges of φ and σ is *finite*, since corollaries would be

1. There are only finitely many Mersenne primes.

2. There are only finitely many twin primes.

3. The ERH is false.

Now in a joint papeer with Ford and Luca, we have found a proof of the Erdős conjecture, so unfortunately we have not proved any of those corollaries of the negation!

There are two key thoughts that go into the proof, which is modeled after the ERH argument. First, Heath-Brown had shown in 1983 that either there are infinitely many twin primes or there are no Siegel zeros (loosely speaking). So, if there are are only finitely many twin primes, we get to rigorously assume that a weak form of the ERH holds. Since it is only a weak form, there may be some exceptional primes that need to be dealt with, and for this we use a second idea: a new paper of Ford, Konyagin, & Luca on the distribution of primes p for which a given prime divides a given iterate of φ at p.