Small values of Carmichael's λ-function

Paul Pollack

University of Georgia

partially joint work with Kai (Steve) Fan

The extravagant Euler

Euler's theorem

Let $n \geq 1$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where

$$\varphi(n) = \prod_{p^k \| n} p^{k-1}(p-1).$$



Leonhard Euler

The extravagant Euler

Euler's theorem

Let $n \geq 1$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where

$$\varphi(n) = \prod_{p^k \| n} p^{k-1}(p-1).$$



Leonhard Euler

Gauss–Carmichael theorem

Let $n \geq 1$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then

$$a^{\lambda(n)} \equiv 1 \pmod{n},$$

where

$$\lambda(n) \text{ “}=\text{”} \operatorname{lcm}_{p^k \| n}[p^{k-1}(p-1)];$$

the scare quotes mean that when $p = 2$ and $k \geq 3$, we replace p^{k-1} with p^{k-2}. Moreover, $\lambda(n)$ is the least positive exponent that works for every a coprime to n.



R. D. Carmichael

What sorcery is this?

Certainly, $\varphi(n) < n$ for all $n > 1$. But $\varphi(n)$ is never *that* much smaller than n: a 1903 theorem of Landau guarantees that $\varphi(n) \geq (e^{-\gamma} + o(1))n/\log\log n$ (which is sharp).

The story for λ is very different. For instance, consider

$$n = 844796819344392873681978325678053305083624871269983 \\ 308408218071576042914310.$$

What sorcery is this?

Certainly, $\varphi(n) < n$ for all $n > 1$. But $\varphi(n)$ is never *that* much smaller than n: a 1903 theorem of Landau guarantees that $\varphi(n) \geq (e^{-\gamma} + o(1))n/\log\log n$ (which is sharp).

The story for λ is very different. For instance, consider

$$n = 844796819344392873681978325678053305083624871269983 \\ 308408218071576042914310.$$

Here

$$\boxed{\varphi(n) = 113345395224968379331141577215315098464675353478880559104000000000000000000}$$

while . . .

What sorcery is this?

Certainly, $\varphi(n) < n$ for all $n > 1$. But $\varphi(n)$ is never *that* much smaller than n: a 1903 theorem of Landau guarantees that $\varphi(n) \geq (e^{-\gamma} + o(1))n/\log\log n$ (which is sharp).

The story for λ is very different. For instance, consider

$$n = 844796819344392873681978325678053305083624871269983 \\ 308408218071576042914310.$$

Here

$$\boxed{\varphi(n) = 113345395224968379331141577215315098464675353478880559104000000000000000000}$$

while . . .

$$\boxed{\lambda(n) = 27720.}$$

A mathematician is a magician who reveals their secrets

For squarefree N, we have $\lambda(N) = \mathrm{lcm}_{p|N}(p-1)$. Put

$$\omega^*(m) = \#\{p : \ p-1 \mid m\}, \qquad N(m) = \prod_{p-1|m} p.$$

Then

$$\boxed{\lambda(N(m)) \mid m.}$$

A mathematician is a magician who reveals their secrets

For squarefree N, we have $\lambda(N) = \operatorname{lcm}_{p|N}(p-1)$. Put

$$\omega^*(m) = \#\{p : \ p-1 \mid m\}, \qquad N(m) = \prod_{p-1|m} p.$$

Then

$$\boxed{\lambda(N(m)) \mid m.}$$

There are $\omega^*(27720) = 36$ primes p for which $p-1 \mid 27720$, namely

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 61,\ 67,\ 71,\ 73,\ 89,$$
$$127,\ 181,\ 199,\ 211,\ 281,\ 331,\ 397,\ 421,\ 463,\ 617,\ 631,\ 661,\ 991,$$
$$1321,\ 2311,\ 2521,\ 4621,\ 9241.$$

The n from the last slide is precisely $N(27720)$.

How small can $\lambda(n)$ be?

Adleman–Pomerance–Rumely (1983)

For some $c > 0$, and infinitely many m,

$$\omega^*(m) > \exp\left((c + o(1))\frac{\log m}{\log\log m}\right).$$



Carl Pomerance

In this case, taking $n = N(m)$, we get that

$$\boxed{\lambda(n) < (\log n)^{(1/c+o(1))\log\log\log n}.}$$

How small can $\lambda(n)$ be?

Adleman–Pomerance–Rumely (1983)

For some $c > 0$, and infinitely many m,

$$\omega^*(m) > \exp\left((c + o(1))\frac{\log m}{\log\log m}\right).$$



Carl Pomerance

In this case, taking $n = N(m)$, we get that

$$\boxed{\lambda(n) < (\log n)^{(1/c+o(1))\log\log\log n}.}$$

The shape of this bound is best possible, since they also proved that

$$\lambda(n) > (\log n)^{(1/\log 2+o(1))\log\log\log n}.$$

whenever $n \to \infty$.

c clearly (now)?

Fan–Pollack (2025)

The ω^* bound holds with the following constants:

	c	$C = 1/c$
Unconditionally	$0.6736 \log 2$	$2.141768\ldots$
Under GRH	$\log\left(\frac{1+\sqrt{5}}{2}\right)$	$2.078087\ldots$

c clearly (now)?

Fan–Pollack (2025)

The ω^* bound holds with the following constants:

	c	$C = 1/c$
Unconditionally	$0.6736 \log 2$	$2.141768\ldots$
Under GRH	$\log\left(\frac{1+\sqrt{5}}{2}\right)$	$2.078087\ldots$

APR conjecture $c = \log 2$ is admissible. Since

$$\omega^*(m) \le \tau(m) \le \exp\left((\log 2 + o(1))\frac{\log m}{\log\log m}\right),$$

that would be best possible. The APR conjecture would give infinitely many n with $\lambda(n) = (\log n)^{(1/\log 2 + o(1))\log\log\log n}$.

Out, liars!

Although $\lambda(n)$ can be very small, these examples are misleading. Typically, $\lambda(n) = n/\exp\{(1+o(1))(\log\log n)(\log\log\log n)\}$. More precisely:

Erdős–Pomerance–Schmutz (1991)

As $n \to \infty$ through a set of asymptotic density 1,

$$\boxed{\lambda(n) = \frac{n}{(\log n)^{\log\log\log n + A + o(1)}}},$$

where

$$A = -1 + \sum_p \frac{\log p}{(p-1)^2} = 0.2269688\ldots.$$

What can we say, more generally, about the distribution of $\lambda(n)$ values on $n \le x$?

The main event

Write $\log_k$ for the kth iterated logarithm, and put

$$L(x,y) = \#\{n \le x : \lambda(n) \le y\},$$

$$\mathcal{L}(x,y) = \exp\left(\frac{\log x \, \log_3 x}{\log_2 y}\right), \qquad \mathcal{L}(x) = \mathcal{L}(x,x).$$

Theorem (P., 2026)

Suppose y stays well above the minimal-order scale and well below the typical-order scale.

Then, as $x \to \infty$,

$$\boxed{\frac{L(x,y)}{x} \le \begin{cases} \mathcal{L}(x/y)^{-1+o(1)}, & y \ge \mathcal{L}(x)^2, \\ \mathcal{L}(x,y)^{-1+o(1)}, & y < \mathcal{L}(x)^2. \end{cases}}$$

Under Hypothesis U, equality holds in both cases.

The main event

Write $\log_k$ for the kth iterated logarithm, and put

$$L(x,y) = \#\{n \le x : \lambda(n) \le y\},$$

$$\mathcal{L}(x,y) = \exp\left(\frac{\log x \, \log_3 x}{\log_2 y}\right), \qquad \mathcal{L}(x) = \mathcal{L}(x,x).$$

Theorem (P., 2026)

Fix $\varepsilon > 0$. For $x, y \ge 100$, suppose $\exp((\log_2 x)^{1+\varepsilon}) \le y \le x\exp(-(\log_2 x)^{1+\varepsilon})$.

Then, as $x \to \infty$,

$$\boxed{\frac{L(x,y)}{x} \le \begin{cases} \mathcal{L}(x/y)^{-1+o(1)}, & y \ge \mathcal{L}(x)^2, \\ \mathcal{L}(x,y)^{-1+o(1)}, & y < \mathcal{L}(x)^2. \end{cases}}$$

Under Hypothesis U, equality holds in both cases.

A sampling of y values

Recall $L(x,y) = \#\{n \le x : \lambda(n) \le y\}$.

Threshold y	**Upper bound for $L(x,y)$**
$\sqrt{x}$	$\dfrac{x}{\mathcal{L}(x)^{1/2+o(1)}}$
$\exp(\sqrt{\log x})$	$\dfrac{x}{\mathcal{L}(x)^{2+o(1)}}$
$\exp((\log_2 x)^2)$	$x^{1/2+o(1)}$

Here $\mathcal{L}(x) = \exp\left(\dfrac{\log x \, \log_3 x}{\log_2 x}\right)$.

Under Hypothesis U, each exponent is sharp.

Hypothesis U

Let $P^*(r)$ be the largest prime power dividing r, with $P^*(1) = 1$. Put

$$\Pi^*(X, Y) = \#\{p \le X : P^*(p-1) \le Y\}.$$

Hypothesis U

Fix $\varepsilon > 0$. As X, Y and $u = \log X / \log Y$ tend to infinity, with $Y \ge (\log X)^{1+\varepsilon}$,

$$\boxed{\Pi^*(X, Y) = \pi(X) \exp\big(-(1 + o(1))u \log u\big).}$$

That is: shifted primes are powersmooth with the same (rough) relative frequency as ordinary integers of the same size. The upper bound in Hypothesis U is known, but we need the lower bound!

Similar conjectures have been used to study popular values of φ, perfect-power values of φ, and the distribution of Carmichael numbers.

Application to multiplicative orders

For odd n, let $\ell(n) := \mathrm{ord}_n(2)$ be the multiplicative order of 2 mod n.

We believe that $\ell(n)$ is usually almost as large as n itself. More precisely: For each fixed $\epsilon > 0$, asymptotically 100% of odd integers $n \leq x$ have

$$\ell(n) > x^{1-\epsilon}.$$

This is known for $\epsilon = 1/2$ but not for any smaller positive value of ϵ.

Application to multiplicative orders

For odd n, let $\ell(n) := \mathrm{ord}_n(2)$ be the multiplicative order of 2 mod n.

We believe that $\ell(n)$ is usually almost as large as n itself. More precisely: For each fixed $\epsilon > 0$, asymptotically 100% of odd integers $n \le x$ have

$$\ell(n) > x^{1-\epsilon}.$$

This is known for $\epsilon = 1/2$ but not for any smaller positive value of ϵ.

Corollary 1.2 (unconditional)

Fix $\delta > 0$. For all sufficiently large x,

$$\boxed{\#\{n \le x : n \text{ odd}, \ \ell(n) \le x^{\beta}\} \le \frac{x}{\mathcal{L}(x)^{1/2-\beta-\delta}}}$$

uniformly for $\beta \ge 0$.

What Erdős's conjecture would give

A conjecture of Erdős

For every $\varepsilon > 0$,

$$\#\{p \text{ odd prime} : \mathrm{ord}_p(2) = r\} \ll_\varepsilon r^\varepsilon.$$



Paul Erdős

What Erdős's conjecture would give



Paul Erdős

A conjecture of Erdős

For every $\varepsilon > 0$,

$$\#\{p \text{ odd prime} : \mathrm{ord}_p(2) = r\} \ll_\varepsilon r^\varepsilon.$$

This would improve $\frac{1}{2} - \beta$ to $1 - \beta$:

$$\boxed{\#\{n \le x : n \text{ odd},\ \ell(n) \le x^\beta\} \le \frac{x}{\mathcal{L}(x)^{1-\beta-\delta}}}$$

for every fixed $\delta > 0$ and all large x (uniformly for $\beta \ge 0$).

Under Hypothesis U as well, the exponent is sharp for each fixed $\beta \in (0, 1)$.

Peeks at a proof

We discuss only upper bounds, in the interests of time. We omit the lower bound constructions that depend on Hypothesis U.

For small y, we lean on an idea of Pomerance. Put

$$a(x,m) = \#\{n \le x : \lambda(n) = m\}.$$

If $\lambda(n) = m$, every prime $p \mid n$ has $p-1 \mid m$. Hence, by Rankin's trick,

$$\begin{aligned} a(x,m) &\le x^s \prod_{p:\, p-1 \mid m} (1-p^{-s})^{-1} \qquad (s>0) \\ &\le x^s \prod_{d \mid m} \bigl(1-(d+1)^{-s}\bigr)^{-1}. \end{aligned}$$

Adapting Pomerance's choice of s gives

$$a(x,m) \le x\mathcal{L}(x,y)^{-1+o(1)},$$

uniformly for $m \le y$. Summing over $m \le y$ gives the theorem for $y \le x^{1/\log_2 x}$.

Bigger is badder!

Larger y are more troublesome.

To give the main idea, suppose n is squarefree. (We can reduce to this case.) We put

$$d := \frac{\varphi(n)}{\lambda(n)}.$$

When n is near x and $\lambda(n) \le y$, this quotient is of size $\gtrapprox x/y$.

The key observation is

$$\boxed{d \operatorname{rad}(d) \mid \varphi(n),} \qquad \operatorname{rad}(d) = \prod_{p \mid d} p.$$

(To prove this, use that $\varphi(n)$ and $\lambda(n)$ have the same prime divisors.)

We are led to count squarefree n with $q \mid \varphi(n)$, for $q = d \operatorname{rad}(d)$.

How often does q divide $\varphi(n)$?

Let $g_w(q)$ count ordered factorizations

$$q = q_1 \cdots q_w, \qquad q_i \geq 2.$$

Our fundamental counting lemma

For $x \geq 3$, $W > 0$, and any positive integer q,

$$\#\{n \leq x : n \text{ squarefree}, \ \omega(n) \leq W, \ q \mid \varphi(n)\}$$
$$\leq \boxed{\frac{x}{q} \sum_{0 \leq w \leq W} \frac{\left(C_\varphi \log_2 x \, \log_2(3q)\right)^w}{w!} g_w(q),}$$

where $C_\varphi > 0$ is absolute.

We sum this estimate over values of $q = d \, \mathrm{rad}(d)$ with $d \gtrapprox x/y$.

Gee whiz, g_w !

The divisors $d\,\mathrm{rad}(d)$ are squarefull, hence sparse. To make all this go, we need to control the first moments of the functions g_w, across sparse sets, for w in a wide range.

First moment bound for the g_w

Fix $\delta > 0$. For all sufficiently large X, if

$$S \subseteq [1, X], \qquad \#S \leq X^{1-\beta}, \qquad \frac{1}{1000} \leq \beta \leq 1,$$

then

$$\boxed{\sum_{q \in S} g_w(q) \leq \frac{X}{\mathcal{L}(X)^{\beta-\delta}}}$$

uniformly for

$$1 \leq w \leq \frac{\log X\,(\log_3 X)^2}{(\log_2 X)^2}.$$

Thank you!

