Iterates of the Carmichael λ-function

Greg Martin
University of British Columbia

joint work with Carl Pomerance
Dartmouth College

Illinois Number Theory Fest
May 16, 2007

slides can be found on my web page
www.math.ubc.ca/∼gerg/index.shtml?slides

Outline

Definition of λ

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n) that are relatively prime to n.

- The size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$.
- Euler proved that $a^{\phi(n)} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- However, the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is often smaller than $\phi(n)$.

Definition

The Carmichael λ-function $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the largest multiplicative order (mod n) of any integer that is relatively prime to n.

Definition of λ

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n) that are relatively prime to n.

- The size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$.
- Euler proved that $a^{\phi(n)} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- However, the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is often smaller than $\phi(n)$.

Definition

The Carmichael λ-function $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the largest multiplicative order (mod n) of any integer that is relatively prime to n.

Definition of λ

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n) that are relatively prime to n.

- The size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$.
- Euler proved that $a^{\phi(n)} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- However, the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is often smaller than $\phi(n)$.

Definition

The Carmichael λ-function $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the largest multiplicative order (mod n) of any integer that is relatively prime to n.

Definition of λ

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n) that are relatively prime to n.

- The size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$.
- Euler proved that $a^{\phi(n)} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- However, the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is often smaller than $\phi(n)$.

Definition

The Carmichael λ-function $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the largest multiplicative order (mod n) of any integer that is relatively prime to n.

Definition of λ

$(\mathbb{Z}/n\mathbb{Z})^\times$ is the multiplicative group of residue classes (mod n) that are relatively prime to n.

Definition

$\lambda(n)$ is the *smallest* positive integer such that $a^{\lambda(n)} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Definition

The Carmichael λ-function $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^\times$, that is, the largest multiplicative order (mod n) of any integer that is relatively prime to n.

Formulas for $\phi(n)$ and $\lambda(n)$

Easy to compute given the prime factorization of n:

Euler ϕ-function

- $\phi(p^\alpha) = (p-1)p^{\alpha-1}$ for all primes p
- $\phi(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \times \cdots \times \phi(p_r^{\alpha_r})$

Carmichael λ-function

- $\lambda(p^\alpha) = (p-1)p^{\alpha-1}$ for all odd primes p
- $\lambda(2) = 1$ and $\lambda(4) = 2$, but $\lambda(2^\alpha) = 2^{\alpha-2}$ for $\alpha \geq 3$
- $\lambda(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})]$

Note: $\lambda(n)$ divides $\phi(n)$, and the same primes divide $\lambda(n)$ and $\phi(n)$, but often with higher multiplicity in $\phi(n)$ than in $\lambda(n)$.

Formulas for $\phi(n)$ and $\lambda(n)$

Easy to compute given the prime factorization of n:

Euler ϕ-function

- $\phi(p^\alpha) = (p-1)p^{\alpha-1}$ for all primes p
- $\phi(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \times \cdots \times \phi(p_r^{\alpha_r})$

Carmichael λ-function

- $\lambda(p^\alpha) = (p-1)p^{\alpha-1}$ for all odd primes p
- $\lambda(2) = 1$ and $\lambda(4) = 2$, but $\lambda(2^\alpha) = 2^{\alpha-2}$ for $\alpha \geq 3$
- $\lambda(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})]$

Note: $\lambda(n)$ divides $\phi(n)$, and the same primes divide $\lambda(n)$ and $\phi(n)$, but often with higher multiplicity in $\phi(n)$ than in $\lambda(n)$.

Formulas for $\phi(n)$ and $\lambda(n)$

Easy to compute given the prime factorization of n:

Euler ϕ-function

- $\phi(p^\alpha) = (p-1)p^{\alpha-1}$ for all primes p
- $\phi(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \times \cdots \times \phi(p_r^{\alpha_r})$

Carmichael λ-function

- $\lambda(p^\alpha) = (p-1)p^{\alpha-1}$ for all odd primes p
- $\lambda(2) = 1$ and $\lambda(4) = 2$, but $\lambda(2^\alpha) = 2^{\alpha-2}$ for $\alpha \geq 3$
- $\lambda(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})]$

Note: $\lambda(n)$ divides $\phi(n)$, and the same primes divide $\lambda(n)$ and $\phi(n)$, but often with higher multiplicity in $\phi(n)$ than in $\lambda(n)$.

Formulas for $\phi(n)$ and $\lambda(n)$

Easy to compute given the prime factorization of n:

Euler ϕ-function

- $\phi(p^\alpha) = (p-1)p^{\alpha-1}$ for all primes p
- $\phi(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \times \cdots \times \phi(p_r^{\alpha_r})$

Carmichael λ-function

- $\lambda(p^\alpha) = (p-1)p^{\alpha-1}$ for all odd primes p
- $\lambda(2) = 1$ and $\lambda(4) = 2$, but $\lambda(2^\alpha) = 2^{\alpha-2}$ for $\alpha \geq 3$
- $\lambda(p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}) = \operatorname{lcm}[\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_r^{\alpha_r})]$

Note: $\lambda(n)$ divides $\phi(n)$, and the same primes divide $\lambda(n)$ and $\phi(n)$, but often with higher multiplicity in $\phi(n)$ than in $\lambda(n)$.

Connection to pseudorandom number generators

A toy pseudorandom number generator:

- Choose a modulus n and a multiplier $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv cx_k \pmod{n}$.

Since $x_k \equiv c^k x_0 \pmod{n}$, the period of this sequence is the order of c modulo n, which is at most $\lambda(n)$.

This generator is easy to "crack": given n, the multiplier c can be calculated from any two consecutive terms of $\{x_k\}$.

Puzzle

How can this generator be "cracked" from $\{x_k\}$, if you know neither c nor n?

Connection to pseudorandom number generators

A toy pseudorandom number generator:

- Choose a modulus n and a multiplier $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv cx_k \pmod{n}$.

Since $x_k \equiv c^k x_0 \pmod{n}$, the period of this sequence is the order of c modulo n, which is at most $\lambda(n)$.

This generator is easy to "crack": given n, the multiplier c can be calculated from any two consecutive terms of $\{x_k\}$.

Puzzle

How can this generator be "cracked" from $\{x_k\}$, if you know neither c nor n?

Connection to pseudorandom number generators

A toy pseudorandom number generator:

- Choose a modulus n and a multiplier $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv cx_k \pmod{n}$.

Since $x_k \equiv c^k x_0 \pmod{n}$, the period of this sequence is the order of c modulo n, which is at most $\lambda(n)$.

This generator is easy to "crack": given n, the multiplier c can be calculated from any two consecutive terms of $\{x_k\}$.

Puzzle

How can this generator be "cracked" from $\{x_k\}$, if you know neither c nor n?

Connection to pseudorandom number generators

A toy pseudorandom number generator:

- Choose a modulus n and a multiplier $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv cx_k \pmod{n}$.

Since $x_k \equiv c^k x_0 \pmod{n}$, the period of this sequence is the order of c modulo n, which is at most $\lambda(n)$.

This generator is easy to "crack": given n, the multiplier c can be calculated from any two consecutive terms of $\{x_k\}$.

Puzzle

How can this generator be "cracked" from $\{x_k\}$, if you know neither c nor n?

Connection to pseudorandom number generators

A better pseudorandom number generator:

- Choose a modulus n and an exponent c that's relatively prime to $\phi(n)$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv x_k^c \pmod{n}$.

Since $x_k \equiv x_0^{c^k} \pmod{n}$, the period of this sequence is the order of c modulo *the order of x_0 modulo n*, which is at most $\lambda(\lambda(n))$.

This leads us to ask:

1. How large is $\lambda(\lambda(n))$ typically?
2. Each initial value x_0 generates a purely periodic cycle inside $(\mathbb{Z}/n\mathbb{Z})^\times$. How many such cycles are there?

Connection to pseudorandom number generators

A better pseudorandom number generator:

- Choose a modulus n and an exponent c that's relatively prime to $\phi(n)$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv x_k^c \pmod{n}$.

Since $x_k \equiv x_0^{c^k} \pmod{n}$, the period of this sequence is the order of c modulo *the order of x_0 modulo n*, which is at most $\lambda(\lambda(n))$.

This leads us to ask:

1. How large is $\lambda(\lambda(n))$ typically?
2. Each initial value x_0 generates a purely periodic cycle inside $(\mathbb{Z}/n\mathbb{Z})^\times$. How many such cycles are there?

Connection to pseudorandom number generators

A better pseudorandom number generator:

- Choose a modulus n and an exponent c that's relatively prime to $\phi(n)$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv x_k^c \pmod{n}$.

Since $x_k \equiv x_0^{c^k} \pmod{n}$, the period of this sequence is the order of c modulo *the order of x_0 modulo n*, which is at most $\lambda(\lambda(n))$.

This leads us to ask:

1. How large is $\lambda(\lambda(n))$ typically?
2. Each initial value x_0 generates a purely periodic cycle inside $(\mathbb{Z}/n\mathbb{Z})^\times$. How many such cycles are there?

Connection to pseudorandom number generators

A better pseudorandom number generator:

- Choose a modulus n and an exponent c that's relatively prime to $\phi(n)$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv x_k^c \pmod{n}$.

Since $x_k \equiv x_0^{c^k} \pmod{n}$, the period of this sequence is the order of c modulo *the order of* x_0 *modulo* n, which is at most $\lambda(\lambda(n))$.

This leads us to ask:

1. How large is $\lambda(\lambda(n))$ typically?
2. Each initial value x_0 generates a purely periodic cycle inside $(\mathbb{Z}/n\mathbb{Z})^\times$. How many such cycles are there?

Connection to pseudorandom number generators

A better pseudorandom number generator:

- Choose a modulus n and an exponent c that's relatively prime to $\phi(n)$, and set an initial value $x_0 \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Define $\{x_k\}$ recursively by $x_{k+1} \equiv x_k^c \pmod{n}$.

Since $x_k \equiv x_0^{c^k} \pmod{n}$, the period of this sequence is the order of c modulo *the order of x_0 modulo n*, which is at most $\lambda(\lambda(n))$.

This leads us to ask:

1. How large is $\lambda(\lambda(n))$ typically?
2. Each initial value x_0 generates a purely periodic cycle inside $(\mathbb{Z}/n\mathbb{Z})^\times$. How many such cycles are there?

Definition of normal order

Definition

A function $f(n)$ has *normal order* $g(n)$ if there is a set of positive integers S of asymptotic density 1 such that $f(n) \sim g(n)$ for $n \in S$.

In other words, there exists an increasing sequence $\{n_1, n_2, \dots\}$ of positive integers such that

- $\lim_{j\to\infty} \dfrac{n_j}{j} = 1$
- $\lim_{j\to\infty} \dfrac{f(n_j)}{g(n_j)} = 1$

Normal orders for iterates of ϕ

The function $\phi(n)$ itself does not have a normal order.

Theorem (Schoenberg, 1928)

The quotient $n/\phi(n)$ has a distribution function: the asymptotic density of the set $\{n \in \mathbb{N} : n/\phi(n) < t\}$ exists for every real t.

However, the higher iterates of ϕ are tamer. Let $\phi_1(n) = \phi(n)$, $\phi_2(n) = \phi(\phi(n))$, $\phi_3(n) = \phi(\phi(\phi(n)))$, and so on.

Theorem (Erdős–Granville–Pomerance–Spiro, 1997)

For each $k \geq 1$,

$$\frac{\phi_k(n)}{\phi_{k+1}(n)} \text{ has normal order } ke^\gamma \log\log\log n.$$

Normal orders for iterates of ϕ

The function $\phi(n)$ itself does not have a normal order.

Theorem (Schoenberg, 1928)

The quotient $n/\phi(n)$ has a distribution function: the asymptotic density of the set $\{n \in \mathbb{N} : n/\phi(n) < t\}$ exists for every real t.

However, the higher iterates of ϕ are tamer. Let $\phi_1(n) = \phi(n)$, $\phi_2(n) = \phi(\phi(n))$, $\phi_3(n) = \phi(\phi(\phi(n)))$, and so on.

Theorem (Erdős–Granville–Pomerance–Spiro, 1997)

For each $k \geq 1$,

$$\frac{\phi_k(n)}{\phi_{k+1}(n)} \text{ has normal order } ke^{\gamma} \log\log\log n.$$

A normal order result for λ

Theorem (Erdős–Pomerance–Schmutz, 1991)

$\log\left(\frac{n}{\lambda(n)}\right)$ *has normal order* $\log\log n \log\log\log n$.

In particular,

$$\lambda(n) = \frac{n}{e^{(1+o(1))\log\log n \log\log\log n}} = \frac{n}{(\log n)^{(1+o(1))\log\log\log n}}$$

for almost all n.

(Compare with $\phi(n) \gg \frac{n}{\log\log n}$ for every n.)

A normal order result for λ

Theorem (Erdős–Pomerance–Schmutz, 1991)

$\log\left(\frac{n}{\lambda(n)}\right)$ *has normal order* $\log\log n \log\log\log n$.

In particular,

$$\lambda(n) = \frac{n}{e^{(1+o(1))\log\log n \log\log\log n}} = \frac{n}{(\log n)^{(1+o(1))\log\log\log n}}$$

for almost all n.

(Compare with $\phi(n) \gg \frac{n}{\log\log n}$ for every n.)

A normal order result for $\lambda \circ \lambda$

Theorem (M.–Pomerance, 2005)

$$\log\left(\frac{\lambda(n)}{\lambda(\lambda(n))}\right) \textit{ has normal order } (\log\log n)^2 \log\log\log n.$$

In particular, $\lambda(\lambda(n)) = \dfrac{n}{e^{(1+o(1))(\log\log n)^2 \log\log\log n}}$ for almost all n.

The proof uses primarily elementary methods and:

- the Brun-Titchmarsh inequality and a weak form of the Bombieri-Vinogradov inequality
- the Turán-Kubilius inequality for the variance of an additive function

A normal order result for $\lambda \circ \lambda$

Theorem (M.–Pomerance, 2005)

$$\log\left(\frac{\lambda(n)}{\lambda(\lambda(n))}\right) \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

In particular, $\lambda(\lambda(n)) = \dfrac{n}{e^{(1+o(1))(\log\log n)^2 \log\log\log n}}$ for almost all n.

The proof uses primarily elementary methods and:

- the Brun-Titchmarsh inequality and a weak form of the Bombieri-Vinogradov inequality
- the Turán-Kubilius inequality for the variance of an additive function

A normal order result for $\lambda \circ \lambda$

Theorem (M.–Pomerance, 2005)

$$\log\left(\frac{\lambda(n)}{\lambda(\lambda(n))}\right) \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

In particular, $\lambda(\lambda(n)) = \dfrac{n}{e^{(1+o(1))(\log\log n)^2 \log\log\log n}}$ for almost all n.

The proof uses primarily elementary methods and:

- the Brun-Titchmarsh inequality and a weak form of the Bombieri-Vinogradov inequality
- the Turán-Kubilius inequality for the variance of an additive function

A normal order result for $\lambda \circ \lambda$

Theorem (M.–Pomerance, 2005)

$$\log\left(\frac{\lambda(n)}{\lambda(\lambda(n))}\right) \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

In particular, $\lambda(\lambda(n)) = \dfrac{n}{e^{(1+o(1))(\log\log n)^2 \log\log\log n}}$ for almost all n.

The proof uses primarily elementary methods and:

- the Brun-Titchmarsh inequality and a weak form of the Bombieri-Vinogradov inequality
- the Turán-Kubilius inequality for the variance of an additive function

A normal order result for $\lambda \circ \lambda$

Theorem (M.–Pomerance, 2005)

$$\log\left(\frac{\lambda(n)}{\lambda(\lambda(n))}\right) \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

In particular, $\lambda(\lambda(n)) = \dfrac{n}{e^{(1+o(1))(\log\log n)^2 \log\log\log n}}$ for almost all n.

The proof uses primarily elementary methods and:

- the Brun-Titchmarsh inequality and a weak form of the Bombieri-Vinogradov inequality
- the Turán-Kubilius inequality for the variance of an additive function

Cycles of the modular power map

Theorem (M.–Pomerance, 2005)

For any fixed integer $c \geq 2$, the number of cycles when iterating the map $x \mapsto x^c \pmod n$ is at least

$$\exp\big((1+o(1))(\log\log n)^2 \log\log\log n\big)$$

for almost all n. Furthermore, this is the actual number of cycles for almost all n, if GRH is true (for Kummerian fields, as in Hooley's proof of Artin's conjecture).

The proof of this theorem uses results of Kurlberg–Pomerance, one of which itself uses the theorem on the previous slide.

Cycles of the modular power map

Theorem (M.–Pomerance, 2005)

For any fixed integer $c \geq 2$, the number of cycles when iterating the map $x \mapsto x^c \pmod n$ is at least

$$\exp\big((1+o(1))(\log\log n)^2 \log\log\log n\big)$$

for almost all n. Furthermore, this is the actual number of cycles for almost all n, if GRH is true (for Kummerian fields, as in Hooley's proof of Artin's conjecture).

The proof of this theorem uses results of Kurlberg–Pomerance, one of which itself uses the theorem on the previous slide.

Cycles of the modular power map

Theorem (M.–Pomerance, 2005)

For any fixed integer $c \geq 2$, the number of cycles when iterating the map $x \mapsto x^c \pmod n$ is at least

$$\exp\big((1+o(1))(\log\log n)^2 \log\log\log n\big)$$

for almost all n. Furthermore, this is the actual number of cycles for almost all n, if GRH is true (for Kummerian fields, as in Hooley's proof of Artin's conjecture).

The proof of this theorem uses results of Kurlberg–Pomerance, one of which itself uses the theorem on the previous slide.

The ϕ-function enters the picture

The prime factors of n and of $\lambda(\lambda(n))$ are quite different in general; however, the prime factors of $\phi(\phi(n))$ and $\lambda(\lambda(n))$ are very similar. Since

$$\frac{n}{\lambda(\lambda(n))} = \frac{n}{\phi(\phi(n))} \frac{\phi(\phi(n))}{\lambda(\lambda(n))}$$

and $n/\phi(\phi(n)) \ll (\log\log n)^2$, it suffices to show that

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

The idea of the proof is to compare $\phi(\phi(n))$ and $\lambda(\lambda(n))$ one prime at a time.

The ϕ-function enters the picture

The prime factors of n and of $\lambda(\lambda(n))$ are quite different in general; however, the prime factors of $\phi(\phi(n))$ and $\lambda(\lambda(n))$ are very similar. Since

$$\frac{n}{\lambda(\lambda(n))} = \frac{n}{\phi(\phi(n))} \frac{\phi(\phi(n))}{\lambda(\lambda(n))}$$

and $n/\phi(\phi(n)) \ll (\log\log n)^2$, it suffices to show that

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

The idea of the proof is to compare $\phi(\phi(n))$ and $\lambda(\lambda(n))$ one prime at a time.

The ϕ-function enters the picture

The prime factors of n and of $\lambda(\lambda(n))$ are quite different in general; however, the prime factors of $\phi(\phi(n))$ and $\lambda(\lambda(n))$ are very similar. Since

$$\frac{n}{\lambda(\lambda(n))} = \frac{n}{\phi(\phi(n))} \frac{\phi(\phi(n))}{\lambda(\lambda(n))}$$

and $n/\phi(\phi(n)) \ll (\log\log n)^2$, it suffices to show that

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

The idea of the proof is to compare $\phi(\phi(n))$ and $\lambda(\lambda(n))$ one prime at a time.

The ϕ-function enters the picture

The prime factors of n and of $\lambda(\lambda(n))$ are quite different in general; however, the prime factors of $\phi(\phi(n))$ and $\lambda(\lambda(n))$ are very similar. Since

$$\frac{n}{\lambda(\lambda(n))} = \frac{n}{\phi(\phi(n))} \frac{\phi(\phi(n))}{\lambda(\lambda(n))}$$

and $n/\phi(\phi(n)) \ll (\log\log n)^2$, it suffices to show that

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

The idea of the proof is to compare $\phi(\phi(n))$ and $\lambda(\lambda(n))$ one prime at a time.

The ϕ-function enters the picture

The prime factors of n and of $\lambda(\lambda(n))$ are quite different in general; however, the prime factors of $\phi(\phi(n))$ and $\lambda(\lambda(n))$ are very similar. Since

$$\frac{n}{\lambda(\lambda(n))} = \frac{n}{\phi(\phi(n))} \frac{\phi(\phi(n))}{\lambda(\lambda(n))}$$

and $n/\phi(\phi(n)) \ll (\log\log n)^2$, it suffices to show that

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \text{ has normal order } (\log\log n)^2 \log\log\log n.$$

The idea of the proof is to compare $\phi(\phi(n))$ and $\lambda(\lambda(n))$ one prime at a time.

Decomposition into individual prime factors

If $v_p(m)$ denotes the multiplicity with which p divides m, then

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} = \sum_p \Big(v_p\big(\phi(\phi(n))\big) - v_p\big(\lambda(\lambda(n))\big) \Big) \log p.$$

- For most "large" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is typically the same as $v_p\big(\phi(\phi(n))\big)$.
- For "small" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is much smaller than $v_p\big(\phi(\phi(n))\big)$ on average.

The conclusion is that for almost all integers n,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p \text{ small}} v_p\big(\phi(\phi(n))\big) \log p.$$

Decomposition into individual prime factors

If $v_p(m)$ denotes the multiplicity with which p divides m, then

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} = \sum_p \Big(v_p\big(\phi(\phi(n))\big) - v_p\big(\lambda(\lambda(n))\big) \Big) \log p.$$

- For most "large" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is typically the same as $v_p\big(\phi(\phi(n))\big)$.
- For "small" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is much smaller than $v_p\big(\phi(\phi(n))\big)$ on average.

The conclusion is that for almost all integers n,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p \text{ small}} v_p\big(\phi(\phi(n))\big) \log p.$$

Decomposition into individual prime factors

If $v_p(m)$ denotes the multiplicity with which p divides m, then

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} = \sum_p \Big(v_p\big(\phi(\phi(n))\big) - v_p\big(\lambda(\lambda(n))\big) \Big) \log p.$$

- For most "large" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is typically the same as $v_p\big(\phi(\phi(n))\big)$.
- For "small" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is much smaller than $v_p\big(\phi(\phi(n))\big)$ on average.

The conclusion is that for almost all integers n,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p \text{ small}} v_p\big(\phi(\phi(n))\big) \log p.$$

Decomposition into individual prime factors

If $v_p(m)$ denotes the multiplicity with which p divides m, then

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} = \sum_p \Big(v_p\big(\phi(\phi(n))\big) - v_p\big(\lambda(\lambda(n))\big) \Big) \log p.$$

- For most "large" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is typically the same as $v_p\big(\phi(\phi(n))\big)$.
- For "small" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is much smaller than $v_p\big(\phi(\phi(n))\big)$ on average.

The conclusion is that for almost all integers n,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p \text{ small}} v_p\big(\phi(\phi(n))\big) \log p.$$

Decomposition into individual prime factors

If $v_p(m)$ denotes the multiplicity with which p divides m, then

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} = \sum_p \Big(v_p\big(\phi(\phi(n))\big) - v_p\big(\lambda(\lambda(n))\big) \Big) \log p.$$

- For most "large" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is typically the same as $v_p\big(\phi(\phi(n))\big)$.
- For "small" primes p, we show that $v_p\big(\lambda(\lambda(n))\big)$ is much smaller than $v_p\big(\phi(\phi(n))\big)$ on average.

The conclusion is that for almost all integers $n \asymp x$,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p < (\log\log x)^2} v_p\big(\phi(\phi(n))\big) \log p.$$

Reduction to an additive function

For almost all integers $n \asymp x$,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p<(\log\log x)^2} v_p\big(\phi(\phi(n))\big) \log p$$

If n has prime factors, ℓ, such that $\ell - 1$ has prime factors, q, such that $q \equiv 1 \pmod{p}$, then factors of p will arise in $\phi(\phi(n))$. The contribution from such primes is counted by the function

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p<(\log\log x)^2} v_p(q-1) \log p \Bigg)$$

Although there are other ways for p to divide $\phi(\phi(n))$, this additive function is typically the dominant contribution.

Reduction to an additive function

For almost all integers $n \asymp x$,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p<(\log\log x)^2} v_p\big(\phi(\phi(n))\big) \log p$$

If n has prime factors, ℓ, such that $\ell - 1$ has prime factors, q, such that $q \equiv 1 \pmod{p}$, then factors of p will arise in $\phi(\phi(n))$.

The contribution from such primes is counted by the function

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p<(\log\log x)^2} v_p(q-1) \log p \Bigg)$$

Although there are other ways for p to divide $\phi(\phi(n))$, this additive function is typically the dominant contribution.

Reduction to an additive function

For almost all integers $n \asymp x$,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim \sum_{p<(\log\log x)^2} v_p\big(\phi(\phi(n))\big) \log p$$

If n has prime factors, ℓ, such that $\ell - 1$ has prime factors, q, such that $q \equiv 1 \pmod{p}$, then factors of p will arise in $\phi(\phi(n))$. The contribution from such primes is counted by the function

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p<(\log\log x)^2} v_p(q-1) \log p \Bigg)$$

Although there are other ways for p to divide $\phi(\phi(n))$, this additive function is typically the dominant contribution.

Reduction to an additive function

For almost all integers $n \asymp x$,

$$\log \frac{\phi(\phi(n))}{\lambda(\lambda(n))} \sim h(n)$$

If n has prime factors, ℓ, such that $\ell - 1$ has prime factors, q, such that $q \equiv 1 \pmod{p}$, then factors of p will arise in $\phi(\phi(n))$. The contribution from such primes is counted by the function

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p < (\log\log x)^2} v_p(q-1) \log p \Bigg)$$

Although there are other ways for p to divide $\phi(\phi(n))$, this additive function is typically the dominant contribution.

The Turán-Kubilius inequality

It suffices to show $(\log\log n)^2 \log\log\log n$ is the normal order of

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p < (\log\log x)^2} v_p(q-1) \log p \Bigg).$$

Turán-Kubilius inequality

If $h(n)$ is additive, then $\sum_{n \le x} (h(n) - M_1)^2 \ll x M_2$, where

$$M_1 = \sum_{p \le x} \frac{h(p)}{p} \quad \text{and} \quad M_2 = \sum_{p \le x} \frac{h(p)^2}{p}.$$

In particular, if $M_2 = o(M_1^2)$, then the normal order of $h(n)$ is M_1.

The Turán-Kubilius inequality

It suffices to show $(\log\log n)^2 \log\log\log n$ is the normal order of

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p < (\log\log x)^2} v_p(q-1) \log p \Bigg).$$

Turán-Kubilius inequality

If $h(n)$ is additive, then $\sum_{n \le x} (h(n) - M_1)^2 \ll x M_2$, where

$$M_1 = \sum_{p \le x} \frac{h(p)}{p} \quad \text{and} \quad M_2 = \sum_{p \le x} \frac{h(p)^2}{p}.$$

In particular, if $M_2 = o(M_1^2)$, then the normal order of $h(n)$ is M_1.

The Turán-Kubilius inequality

It suffices to show $(\log\log n)^2 \log\log\log n$ is the normal order of

$$h(n) = \sum_{\ell \mid n} \Bigg(\sum_{q \mid (\ell-1)} \sum_{p < (\log\log x)^2} v_p(q-1) \log p \Bigg).$$

Turán-Kubilius inequality

If $h(n)$ is additive, then $\sum_{n \le x} (h(n) - M_1)^2 \ll x M_2$, where

$$M_1 = \sum_{p \le x} \frac{h(p)}{p} \quad \text{and} \quad M_2 = \sum_{p \le x} \frac{h(p)^2}{p}.$$

In particular, if $M_2 = o(M_1^2)$, then the normal order of $h(n)$ is M_1.

Conjecture for higher iterates of λ

Let $\lambda_1(n) = \lambda(n)$, $\lambda_2(n) = \lambda(\lambda(n))$, $\lambda_3(n) = \lambda(\lambda(\lambda(n)))$, and so on. We know:

1. $\log\left(\frac{n}{\lambda(n)}\right)$ has normal order $\log\log n \log\log\log n$
2. $\log\left(\frac{n}{\lambda(\lambda(n))}\right)$ has normal order $(\log\log n)^2 \log\log\log n$

Conjecture

$$\log\left(\frac{n}{\lambda_k(n)}\right) \text{ has normal order } \frac{1}{(k-1)!}(\log\log n)^k \log\log\log n.$$

What are the challenges to proving this conjecture?

Conjecture for higher iterates of λ

Let $\lambda_1(n) = \lambda(n)$, $\lambda_2(n) = \lambda(\lambda(n))$, $\lambda_3(n) = \lambda(\lambda(\lambda(n)))$, and so on. We know:

1. $\log\left(\dfrac{n}{\lambda(n)}\right)$ has normal order $\log\log n \log\log\log n$
2. $\log\left(\dfrac{n}{\lambda(\lambda(n))}\right)$ has normal order $(\log\log n)^2 \log\log\log n$

Conjecture

$$\log\left(\frac{n}{\lambda_k(n)}\right) \text{ has normal order } \frac{1}{(k-1)!}(\log\log n)^k \log\log\log n.$$

What are the challenges to proving this conjecture?

Conjecture for higher iterates of λ

Let $\lambda_1(n) = \lambda(n)$, $\lambda_2(n) = \lambda(\lambda(n))$, $\lambda_3(n) = \lambda(\lambda(\lambda(n)))$, and so on. We know:

1. $\log\left(\frac{n}{\lambda(n)}\right)$ has normal order $\log\log n \log\log\log n$
2. $\log\left(\frac{n}{\lambda(\lambda(n))}\right)$ has normal order $(\log\log n)^2 \log\log\log n$

Conjecture

$$\log\left(\frac{n}{\lambda_k(n)}\right) \text{ has normal order } \frac{1}{(k-1)!}(\log\log n)^k \log\log\log n.$$

What are the challenges to proving this conjecture?

Conjecture for higher iterates of λ

Let $\lambda_1(n) = \lambda(n)$, $\lambda_2(n) = \lambda(\lambda(n))$, $\lambda_3(n) = \lambda(\lambda(\lambda(n)))$, and so on. We know:

1. $\log\left(\dfrac{n}{\lambda(n)}\right)$ has normal order $\log\log n \log\log\log n$
2. $\log\left(\dfrac{n}{\lambda(\lambda(n))}\right)$ has normal order $(\log\log n)^2 \log\log\log n$

Conjecture

$\log\left(\dfrac{n}{\lambda_k(n)}\right)$ has normal order $\dfrac{1}{(k-1)!}(\log\log n)^k \log\log\log n$.

What are the challenges to proving this conjecture?

Conjecture for higher iterates of λ

Let $\lambda_1(n) = \lambda(n)$, $\lambda_2(n) = \lambda(\lambda(n))$, $\lambda_3(n) = \lambda(\lambda(\lambda(n)))$, and so on. We know:

1. $\log\left(\dfrac{n}{\lambda(n)}\right)$ has normal order $\log\log n \log\log\log n$
2. $\log\left(\dfrac{n}{\lambda(\lambda(n))}\right)$ has normal order $(\log\log n)^2 \log\log\log n$

Conjecture

$\log\left(\dfrac{n}{\lambda_k(n)}\right)$ has normal order $\dfrac{1}{(k-1)!}(\log\log n)^k \log\log\log n$.

What are the challenges to proving this conjecture?

The "supersquarefree case"

Mentioned earlier: the "large" primes dividing $\phi(\phi(n))$ and $\lambda(\lambda(n))$ typically occur to the same multiplicites.

To confirm this, we needed to bound $v_p(\phi(\phi(n)))$ on average for "large" primes p.

This requires answering: how might p^m divide $\phi(\phi(n))$?

The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

The "supersquarefree case"

Mentioned earlier: the "large" primes dividing $\phi(\phi(n))$ and $\lambda(\lambda(n))$ typically occur to the same multiplicites.

To confirm this, we needed to bound $v_p(\phi(\phi(n)))$ on average for "large" primes p.

This requires answering: how might p^m divide $\phi(\phi(n))$?

The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

The "supersquarefree case"

Mentioned earlier: the "large" primes dividing $\phi(\phi(n))$ and $\lambda(\lambda(n))$ typically occur to the same multiplicites.

To confirm this, we needed to bound $v_p(\phi(\phi(n)))$ on average for "large" primes p.

This requires answering: how might p^m divide $\phi(\phi(n))$?

The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

The "supersquarefree case"

How might p^m divide $\phi(\phi(n))$? The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

Other possibilities all require at least one of the following:

- $p^2 \mid n$
- n has a prime factor $\ell \equiv 1 \pmod{p^2}$
- n has two distinct prime factors $\ell_1 \equiv \ell_2 \equiv 1 \pmod{p}$
- n has a prime factor ℓ with two distinct primes $q_1, q_2 \equiv 1 \pmod{p}$ satisfying $q_1 q_2 \mid (\ell - 1)$

The "supersquarefree case"

How might p^m divide $\phi(\phi(n))$? The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

Other possibilities all require at least one of the following:

- $p^2 \mid n$
- n has a prime factor $\ell \equiv 1 \pmod{p^2}$
- n has two distinct prime factors $\ell_1 \equiv \ell_2 \equiv 1 \pmod{p}$
- n has a prime factor ℓ with two distinct primes $q_1, q_2 \equiv 1 \pmod{p}$ satisfying $q_1 q_2 \mid (\ell - 1)$

The "supersquarefree case"

How might p^m divide $\phi(\phi(n))$? The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

Other possibilities all require at least one of the following:

- $p^2 \mid n$
- n has a prime factor $\ell \equiv 1 \pmod{p^2}$
- n has two distinct prime factors $\ell_1 \equiv \ell_2 \equiv 1 \pmod{p}$
- n has a prime factor ℓ with two distinct primes $q_1, q_2 \equiv 1 \pmod{p}$ satisfying $q_1 q_2 \mid (\ell - 1)$

The "supersquarefree case"

How might p^m divide $\phi(\phi(n))$? The most common way:

Supersquarefree case

There exist m distinct prime factors $\ell_1, \dots, \ell_m$ of n, each with a corresponding prime $q_j \equiv 1 \pmod{p}$ satisfying $q_j \mid (\ell_j - 1)$.

Other possibilities all require at least one of the following:

- $p^2 \mid n$
- n has a prime factor $\ell \equiv 1 \pmod{p^2}$
- n has two distinct prime factors $\ell_1 \equiv \ell_2 \equiv 1 \pmod{p}$
- n has a prime factor ℓ with two distinct primes $q_1, q_2 \equiv 1 \pmod{p}$ satisfying $q_1 q_2 \mid (\ell - 1)$

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?

We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?
We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?
We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?
We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?
We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

The "supersquarefree case"

The generalization requires asking: how might p^m divide $\phi_k(n)$?
We believe the most common way is still:

Supersquarefree case

There exist distinct primes $q_{1,1}, \dots, q_{1,m} \mid n$,
distinct primes $q_{2,1} \mid (q_{1,1} - 1), \dots, q_{2,m} \mid (q_{1,m} - 1)$,
$\dots$, and
distinct primes $q_{k,1} \mid (q_{k-1,1} - 1), \dots, q_{k,m} \mid (q_{k-1,m} - 1)$
with $q_{k,1} \equiv \cdots \equiv q_{k,m} \equiv 1 \pmod{p}$.

Challenge 1

Enumerate all other possibilities, and bound the frequency of each one on average over "large" primes p.

Normal order of the corresponding additive function

The supersquarefree case is important for "small" primes too, encoded in the additive function

$$h(n) = \sum_{r|n} \sum_{q|(r-1)} \sum_{p<(\log\log x)^2} v_p(q-1)\log p.$$

Challenge 2

Find the normal order of h_k; in particular, find an asymptotic formula for the sum over primes $\sum_{\ell<x} h_k(\ell)/\ell$.

A heuristic evaluation, using the main terms in asymptotic formulas for primes in arithmetic progressions, suggests that h_k has normal order $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$; but the required uniformity in the error terms is problematic.

Normal order of the corresponding additive function

The supersquarefree case is important for "small" primes too, encoded in the additive function

$$h_k(n) = \sum_{q_1 \mid n} \sum_{q_2 \mid (q_1-1)} \cdots \sum_{q_k \mid (q_{k-1}-1)} \sum_{p < (\log\log x)^k} v_p(q_k - 1) \log p.$$

Challenge 2

Find the normal order of h_k; in particular, find an asymptotic formula for the sum over primes $\sum_{\ell < x} h_k(\ell)/\ell$.

A heuristic evaluation, using the main terms in asymptotic formulas for primes in arithmetic progressions, suggests that h_k has normal order $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$; but the required uniformity in the error terms is problematic.

Normal order of the corresponding additive function

The supersquarefree case is important for "small" primes too, encoded in the additive function

$$h_k(n) = \sum_{q_1 \mid n} \sum_{q_2 \mid (q_1-1)} \cdots \sum_{q_k \mid (q_{k-1}-1)} \sum_{p < (\log\log x)^k} v_p(q_k - 1) \log p.$$

Challenge 2

Find the normal order of h_k; in particular, find an asymptotic formula for the sum over primes $\sum_{\ell < x} h_k(\ell)/\ell$.

A heuristic evaluation, using the main terms in asymptotic formulas for primes in arithmetic progressions, suggests that h_k has normal order $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$; but the required uniformity in the error terms is problematic.

Normal order of the corresponding additive function

The supersquarefree case is important for "small" primes too, encoded in the additive function

$$h_k(n) = \sum_{q_1 \mid n} \sum_{q_2 \mid (q_1-1)} \cdots \sum_{q_k \mid (q_{k-1}-1)} \sum_{p < (\log\log x)^k} v_p(q_k - 1) \log p.$$

Challenge 2

Find the normal order of h_k; in particular, find an asymptotic formula for the sum over primes $\sum_{\ell < x} h_k(\ell)/\ell$.

A heuristic evaluation, using the main terms in asymptotic formulas for primes in arithmetic progressions, suggests that h_k has normal order $\frac{1}{(k-1)!}(\log\log n)^k \log\log\log n$; but the required uniformity in the error terms is problematic.