The Iterated Carmichael Lambda Function

Nick Harland
University of British Columbia

CNTA XII
University of Lethbridge
June 21, 2012

Definitions

Definition of Carmichael Lambda Function

$\lambda(n)$ is the smallest natural number m such that

$$a^m \equiv 1 \pmod{n}$$

for all $(a, n) = 1$.

Recall the Euler Totient function $\phi(n)$ is the multiplicative function defined on prime powers to be $\phi(p^k) = p^k(p-1)$.

Definitions

Definition of Carmichael Lambda Function

$\lambda(n)$ is the smallest natural number m such that

$$a^m \equiv 1 \pmod{n}$$

for all $(a, n) = 1$.

Recall the Euler Totient function $\phi(n)$ is the multiplicative function defined on prime powers to be $\phi(p^k) = p^k(p-1)$.

Calculating $\lambda(n)$

Euler's Theorem states

Theorem (Euler)

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

for all $(a, n) = 1$.

Hence we know that $\lambda(n) \mid \phi(n)$. The two are equal when there exists some a such that $a^m \not\equiv 1$ for all $0 < m < \phi(n)$.

Calculating $\lambda(n)$

Euler's Theorem states

Theorem (Euler)

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

for all $(a, n) = 1$.

Hence we know that $\lambda(n) \mid \phi(n)$. The two are equal when there exists some a such that $a^m \not\equiv 1$ for all $0 < m < \phi(n)$.

Calculating $\lambda(n)$

Euler's Theorem states

Theorem (Euler)

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

for all $(a, n) = 1$.

Hence we know that $\lambda(n) \mid \phi(n)$. The two are equal when there exists some a such that $a^m \not\equiv 1$ for all $0 < m < \phi(n)$.

Calculating $\lambda(n)$

Therefore we get the following calculations.

On odd prime powers, $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.

On the odder prime powers

$$\lambda(2) = 1, \lambda(4) = 2 \text{ and } \lambda(2^k) = \frac{1}{2}\phi(2^k) = 2^{k-2}$$

for $k \geq 3$.

Question

What if n is not a prime power?

Calculating $\lambda(n)$

Therefore we get the following calculations.
On odd prime powers, $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.
On the odder prime powers

$$\lambda(2) = 1, \lambda(4) = 2 \text{ and } \lambda(2^k) = \frac{1}{2}\phi(2^k) = 2^{k-2}$$

for $k \geq 3$.

Question

What if n is not a prime power?

Calculating $\lambda(n)$

Therefore we get the following calculations.
On odd prime powers, $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.
On the odder prime powers

$$\lambda(2) = 1, \lambda(4) = 2 \text{ and } \lambda(2^k) = \frac{1}{2}\phi(2^k) = 2^{k-2}$$

for $k \geq 3$.

Question

What if n is not a prime power?

Calculating $\lambda(n)$

Therefore we get the following calculations.
On odd prime powers, $\lambda(p^k) = \phi(p^k) = (p-1)p^{k-1}$.
On the odder prime powers

$$\lambda(2) = 1, \lambda(4) = 2 \text{ and } \lambda(2^k) = \frac{1}{2}\phi(2^k) = 2^{k-2}$$

for $k \geq 3$.

Question

What if n is not a prime power?

Calculating $\lambda(n)$

By the Chinese Remainder Theorem we can get that for $(a,b)=1$,

$$\lambda(ab) = \mathrm{lcm}\{\lambda(a), \lambda(b)\}.$$

Example 1

What is $\lambda(547808)$?

$547808 = (2^5)(17)(19)(53)$, so

$$\begin{aligned}\lambda(547808) &= \mathrm{lcm}\{\lambda(2^5), \lambda(17), \lambda(19), \lambda(53)\} \\ &= \mathrm{lcm}\{2^3, 16, 18, 52\} = (2^4)(3^2)(13) = 1872.\end{aligned}$$

Calculating $\lambda(n)$

By the Chinese Remainder Theorem we can get that for $(a,b)=1$,

$$\lambda(ab) = \operatorname{lcm}\{\lambda(a), \lambda(b)\}.$$

Example 1

What is $\lambda(547808)$?

$547808 = (2^5)(17)(19)(53)$, so

$$\begin{aligned}\lambda(547808) &= \operatorname{lcm}\{\lambda(2^5), \lambda(17), \lambda(19), \lambda(53)\} \\ &= \operatorname{lcm}\{2^3, 16, 18, 52\} = (2^4)(3^2)(13) = 1872.\end{aligned}$$

Calculating $\lambda(n)$

Example b

What is $\lambda_2(547808) = \lambda\lambda(547808)$?

$$\begin{aligned}\lambda_2(547808) = \lambda((2^4)(3^2)(13)) &= \mathrm{lcm}\{\lambda(2^4), \lambda(3^2), \lambda(13)\}\\ &= \mathrm{lcm}\{2^2, 6, 12\} = 12.\end{aligned}$$

Calculating $\lambda(n)$

Example b

What is $\lambda_2(547808) = \lambda\lambda(547808)$?

$$\begin{aligned}\lambda_2(547808) = \lambda((2^4)(3^2)(13)) &= \operatorname{lcm}\{\lambda(2^4), \lambda(3^2), \lambda(13)\} \\ &= \operatorname{lcm}\{2^2, 6, 12\} = 12.\end{aligned}$$

Calculating $\lambda(n)$

Example iii

What is $L(547808)$, where $L(n)$ is the smallest k such that $\lambda_k(n) = 1$?

$\lambda_3(547808) = \lambda(12) = 2.$
$\lambda_4(547808) = \lambda(2) = 1 \Rightarrow L(547808) = 4.$

That's Typical

Question

What is the "typical" value of $\lambda(n)$?

Theorem (Erdős, Pomerance, Schmutz (1991))

There exists a set S of asymptotic density 1, where for all $n \in S$

$$\lambda(n) = n/(\log n)^{\log\log\log n + A + o(1)}$$

where $A = 0.2269688\ldots$

$2 > 1$

Question

What about $\lambda_2(n) = \lambda(\lambda(n))$?

Theorem (Martin, Pomerance (2005))

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

$$\lambda_2(n) = n \exp\big(- (1 + o(1))(\log\log n)^2 \log\log\log n \big).$$

Question

What happens for more iterations?!?!?!

$2 > 1$

Question

What about $\lambda_2(n) = \lambda(\lambda(n))$?

Theorem (Martin, Pomerance (2005))

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

$$\lambda_2(n) = n \exp\left(-(1 + o(1))(\log\log n)^2 \log\log\log n \right).$$

Question

What happens for more iterations?!?!?!

Why do 2 when you can do them all?

In the same paper, Martin and Pomerance gave the following conjecture, which has since been proved.

Theorem (H. (2012))

For any fixed $k \geq 1$,

$$\lambda_k(n) = n \exp\left(- \left(\frac{1}{(k-1)!} + o_k(1) \right) (\log\log n)^k \log\log\log n \right)$$

for almost all n.

$L(n)$

As for $L(n)$, very little is known. It can be show that there exists n such that $L(n) > c \log n$ for some $c > 0$, but these are likely very rare. It is more likely in light of the theorem on $\lambda_k(n)$ that $L(n)$ is usually around $\log \log n$. Although some results are known including a decent lower bound and an awful upper bound.

$L(n)$

Theorem (Martin, Pomerance (2005))

There exists an infinite number of n such that

$$L(n) < \left(\frac{1}{\log 2} + o(1)\right) \log\log n.$$

Theorem (H. (2012))

For all $c < \left(\frac{1}{e^{-1}+\log 2}\right)$,

$$L(n) \geq c \log\log n,$$

for almost all n.

$L(n)$

Theorem (Martin, Pomerance (2005))

There exists an infinite number of n such that

$$L(n) < \left(\frac{1}{\log 2} + o(1)\right) \log\log n.$$

Theorem (H. (2012))

For all $c < \left(\frac{1}{e^{-1}+\log 2}\right)$,

$$L(n) \geq c \log\log n,$$

for almost all n.

$L(n)$

As for an upper bound, until recently, the best known upper bound was the trivial upper bound $L(n) \ll \log n$. However a recent result is

Theorem (H. (2012))

For almost all n,

$$L(n) \leq (\log n)^{\gamma}$$

where the γ can be taken around 0.9503.

$L(n)$

As for an upper bound, until recently, the best known upper bound was the trivial upper bound $L(n) \ll \log n$. However a recent result is

Theorem (H. (2012))

For almost all n,

$$L(n) \leq (\log n)^{\gamma}$$

where the γ can be taken around 0.9503.

$L(n)$

It should be noted that under the Elliot–Halberstam conjecture, the constant $1/(e^{-1} + \log 2)$ can just be replaced with e. This is noteworthy because it's likely the upper bound as well.

Conjecture

$L(n)$ has normal order $e \log\log n$.

In other words, the lower bound is close, and the upper bound is way way off.

$L(n)$

It should be noted that under the Elliot–Halberstam conjecture, the constant $1/(e^{-1} + \log 2)$ can just be replaced with e. This is noteworthy because it's likely the upper bound as well.

Conjecture

$L(n)$ has normal order $e \log\log n$.

In other words, the lower bound is close, and the upper bound is way way off.

A Few Details

The way we establish the normal order of $\lambda_k(n)$ is to show

$$\begin{aligned}
\log\left(n/\lambda_k(n)\right) &\approx \log\left(\phi_k(n)/\lambda_k(n)\right) \\
&\approx \sum_{q\le(\log\log x)^k} v_q(\phi_k(n))\log q \\
&\approx h_k(n) \\
&:= \sum_{p_1|n}\sum_{p_2|p_1-1}\cdots\sum_{p_k|p_{k-1}-1}\sum_{q\le(\log\log x)^k} \nu_q(p_k-1)\log q.
\end{aligned}$$

A Few Details

We then use Turan–Kubilius and Euler summation on

$$\sum_{p\le t} h_k(p) = \sum_{p\le t}\sum_{p_2\mid p-1}\cdots\sum_{p_k\mid p_{k-1}-1}\sum_{q\le(\log\log x)^k}\nu_q(p_k-1)\log q$$
$$\approx \sum_{q\le(\log\log x)^k}\log q\sum_{a\in\mathbb{N}}\sum_{p_k\in\mathcal{P}_{q^a}}\sum_{p_{k-1}\in\mathcal{P}_{p_k}}\cdots\sum_{p_2\in\mathcal{P}_{p_3}}\pi(t;p_2,1)$$

A Few Details

We then use Bombieri–Vinogradov to replace π by li and then partial summation to recover π. Continuing this recursion yields our result

$$\log\big(n/\lambda_k(n)\big) \approx h_k(n) \approx \frac{1}{(k-1)!}(\log\log x)^k \log\log\log x$$

for almost all $n \leq x$.

The end

Thanks for your attention. These slides and more detailed proofs are available at my website at www.nickharland.com