The Iterated Carmichael Lambda Function

Nick Harland

University of Manitoba Colloquium

October 12, 2012

Outline

Definitions

Definition of Carmichael Lambda Function

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

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

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

Definition of Euler Totient Function

$\phi(n) = \#\{1 \leq a \leq n | (a, n) = 1\}.$

Definitions

Definition of Carmichael Lambda Function

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

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

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

Definition of Euler Totient Function

$\phi(n) = \#\{1 \leq a \leq n | (a, n) = 1\}$.

Calculating $\phi(n)$

Facts about $\phi(n)$.

- $\phi(n)$ is multiplicative. (i.e. if $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.)
- $\phi(p^k) = p^k - p^{k-1}$.

These allow us to evaluate $\phi(n)$ for any natural number n. We also have the following theorem.

Theorem (Euler)

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

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

Calculating $\phi(n)$

Facts about $\phi(n)$.

- $\phi(n)$ is multiplicative. (i.e. if $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.)
- $\phi(p^k) = p^k - p^{k-1}$.

These allow us to evaluate $\phi(n)$ for any natural number n. We also have the following theorem.

Theorem (Euler)

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

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

Calculating $\phi(n)$

Facts about $\phi(n)$.

- $\phi(n)$ is multiplicative. (i.e. if $(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$.)
- $\phi(p^k) = p^k - p^{k-1}$.

These allow us to evaluate $\phi(n)$ for any natural number n. We also have the following theorem.

Theorem (Euler)

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

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

Calculating $\lambda(n)$

Recall the definition of $\lambda(n)$ says that $\lambda(n)$ is the smallest such exponent. Therefore we know that $\lambda(n) \leq \phi(n)$. In fact 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 $1 \leq m < \phi(n)$ which is the definition of there being a primitive root modulo n.

It is well known that a primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime power.

Calculating $\lambda(n)$

Recall the definition of $\lambda(n)$ says that $\lambda(n)$ is the smallest such exponent. Therefore we know that $\lambda(n) \leq \phi(n)$. In fact 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 $1 \leq m < \phi(n)$ which is the definition of there being a primitive root modulo n.

It is well known that a primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime power.

Calculating $\lambda(n)$

Recall the definition of $\lambda(n)$ says that $\lambda(n)$ is the smallest such exponent. Therefore we know that $\lambda(n) \leq \phi(n)$. In fact 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 $1 \leq m < \phi(n)$ which is the definition of there being a primitive root modulo n.

It is well known that a primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd 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 other 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 other 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 other 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 other 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

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

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

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

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 $\lambda(n)$

Example 2

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 2

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 $L(n)$

Definition of $L(n)$

Let $L(n)$ be the smallest k such that $\lambda_k(n) = 1$.

Example 3

What is $L(547808)$?

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

Calculating $L(n)$

Definition of $L(n)$

Let $L(n)$ be the smallest k such that $\lambda_k(n) = 1$.

Example 3

What is $L(547808)$?

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

Calculating $L(n)$

Definition of $L(n)$

Let $L(n)$ be the smallest k such that $\lambda_k(n) = 1$.

Example 3

What is $L(547808)$?

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

Upper Bound for $\lambda(n)$

$\lambda(n)$ has a trivial upper bound of $\frac{2}{n}\sum_{i=1}^{n-1} i$ which is reached whenever n is prime.

Lower Bound for $\lambda(n)$

Theorem (Erdős, Pomerance, Schmutz (1991))

For any increasing sequence (n_i), for sufficiently large i

$$\lambda(n_i) > (\log n_i)^{c_0 \log\log\log n_i}$$

for any constant $0 < c_0 < 1/\log 2$.

They also showed that this can be acheived with some different effective constant in place of c_0.

Lower Bound for $\lambda(n)$

Theorem (Erdős, Pomerance, Schmutz (1991))

For any increasing sequence (n_i), for sufficiently large i

$$\lambda(n_i) > (\log n_i)^{c_0 \log\log\log n_i}$$

for any constant $0 < c_0 < 1/\log 2$.

They also showed that this can be acheived with some different effective constant in place of c_0.

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 $A = 0.2269688...$

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 $A = 0.2269688...$

$2 > 1$

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?!?!?!

$2 > 1$

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?!?!?!

Why do 2 when you can do them all?

In the same paper, Martin and Pomerance gave the following conjecture, which I proved.

Theorem (H. (2012))

For any fixed $k \geq 1$,

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

for almost all n.

Why do 2 when you can do them all?

In the same paper, Martin and Pomerance gave the following conjecture, which I proved.

Theorem (H. (2012))

For any fixed $k \geq 1$,

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

for almost all n.

How long to get to 1?

Let $k(n)$ be the smallest number k such that $\phi_k(n)$. Bounds on $k(n)$ can be shown to be

Theorem (Pillai (1929))

$$\left\lceil \frac{\log n}{\log 3} \right\rceil \le k(n) \le \left\lceil \frac{\log n}{\log 2} \right\rceil$$

and that both sides can be obtained infinitely often. See if you can guess how.

How long to get to 1?

Let $k(n)$ be the smallest number k such that $\phi_k(n)$. Bounds on $k(n)$ can be shown to be

Theorem (Pillai (1929))

$$\left\lceil \frac{\log n}{\log 3} \right\rceil \leq k(n) \leq \left\lceil \frac{\log n}{\log 2} \right\rceil$$

and that both sides can be obtained infinitely often. See if you can guess how.

$L(n)$

As for $L(n)$, very little is known. It can be shown 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

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

The n_i can be defined by $n_i = \operatorname{lcm}\{1, 2, \ldots, i\}$.

$L(n)$

Theorem (Martin, Pomerance (2005))

There exists an infinite number of n such that

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

The n_i can be defined by $n_i = \operatorname{lcm}\{1, 2, \ldots, i\}$.

Useful Theorems and Conjectures

Let $\pi(x, q, a)$ be the number of primes p less than or equal to x such that $p \equiv a$ modulo q. The prime number theorem for arithmetic progressions says that

$$\pi(x, q, a) \approx \frac{\pi(x)}{\phi(q)}$$

for $q \leq (\log x)^A$.

The error in this calculation is $\frac{x}{(\log x)^A}$ although under the Generalized Riemann Hypothesis, it can be improved to $x^{1/2} \log^2 x$.

Useful Theorems and Conjectures

Let $\pi(x, q, a)$ be the number of primes p less than or equal to x such that $p \equiv a$ modulo q. The prime number theorem for arithmetic progressions says that

$$\pi(x, q, a) \approx \frac{\pi(x)}{\phi(q)}$$

for $q \leq (\log x)^A$.

The error in this calculation is $\frac{x}{(\log x)^A}$ although under the Generalized Riemann Hypothesis, it can be improved to $x^{1/2} \log^2 x$.

Useful Theorems and Conjectures

The Elliot–Halberstam conjecture says that the combined error for all q up to a certain point is not too large.

$$\sum_{q \le x^{\theta}} \left| \pi(x, q, a) - \frac{\pi(x)}{\phi(q)} \right| \ll \frac{x}{\log^{A} x}$$

for all $\theta < 1$.

The Bombieri–Vinogradov Theorem is unconditional and says the above is true for all $\theta < 1/2$. Note that this implies the error bound from GRH is true on average.

Useful Theorems and Conjectures

The Elliot–Halberstam conjecture says that the combined error for all q up to a certain point is not too large.

$$\sum_{q \le x^\theta} \left| \pi(x, q, a) - \frac{\pi(x)}{\phi(q)} \right| \ll \frac{x}{\log^A x}$$

for all $\theta < 1$.

The Bombieri–Vinogradov Theorem is unconditional and says the above is true for all $\theta < 1/2$. Note that this implies the error bound from GRH is true on average.

$L(n)$

For an lower bound we have the following.

Theorem (H. (2012))

For almost all n,

$$L(n) \geq \left(\frac{1}{e^{-1} + \log 2} \right) \log \log n.$$

$L(n)$

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, that 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, that 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.

Wussing out

The following is a sketch of the proof of the normal order of $\log\left(n/\lambda_k(n)\right)$ when $k = 1$. It should be noted that the ideas begin in the same way for general k, however the details get about 35 pages more messy.

$\lambda(n)$ and $\phi(n)$ are friends

We are looking for the normal order of $\log(n/\lambda(n))$. However the relationship between n and $\lambda(n)$ is hard to see. It would be easier to look at the relationship between $\lambda(n)$ and $\phi(n)$. We do this by

$$\log\left(\frac{n}{\lambda(n)}\right) = \log\left(\frac{n}{\phi(n)}\right) + \log\left(\frac{\phi(n)}{\lambda(n)}\right).$$

The first term is $O(\log\log\log n)$ and get sucked into the error.

$\lambda(n)$ and $\phi(n)$ are friends

We are looking for the normal order of $\log(n/\lambda(n))$. However the relationship between n and $\lambda(n)$ is hard to see. It would be easier to look at the relationship between $\lambda(n)$ and $\phi(n)$. We do this by

$$\log\left(\frac{n}{\lambda(n)}\right) = \log\left(\frac{n}{\phi(n)}\right) + \log\left(\frac{\phi(n)}{\lambda(n)}\right).$$

The first term is $O(\log\log\log n)$ and get sucked into the error.

$\lambda(n)$ and $\phi(n)$ are friends

We are looking for the normal order of $\log(n/\lambda(n))$. However the relationship between n and $\lambda(n)$ is hard to see. It would be easier to look at the relationship between $\lambda(n)$ and $\phi(n)$. We do this by

$$\log\left(\frac{n}{\lambda(n)}\right) = \log\left(\frac{n}{\phi(n)}\right) + \log\left(\frac{\phi(n)}{\lambda(n)}\right).$$

The first term is $O(\log\log\log n)$ and get sucked into the error.

Why have one log when you can have many sums?

Let q be a prime and $a = v_q(n)$ be the largest power of q such that $q^a \mid n$. Let $y = \log\log x$. Then

$$\log\left(\frac{\phi(n)}{\lambda(n)}\right) = \sum_{\substack{q>y \\ \nu_q(\phi(n))=1}} (\nu_q(\phi(n)) - \nu_q(\lambda(n)))\log q + \sum_{\substack{q>y \\ \nu_q(\phi(n))\geq 2}} (\nu_q(\phi(n)) - \nu_q(\lambda(n)))\log q + \sum_{q\leq y}\nu_q(\phi(n))\log q - \sum_{q\leq y}\nu_q(\lambda(n))\log q.$$

Why have one log when you can have many sums?

Let q be a prime and $a = v_q(n)$ be the largest power of q such that $q^a \mid n$. Let $y = \log\log x$. Then

$$\begin{aligned}\log\left(\frac{\phi(n)}{\lambda(n)}\right) &= \sum_{\substack{q>y \\ \nu_q(\phi(n))=1}} (\nu_q(\phi(n)) - \nu_q(\lambda(n)))\log q \\ &+ \sum_{\substack{q>y \\ \nu_q(\phi(n))\geq 2}} (\nu_q(\phi(n)) - \nu_q(\lambda(n)))\log q \\ &+ \sum_{q\leq y} \nu_q(\phi(n))\log q - \sum_{q\leq y} \nu_q(\lambda(n))\log q.\end{aligned}$$

Which sum matters?

Of the 4 summations, only one matters enough to give us our main term. That summation is

$$h(n) := \sum_{q \le y} \nu_q(\phi(n)) \log q$$

Regardless, in light of the appearance of v_q, it's very important to see how primes divide $\phi(n)$ and $\lambda(n)$.

Which sum matters?

Of the 4 summations, only one matters enough to give us our main term. That summation is

$$h(n) := \sum_{q \leq y} \nu_q(\phi(n)) \log q$$

Regardless, in light of the appearance of v_q, it's very important to see how primes divide $\phi(n)$ and $\lambda(n)$.

Turán-Kubilius

The strategy is to use the Turán–Kubilius inequality for the strongly additive function $h(n)$ which says that

$$\sum_{n\le x}\left(h(n)-\sum_{p\le x}\frac{h(p)}{p}\right)^2 \ll x\sum_{p\le x}\frac{h(p)^2}{p}$$

h(p)

Using that $v_q(p-1) = \sum_{a\geq 1} \sum_{\substack{p\leq x \\ p\equiv 1 (q^a)}} 1$ we get

$$\begin{aligned}
\sum_{p\leq x} \frac{h(p)}{p} &= \sum_{q\leq y} \log q \sum_{p\leq x} \frac{\nu_q(\phi(p))}{p} \\
&= \sum_{q\leq y} \log q \sum_{a\geq 1} \sum_{\substack{p\leq x \\ p\equiv 1 (q^a)}} \frac{1}{p} \\
&= \sum_{q\leq y} \log q \sum_{a\geq 1} \frac{y}{\phi(q^a)} + error
\end{aligned}$$

h(p)

$$= \sum_{q \le y} \log q \sum_{a \ge 1} \frac{y}{\phi(q^a)} + error$$

$$= \sum_{q \le y} \frac{\log q}{q-1} \sum_{a \ge 1} \frac{y}{q^{a-1}} + ERror$$

$$= y \sum_{q \le y} \frac{\log q}{q} + ERROr$$

$$= y \log y + ERROR.$$

The error can be shown to be $O(y \log \log y)$

h(p)

Similarly we can show

$$\sum_{p \le x} \frac{h(p)^2}{p} \ll y \log^2 y.$$

Hence we obtain

h(p)

Similarly we can show

$$\sum_{p \leq x} \frac{h(p)^2}{p} \ll y \log^2 y.$$

Hence we obtain

h(p)

$$\sum_{n\le x}\left(h(n)-\sum_{p\le x}\frac{h(p)}{p}\right)^2 \ll xy\log^2 y.$$

This implies that the number of n for which $|h(n)-y\log y| > y\log\log y$ is

$$O\left(\frac{xy\log^2 y}{(y\log\log y)^2}\right)=o(x).$$

h(p)

$$\sum_{n\leq x}\left(h(n)-\sum_{p\leq x}\frac{h(p)}{p}\right)^2 \ll xy\log^2 y.$$

This implies that the number of n for which $|h(n)-y\log y| > y\log\log y$ is

$$O\left(\frac{xy\log^2 y}{(y\log\log y)^2}\right)=o(x).$$

h(p)

$$\sum_{n \le x} \left(h(n) - \sum_{p \le x} \frac{h(p)}{p} \right)^2 \ll xy \log^2 y.$$

This implies that the number of n for which $|h(n) - y \log y| > y \log \log y$ is

$$O\left(\frac{xy \log^2 y}{(y \log \log y)^2} \right) = o(x).$$

YAY!

Hence for almost all $n \leq x$

$$\log\left(\frac{n}{\lambda(n)}\right) \approx h(n) \approx y \log y = \log\log x \log\log\log x$$

Obstacles for larger k

The first major obstacle is replacing $\log\big(\phi_k(n)/\lambda_k(n)\big)$ by

$$\sum_{q \le y^k} v_q(\phi_k(n)) \log q.$$

The other terms are

$$-\sum_{q \le y^k} v_q(\lambda_k(n)) \log q, \qquad \sum_{q > y^k} \big(v_q(\phi_k(n)) - v_q(\lambda_k(n))\big) \log q$$

Obstacles for larger k

The first major obstacle is replacing $\log\big(\phi_k(n)/\lambda_k(n)\big)$ by

$$\sum_{q \le y^k} v_q(\phi_k(n)) \log q.$$

The other terms are

$$-\sum_{q \le y^k} v_q(\lambda_k(n)) \log q, \qquad \sum_{q > y^k} \big(v_q(\phi_k(n)) - v_q(\lambda_k(n))\big) \log q$$

Obstacles for larger k

Showing the second term is small involves a complex description of how prime powers can divide $\phi_k(n)$.

This was done by splitting off easier cases, for example $q^2 \mid n$, and then splitting the remaining cases into an array.

After that I showed that there is a way of organizing those cases there aren't too many, and in any individual case the number of n such that $q^a \mid n$ is small enough to make the sum small.

Obstacles for larger k

Showing the second term is small involves a complex description of how prime powers can divide $\phi_k(n)$.
This was done by splitting off easier cases, for example $q^2 \mid n$, and then splitting the remaining cases into an array.
After that I showed that there is a way of organizing those cases there aren't too many, and in any individual case the number of n such that $q^a \mid n$ is small enough to make the sum small.

Obstacles for larger k

Showing the second term is small involves a complex description of how prime powers can divide $\phi_k(n)$.
This was done by splitting off easier cases, for example $q^2 \mid n$, and then splitting the remaining cases into an array.
After that I showed that there is a way of organizing those cases there aren't too many, and in any individual case the number of n such that $q^a \mid n$ is small enough to make the sum small.

Obstacles for larger k

The second major obstacle is when trying to approximate $h_k(n)$. The idea is to use the Bombieri–Vinogradov Thereom on a multiple sum over primes of $\pi(t, p, 1)$. Unfortunately the theorem only allows the use of q up to some power of x less than $1/2$. Hence we need to split off the larger primes. Splitting off those primes involves sieve techniques. Using Brun's Sieve turns the error into multiples sums involving the totient function ϕ. Repeatedly using induction and Cauchy–Schwarz can bound these sums giving us our result.

Obstacles for larger k

The second major obstacle is when trying to approximate $h_k(n)$. The idea is to use the Bombieri–Vinogradov Thereom on a multiple sum over primes of $\pi(t, p, 1)$. Unfortunately the theorem only allows the use of q up to some power of x less than $1/2$. Hence we need to split off the larger primes. Splitting off those primes involves sieve techniques. Using Brun's Sieve turns the error into multiples sums involving the totient function ϕ. Repeatedly using induction and Cauchy–Schwarz can bound these sums giving us our result.

Obstacles for larger k

The second major obstacle is when trying to approximate $h_k(n)$. The idea is to use the Bombieri–Vinogradov Thereom on a multiple sum over primes of $\pi(t, p, 1)$. Unfortunately the theorem only allows the use of q up to some power of x less than $1/2$. Hence we need to split off the larger primes. Splitting off those primes involves sieve techniques. Using Brun's Sieve turns the error into multiples sums involving the totient function ϕ. Repeatedly using induction and Cauchy–Schwarz can bound these sums giving us our result.

Obstacles for larger k

The second major obstacle is when trying to approximate $h_k(n)$. The idea is to use the Bombieri–Vinogradov Thereom on a multiple sum over primes of $\pi(t, p, 1)$. Unfortunately the theorem only allows the use of q up to some power of x less than $1/2$. Hence we need to split off the larger primes. Splitting off those primes involves sieve techniques. Using Brun's Sieve turns the error into multiples sums involving the totient function ϕ. Repeatedly using induction and Cauchy–Schwarz can bound these sums giving us our result.

Power Generator

The power generator is

$$u_{n+1} \equiv u_n^l \pmod{m}$$

where $0 \leq u_n \leq m-1, n = 1, 2, \ldots.$

The power generator has many features that are important in crytography. An important question in cryptography is the largest possible period of the power generator. It can be shown that the largest period is $\lambda\lambda(m)$. Hence the result of Martin and Pomerance can be used to give an estimate on the longest period.

Power Generator

The power generator is

$$u_{n+1} \equiv u_n^l \pmod{m}$$

where $0 \leq u_n \leq m-1, n = 1, 2, \ldots.$
The power generator has many features that are important in crytography. An important question in cryptography is the largest possible period of the power generator. It can be shown that the largest period is $\lambda\lambda(m)$. Hence the result of Martin and Pomerance can be used to give an estimate on the longest period.

Power Generator

Let x_0 be such that $gcd(x_0, n) = 1$. The power generator generates a purely periodic cycle. A natural question is how many cycles are there? Martin and Pomerance's estimate can be used to say something non–trivial about the number of cycles.

Theorem (Martin, Pomerance (2005))

The number of cycles of the power generator is

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

Power Generator

Let x_0 be such that $gcd(x_0, n) = 1$. The power generator generates a purely periodic cycle. A natural question is how many cycles are there? Martin and Pomerance's estimate can be used to say something non–trivial about the number of cycles.

Theorem (Martin, Pomerance (2005))

The number of cycles of the power generator is

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

Carmichael Conjecture

Question

For what values of m does there exist n such that $\phi(n) = m$.
How many n are there?

The short answer is not many, and probably more than 1.

Carmichael Conjecture

Question

For what values of m does there exist n such that $\phi(n) = m$.
How many n are there?

The short answer is not many, and probably more than 1.

Carmichael Conjecture

Let p be a prime, then it's clear that $p-1$ is a totient for all primes p. Hence there must be at least $\pi(x)$ totients less than x. In fact, Kevin Ford has shown there is not much more.

Theorem (Ford (1998))

The number of totients less than x is

$$\frac{x}{\log x}\exp(O(\log_3 x)^2)$$

Carmichael Conjecture

Let p be a prime, then it's clear that $p-1$ is a totient for all primes p. Hence there must be at least $\pi(x)$ totients less than x. In fact, Kevin Ford has shown there is not much more.

Theorem (Ford (1998))

The number of totients less than x is

$$\frac{x}{\log x}\exp(O(\log_3 x)^2)$$

Carmichael Conjecture

An interesting question is how many n are there with $\phi(n) = m$. Since $\phi(2n) = \phi(n)$, whenever there is an odd n, there must be a corresponding even one. There is enough evidence to suggest that it is never just one.

Conjecture (Carmichael Conjecture)

If $\phi(n) = m$, there exists $n' \neq n$ such that $\phi(n') = m$.

Carmichael Conjecture

An interesting question is how many n are there with $\phi(n) = m$. Since $\phi(2n) = \phi(n)$, whenever there is an odd n, there must be a corresponding even one. There is enough evidence to suggest that it is never just one.

Conjecture (Carmichael Conjecture)

If $\phi(n) = m$, there exists $n' \neq n$ such that $\phi(n') = m$.

Carmichael Conjecture

While the conjecture is still open, any counterexample is pretty big. For example it's true for all $n \leq 10^{10^{10}}$. It's also known that n must have lots of divisors of 2 and 3.

What about $\lambda(n)$?

Carmichael Conjecture

While the conjecture is still open, any counterexample is pretty big. For example it's true for all $n \leq 10^{10^{10}}$. It's also known that n must have lots of divisors of 2 and 3.

What about $\lambda(n)$?

Carmichael Conjecture for λ

An equivalent conjecture has been made for $\lambda(n)$.

Conjecture (Carmichael Conjecture)

If $\lambda(n) = m$, there exists $n' \neq n$ such that $\lambda(n') = m$.

This conjecture seems like it's closer to an answer.

Theorem (Banks, Friedlander, Luca, Pappalardi, Shparlinski (2006))

Any counterexample n must be a multiple of some smallest counterexample n_0.

Carmichael Conjecture for λ

An equivalent conjecture has been made for $\lambda(n)$.

Conjecture (Carmichael Conjecture)

If $\lambda(n) = m$, there exists $n' \neq n$ such that $\lambda(n') = m$.

This conjecture seems like it's closer to an answer.

Theorem (Banks, Friedlander, Luca, Pappalardi, Shparlinski (2006))

Any counterexample n must be a multiple of some smallest counterexample n_0.

Carmichael Conjecture for λ

An equivalent conjecture has been made for $\lambda(n)$.

Conjecture (Carmichael Conjecture)

If $\lambda(n) = m$, there exists $n' \neq n$ such that $\lambda(n') = m$.

This conjecture seems like it's closer to an answer.

Theorem (Banks, Friedlander, Luca, Pappalardi, Shparlinski (2006))

Any counterexample n must be a multiple of some smallest counterexample n_0.

Carmichael Conjecture for λ

It's also elementary to show that if a counterexample exists, then $(i) 2^4 \mid n_0$ and (ii) if $p-1 \mid \lambda(n_0)$ for a prime p, then $p^2 \mid n_0$.
This is useful since we know $4 \mid \lambda(n_0)$, then $3^2, 5^2 \mid n_0$.
However that means $60 \mid \lambda(n_0)$ and so $7^2, 11^2, 13^2, 31^2, 61^2 \mid n_0$.

Carmichael Conjecture for λ

It's also elementary to show that if a counterexample exists, then $(i) 2^4 \mid n_0$ and (ii) if $p-1 \mid \lambda(n_0)$ for a prime p, then $p^2 \mid n_0$. This is useful since we know $4 \mid \lambda(n_0)$, then $3^2, 5^2 \mid n_0$. However that means $60 \mid \lambda(n_0)$ and so $7^2, 11^2, 13^2, 31^2, 61^2 \mid n_0$.

Carmichael Conjecture for λ

It's also elementary to show that if a counterexample exists, then $(i) 2^4 \mid n_0$ and (ii) if $p-1 \mid \lambda(n_0)$ for a prime p, then $p^2 \mid n_0$. This is useful since we know $4 \mid \lambda(n_0)$, then $3^2, 5^2 \mid n_0$. However that means $60 \mid \lambda(n_0)$ and so $7^2, 11^2, 13^2, 31^2, 61^2 \mid n_0$.

Carmichael Conjecture for λ

Therefore if this process can continue indefinitely (which is conjectured), then no n_0 can exist, proving Carmichael's conjecture for $\lambda(n)$.

The end

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