The range of Carmichael's function

Carl Pomerance, Dartmouth College

with

Florian Luca, UNAM, Morelia

Carmichael's function $\lambda(n)$ is related to Euler's function $\varphi(n)$. Concisely,

$$\varphi(n) \text{ is the order of the group } (\mathbb{Z}/n\mathbb{Z})^\times,$$

while

$$\lambda(n) \text{ is the exponent of the group } (\mathbb{Z}/n\mathbb{Z})^\times.$$

That is,

$$\lambda(n) \text{ is the order of the largest cyclic subgroup of } (\mathbb{Z}/n\mathbb{Z})^\times.$$

In formulas, we have for a prime power p^a that

$$\varphi(p^a) = (p-1)p^{a-1},$$

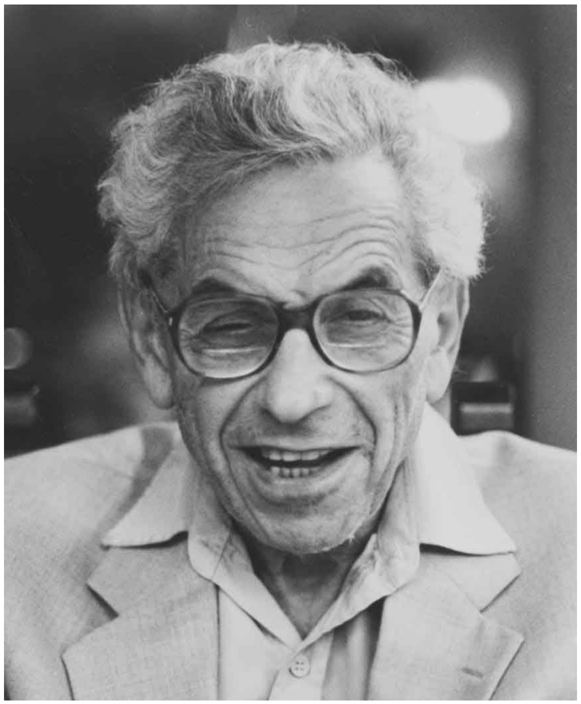
and

$$\lambda(p^a) = \begin{cases} \varphi(p^a), & \text{if } p > 2 \text{ or } a < 3, \\ \frac{1}{2}\varphi(p^a), & \text{if } p = 2 \text{ and } a \geq 3. \end{cases}$$

Further,

$$\varphi(n) = \prod_{p^a \| n} \varphi(p^a), \quad \lambda(n) = \text{lcm}[\lambda(p^a) : p^a \| n].$$

For such important and ubiquitous functions, it would seem good to be able to say something interesting about their ranges.



Let $V_f(x)$ denote the number of values of the nunction $f(n)$ that lie in $[1, x]$.

In 1935, Paul Erdős showed that

$$V_\varphi(x) = \frac{x}{(\log x)^{1+o(1)}}, \ x \to \infty.$$

After subsequent work by Erdős & Hall, Maier & P, and Ford, we now know the true order of magnitude of $V_\varphi(x)$, but we still don't have an asymptotic formula, nor do we know for example that $V_\varphi(2x)/V_\varphi(x) \to 2$ as $x \to \infty$.

However, we know much less about $V_\lambda(x)$. Clearly

$$V_\lambda(x) \ge (1+o(1))\frac{x}{\log x},\ x \to \infty,$$

since $\lambda(p) = p - 1$ for p prime.

In a paper from 1991 by Erdős, P, & Schmutz it was shown that there is a positive number c such that

$$V_\lambda(x) \le \frac{x}{(\log x)^c},\ \text{for all large } x.$$

In particular, the range of λ has asymptotic density 0.

The proof of this theorem uses a result of Erdős & Wagstaff proved in a paper of theirs on Bernoulli numbers. A lemma in that paper:

There is a positive constant c such that for $2 \le y \le x$, the number of integers $n \in [1, x]$ divisible by some $p - 1$, where $p \ge y$ is prime, is $O(x/(\log y)^c)$.

We apply this with $y = x^{1/\log\log x}$, say. Suppose $\lambda(n) \le x$. If this number is not divisible by any $p - 1$ with $p \ge y$, then n is not divisibly by any $p \ge y$, so that $\lambda(n)$ has only primes at most y. Standard estimates give that this set of numbers in $[1, x]$ has at most $O(x/\log x)$ elements. And if a value is divisible by some $p - 1$ with $p \ge y$, this puts the values in a set of cardinality $O(x/(\log y)^c) = x/(\log x)^{c+o(1)}$.

In a 2007 paper, Luca & Friedlander showed that

$$V_\lambda(x) \le \frac{x}{(\log x)^{c_0+o(1)}},\ c_0 = 1 - (e \log 2)/2 = 0.05791\ldots .$$

However, this can be improved to

$$V_\lambda(x) \le \frac{x}{(\log x)^{c_1+o(1)}},\ c_1 = 1-(1+\log\log 2)/\log 2 = 0.08607\ldots ,$$

(Luca & P). The exponent c_1 is known as the Erdős–Ford–Tenenbaum constant: Erdős showed in 1960 that the number of distinct entries in the $N \times N$ multiplication table is $N^2/(\log N)^{c_1+o(1)}$, a result subsequently refined by Tenenbaum and later by Ford.

A heuristic argument can be fashioned to suggest that

$$V_\lambda(x) = \frac{x}{(\log x)^{c_1+o(1)}},$$

(thanks to Granville for a helpful conversation regarding this).

So, this focuses attention then on the lower bound for $V_\lambda(x)$.

In 2006, Banks, Luca, Friedlander, Pappalardi, & Shparlinski "almost" showed that

$$V_\lambda(x) \gg V_\varphi(x),$$

but even all-the-way showing this does not give a lower bound of the shape

$$V_\lambda(x) \geq \frac{x}{(\log x)^c}, \quad \text{for some } c < 1.$$

Our principal new result (Luca & P):

There is a number c with $0 < c < 1$ such that

$$V_\lambda(x) \geq \frac{x}{(\log x)^c}, \quad \textit{for } x \textit{ large.}$$

It is a little unclear what the best (smallest) c can be gotten by our method. We have the details more-or-less written down for $c = 5/8$. The abstract for this talk announced that the result could be proved for $c = 3/5$. In preparing these slides, more careful estimates get c below $1/2$ down to about 0.457041. There is another strategy that can be tried ... . (Note that this talk is a "preliminary report"!)

How do we create many distinct values of $\lambda(n)$? We concentrate on numbers n of the form pq where $p < q$ are primes.

Wait a second: the number of integers $pq \le x$ is about $x(\log\log x)/\log x$, so how could this help?

Well, it is not $pq \le x$ that we are considering, but rather $\lambda(pq) = [p-1, q-1] \le x$. Thus, we are counting distinct integers of the form $abd \le x$ where $\gcd(a,b) = 1$, $ad + 1 = p$ is prime, and $bd + 1 = q$ is prime. Let $r(n)$ be the number of such representations of n as abd. Then, by Cauchy–Schwarz,

$$V_\lambda(x) \ \ge \ \frac{\left(\sum_{n\le x} r(n)\right)^2}{\sum_{n\le x} r(n)^2}.$$

$$V_\lambda(x) \;\geq\; \frac{\left(\sum_{n\leq x} r(n)\right)^2}{\sum_{n\leq x} r(n)^2}.$$

By choosing conditions for a, b, d well we can limit the size of the denominator without sacrificing too much in the numerator, and so get a decent lower bound for $V_\lambda(x)$.

For example, one choice of conditions that works fairly well: Choose $y = \exp((\log x)^\alpha)$, where $0 < \alpha < 1$ and $p = ad + 1 \in (y^{1/2}, y]$. Choose p so that $p - 1 = ad$ has about $\log\log y$ prime factors. Choose $d \mid p - 1$ so that $d < \sqrt{p}$ and d has about $\delta \log\log y$ prime factors. And choose b so that $bd \le x/a$, $bd + 1$ is prime, and b has about $\log\log y$ prime factors in $[1, y]$. Then, compute like crazy and find that an optimal choice for α is near 0.787 and an optimal choice for δ is near 0.542. This gives an estimate greater than $x/(\log x)^{1/2}$ for a lower bound for $V_\lambda(x)$.

The idea we will try next is to take p with $p - 1$ having close to $\beta \log\log y$ prime factors, where β is not necessarily 1, and similarly taking b with about $\gamma \log\log y$ prime factors. Fine tuning will yield perhaps a larger lower bound for $V_\lambda(x)$.

THANK YOU

MAHALO