Values of the Carmichael function versus values of the Euler function

Analytic Number Theory and Surrounding Areas

RIMS – Kyoto, JAPAN

Francesco Pappalardi

October 21, 2004

Introduction

Introduction

$$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$$ Euler φ function

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \quad \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \quad \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Elementary facts:

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \quad \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Elementary facts:

✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \ \ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \ \ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \operatorname{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \ \ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \mathrm{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)
- ✎ $\lambda(n)$ and $\varphi(n)$ have the same prime factors

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \ \ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \operatorname{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)
- ✎ $\lambda(n)$ and $\varphi(n)$ have the same prime factors
- ✎ $\lambda(2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \operatorname{lcm}\{\lambda(2^\alpha), p_1^{\alpha_1 - 1}(p_1 - 1), \ldots, p_s^{\alpha_s - 1}(p_s - 1)\}$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$= \min\{k \in \mathbb{N}$ s.t. $a^k \equiv 1 \bmod n \quad \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \mathrm{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)
- ✎ $\lambda(n)$ and $\varphi(n)$ have the same prime factors
- ✎ $\lambda(2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \mathrm{lcm}\{\lambda(2^\alpha), p_1^{\alpha_1-1}(p_1-1), \ldots, p_s^{\alpha_s-1}(p_s-1)\}$
- ✎ $\lambda(2^\alpha) = 2^{\alpha-2}$ if $\alpha \geq 3$, $\lambda(4) = 2$, $\lambda(2) = 1$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$= \min\{k \in \mathbb{N}$ s.t. $a^k \equiv 1 \bmod n \;\; \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \mathrm{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)
- ✎ $\lambda(n)$ and $\varphi(n)$ have the same prime factors
- ✎ $\lambda(2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \mathrm{lcm}\{\lambda(2^\alpha), p_1^{\alpha_1-1}(p_1-1), \ldots, p_s^{\alpha_s-1}(p_s-1)\}$
- ✎ $\lambda(2^\alpha) = 2^{\alpha-2}$ if $\alpha \geq 3$, $\lambda(4) = 2$, $\lambda(2) = 1$
- ✎ n is a Carmichael number iff $\lambda(n) \mid n-1$

Introduction

$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$ Euler φ function

$\lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^*$ Carmichael λ function

$$= \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n \ \ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$$

Elementary facts:

- ✎ $\varphi(n) = \lambda(n)$ iff $n = 2, 4, p^a, 2p^a$ with $p \geq 3$
- ✎ $\lambda(n) \mid \varphi(n)$ $\forall n \in \mathbb{N}$
- ✎ if $(n, m) = 1$ then $\lambda(nm) = \operatorname{lcm}(\lambda(n), \lambda(m))$ (λ is not multiplicative)
- ✎ $\lambda(n)$ and $\varphi(n)$ have the same prime factors
- ✎ $\lambda(2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \operatorname{lcm}\{\lambda(2^\alpha), p_1^{\alpha_1 - 1}(p_1 - 1), \ldots, p_s^{\alpha_s - 1}(p_s - 1)\}$
- ✎ $\lambda(2^\alpha) = 2^{\alpha-2}$ if $\alpha \geq 3$, $\lambda(4) = 2$, $\lambda(2) = 1$
- ✎ n is a Carmichael number iff $\lambda(n) \mid n - 1$
- ✎ if $n = pq$ is an RSA module then $\lambda(n)$ should not be too small.

Minimal, Normal and Average Orders of λ

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

☞ $\lambda(n) > (\log n)^{1.44 \log_3 n}$ for all large n;

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

- ☞ $\lambda(n) > (\log n)^{1.44 \log_3 n}$ for all large n;

- ☞ $\lambda(n) < (\log n)^{3.24 \log_3 n}$ for ∞-many n's;

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

☞ $\lambda(n) > (\log n)^{1.44 \log_3 n}$ for all large n;

☞ $\lambda(n) < (\log n)^{3.24 \log_3 n}$ for ∞-many n's;

☞ $\lambda(n) = n(\log n)^{-\log_3 n - A + E(n)}$ for almost all n.

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

- ☞ $\lambda(n) > (\log n)^{1.44 \log_3 n}$ for all large n;
- ☞ $\lambda(n) < (\log n)^{3.24 \log_3 n}$ for ∞-many n's;
- ☞ $\lambda(n) = n(\log n)^{-\log_3 n - A + E(n)}$ for almost all n.

  $$A = -1 + \sum_l \frac{\log l}{(l-1)^2} = 0.2269688\cdots, \ E(n) \ll (\log_2 n)^{\varepsilon - 1} \ \forall \varepsilon > 0 \text{ fixed};$$

Minimal, Normal and Average Orders of λ

Erdős, Pomerance & Schmutz (1991):

- $\lambda(n) > (\log n)^{1.44 \log_3 n}$ for all large n;
- $\lambda(n) < (\log n)^{3.24 \log_3 n}$ for ∞-many n's;
- $\lambda(n) = n(\log n)^{-\log_3 n - A + E(n)}$ for almost all n.

  $A = -1 + \sum_l \frac{\log l}{(l-1)^2} = 0.2269688\cdots$, $E(n) \ll (\log_2 n)^{\varepsilon - 1}$ $\forall \varepsilon > 0$ fixed;
- Let $B = e^{-\gamma} \prod_l \left(1 - \frac{1}{(l-1)^2(l+1)}\right) = 0.37537\cdots$. Then

$$\sum_{n \le x} \lambda(n) = \frac{x^2}{\log x} \exp\left\{\frac{B \log_2 x}{\log_3 x}(1 + o(1))\right\} \quad (x \to +\infty)$$

A recent result

A recent result

Friedlander, Pomerance & Shparlinski (2001):

A recent result

Friedlander, Pomerance & Shparlinski (2001):

☞ $\forall \Delta \geq (\log\log N)^3$,

A recent result

Friedlander, Pomerance & Shparlinski (2001):

☞ $\forall \Delta \geq (\log\log N)^3$,

$$\lambda(n) \geq N \exp(-\Delta)$$

for all n with $1 \leq n \leq N$, with at most $N \exp(-0.69(\Delta \log \Delta)^{1/3})$ exceptions

A recent result

Friedlander, Pomerance & Shparlinski (2001):

☞ $\forall\Delta \geq (\log\log N)^3$,

$$\lambda(n) \geq N\exp(-\Delta)$$

for all n with $1 \leq n \leq N$, with at most $N\exp(-0.69(\Delta\log\Delta)^{1/3})$ exceptions

Has Cryptographic Application...

A recent result

Friedlander, Pomerance & Shparlinski (2001):

☞ $\forall \Delta \geq (\log\log N)^3$,

$$\lambda(n) \geq N \exp(-\Delta)$$

for all n with $1 \leq n \leq N$, with at most $N \exp(-0.69(\Delta \log \Delta)^{1/3})$ exceptions

Has Cryptographic Application...

☞Most of the times $\lambda(pq)$ is not too small...

λ-analogue of the Artin Conjecture 1/3

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\text{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\text{ord}_n(a) = \lambda(n)$$

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

✎If $r(n)$ is the number of λ-primitive roots modulo n in $(\mathbb{Z}/n\mathbb{Z})^*$. Then

$$r(n) = \varphi(n) \prod_{p|\lambda(n)} \left(1 - p^{-\Lambda_n(p)}\right)$$

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

✎If $r(n)$ is the number of λ-primitive roots modulo n in $(\mathbb{Z}/n\mathbb{Z})^*$. Then

$$r(n) = \varphi(n) \prod_{p|\lambda(n)} \left(1 - p^{-\Lambda_n(p)}\right)$$

where $\Lambda_n(p)$ is the number of summand with highest p–th power exponent in the decomposition of $(\mathbb{Z}/n\mathbb{Z})^*$ a product of cyclic groups

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

✎If $r(n)$ is the number of λ-primitive roots modulo n in $(\mathbb{Z}/n\mathbb{Z})^*$. Then

$$r(n) = \varphi(n) \prod_{p \mid \lambda(n)} \left(1 - p^{-\Lambda_n(p)}\right)$$

where $\Lambda_n(p)$ is the number of summand with highest p–th power exponent in the decomposition of $(\mathbb{Z}/n\mathbb{Z})^*$ a product of cyclic groups

✎Li (1998): $r(n)/\varphi(n)$ does't have a continuous distribution

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

✎If $r(n)$ is the number of λ-primitive roots modulo n in $(\mathbb{Z}/n\mathbb{Z})^*$. Then

$$r(n) = \varphi(n) \prod_{p|\lambda(n)} \left(1 - p^{-\Lambda_n(p)}\right)$$

where $\Lambda_n(p)$ is the number of summand with highest p–th power exponent in the decomposition of $(\mathbb{Z}/n\mathbb{Z})^*$ a product of cyclic groups

✎Li (1998): $r(n)/\varphi(n)$ does't have a continuous distribution

✎$r(p) = \varphi(p-1)$

λ-analogue of the Artin Conjecture 1/3

✎If $a, n \in \mathbb{N}$ with $(a, n) = 1$, then

$$\mathrm{ord}_n(a) = \min\{k \in \mathbb{N} \text{ s.t. } a^k \equiv 1 \bmod n\}.$$

✎We say that a is a λ–primitive root modulo n if

$$\mathrm{ord}_n(a) = \lambda(n)$$

(i.e. a has the maximum possible order modulo n)

✎If $r(n)$ is the number of λ-primitive roots modulo n in $(\mathbb{Z}/n\mathbb{Z})^*$. Then

$$r(n) = \varphi(n) \prod_{p|\lambda(n)} \left(1 - p^{-\Lambda_n(p)}\right)$$

where $\Lambda_n(p)$ is the number of summand with highest p–th power exponent in the decomposition of $(\mathbb{Z}/n\mathbb{Z})^*$ a product of cyclic groups

✎Li (1998): $r(n)/\varphi(n)$ does't have a continuous distribution

✎$r(p) = \varphi(p-1)$

✎Kátai (1968): $\varphi(p-1)/(p-1)$ has a continuous distribution

λ-analogue of the Artin Conjecture 2/3

λ-analogue of the Artin Conjecture 2/3

✎Artin Conjecture. If $a \neq \square, \pm 1$, $\exists A_a > 0$, s.t.

$$\#\{p \leq x \mid a \text{ is a primitive root mod } p\} \sim A_a \operatorname{li}(x).$$

λ-analogue of the Artin Conjecture 2/3

✎Artin Conjecture. If $a \neq \square, \pm 1$, $\exists A_a > 0$, s.t.

$$\#\{p \leq x \mid a \text{ is a primitive root mod } p\} \sim A_a \operatorname{li}(x).$$

(It is a Theorem under GRH (Hooley's Theorem))

λ-analogue of the Artin Conjecture 2/3

✎Artin Conjecture. If $a \neq \square, \pm 1$, $\exists A_a > 0$, s.t.

$$\#\{p \le x \mid a \text{ is a primitive root mod } p\} \sim A_a \operatorname{li}(x).$$

(It is a Theorem under GRH (Hooley's Theorem))

✎Let

$$N_a(x) = \#\{n \le x \mid (a,n) = 1,\ a \text{ is a } \lambda\text{–primitive root modulo } n\}$$

λ-analogue of the Artin Conjecture 2/3

✎Artin Conjecture. If $a \neq \square, \pm 1$, $\exists A_a > 0$, s.t.

$$\#\{p \leq x \mid a \text{ is a primitive root mod } p\} \sim A_a \operatorname{li}(x).$$

(It is a Theorem under GRH (Hooley's Theorem))

✎Let

$$N_a(x) = \#\{n \leq x \mid (a,n) = 1,\ a \text{ is a } \lambda\text{–primitive root modulo } n\}$$

✎Question(λ-Artin Conjecture): Determine when/if $\exists B_a > 0$, with

$$N_a(x) \sim B_a x?$$

λ-analogue of the Artin Conjecture 3/3

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) > 0 \qquad \text{but} \qquad \liminf_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = 0.$$

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty}\frac{1}{x^2}\sum_{1\le a\le x}N_a(x)>0 \qquad \text{but} \qquad \liminf_{x\to\infty}\frac{1}{x^2}\sum_{1\le a\le x}N_a(x)=0.$$

(λ–Artin Conjecture is wrong on Average)

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) > 0 \qquad \text{but} \qquad \liminf_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = 0.$$

(λ–Artin Conjecture is wrong on Average)

✎Li & Pomerance (2003): On GRH, $\exists A > 0$ such that

$$\limsup_{x\to\infty} \frac{N_a(x)}{x} \ge \frac{A\varphi(|a|)}{|a|},$$

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty}\frac{1}{x^2}\sum_{1\le a\le x}N_a(x)>0 \qquad \text{but} \qquad \liminf_{x\to\infty}\frac{1}{x^2}\sum_{1\le a\le x}N_a(x)=0.$$

(λ–Artin Conjecture is wrong on Average)

✎Li & Pomerance (2003): On GRH, $\exists A>0$ such that

$$\limsup_{x\to\infty}\frac{N_a(x)}{x}\ge\frac{A\varphi(|a|)}{|a|},$$

as long as $a\notin\mathcal{E}:=\{-\Box,\pm2\Box,m^c(c\ge2)\}$ while if $a\in\mathcal{E}\Longrightarrow N_a(x)=o(x)$.

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) > 0 \qquad \text{but} \qquad \liminf_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = 0.$$

(λ–Artin Conjecture is wrong on Average)

✎Li & Pomerance (2003): On GRH, $\exists A > 0$ such that

$$\limsup_{x\to\infty} \frac{N_a(x)}{x} \ge \frac{A\varphi(|a|)}{|a|},$$

as long as $a \notin \mathcal{E} := \{-\square, \pm 2\square, m^c (c \ge 2)\}$ while if $a \in \mathcal{E} \Longrightarrow N_a(x) = o(x)$.

✎Li (1999): For all $a \in \mathbb{Z}$,

$$\liminf_{x\to\infty} \frac{N_a(x)}{x} = 0$$

λ-analogue of the Artin Conjecture 3/3

✎Li (2000):

$$\limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) > 0 \qquad \text{but} \qquad \liminf_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = 0.$$

(λ–Artin Conjecture is wrong on Average)

✎Li & Pomerance (2003): On GRH, $\exists A > 0$ such that

$$\limsup_{x\to\infty} \frac{N_a(x)}{x} \ge \frac{A\varphi(|a|)}{|a|},$$

as long as $a \notin \mathcal{E} := \{-\square, \pm 2\square, m^c (c \ge 2)\}$ while if $a \in \mathcal{E} \Longrightarrow N_a(x) = o(x)$.

✎Li (1999): For all $a \in \mathbb{Z}$,

$$\liminf_{x\to\infty} \frac{N_a(x)}{x} = 0$$

(λ–Artin Conjecture is always wrong)

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

✎Shparlinski & Luca (2003)

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

✎Shparlinski & Luca (2003)

☞Let

$$u(n) := \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}/\mathbb{Z}^*} \mathrm{ord}_n(a)$$

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

✎Shparlinski & Luca (2003)

☞Let

$$u(n) := \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}/\mathbb{Z}^*} \mathrm{ord}_n(a)$$

(the average multiplicative order of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$)

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

✎Shparlinski & Luca (2003)

☞Let

$$u(n) := \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}/\mathbb{Z}^*} \mathrm{ord}_n(a)$$

(the average multiplicative order of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$)

☞

$$\liminf_{n\to\infty} \frac{u(n)\log\log n}{\lambda(n)} = \frac{\pi^2}{6e^\gamma} \qquad \text{and} \qquad \limsup_{n\to\infty} \frac{u(n)}{\lambda(n)} = 1$$

λ vs average order of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

✎Shparlinski & Luca (2003)

☞Let

$$u(n) := \frac{1}{\varphi(n)} \sum_{a \in \mathbb{Z}/\mathbb{Z}^*} \mathrm{ord}_n(a)$$

(the average multiplicative order of the elements of $(\mathbb{Z}/n\mathbb{Z})^*$)

☞

$$\liminf_{n\to\infty} \frac{u(n)\log\log n}{\lambda(n)} = \frac{\pi^2}{6e^\gamma} \qquad \text{and} \qquad \limsup_{n\to\infty} \frac{u(n)}{\lambda(n)} = 1$$

☞The sequence

$$(\ u(n)/\lambda(n)\ )_{n\in\mathbb{N}}$$

is dense in $[0,1]$

k–free values of φ

k–free values of φ

✎Banks & FLP (2003)

k–free values of φ

✎Banks & FP (2003)

$$\mathcal{S}_{\varphi}^{k}(x) = \{n \le x \text{ t.c. } \varphi(n) \text{ is } k\text{–free}\}.$$

k–free values of φ

✎Banks & FP (2003)

$$\mathcal{S}_\varphi^k(x) = \{n \le x \text{ t.c. } \varphi(n) \text{ is } k\text{–free}\}.$$

$\forall k \geq 3$,

$$\mathcal{S}_\varphi^k(x) = \frac{3\alpha_k}{2(k-2)!} \frac{x\,(\log\log x)^{k-2}}{\log x}\,(1 + o_k(1)) \qquad (x \to +\infty)$$

k–free values of φ

✎Banks & FP (2003)

$$\mathcal{S}_{\varphi}^{k}(x) = \{n \le x \text{ t.c. } \varphi(n) \text{ is } k\text{–free}\}.$$

$\forall k \ge 3$,

$$\mathcal{S}_{\varphi}^{k}(x) = \frac{3\alpha_k}{2(k-2)!}\frac{x\,(\log\log x)^{k-2}}{\log x}\left(1+o_k(1)\right) \qquad (x \to +\infty)$$

where

$$\alpha_k := \frac{1}{2^{k-1}}\prod_{l>2}\left(1-\frac{1}{l^{k-1}}\sum_{i=0}^{k-2}\sum_{j=0}^{k-2-i}\binom{k-1}{i}\binom{k-1+j}{j}\frac{(l-2)^j}{(l-1)^{i+j+1}}\right).$$

k–free values of λ

k–free values of λ

✎EP, Saidak & Shparlinski (2002)

k–free values of λ

✎EP, Saidak & Shparlinski (2002)

$$\mathcal{S}_\lambda^k(x) = \#\{n \le x \text{ s.t. } \lambda(n) \text{ is } k\text{–free}\}$$

k–free values of λ

✎EP, Saidak & Shparlinski (2002)

$$\mathcal{S}_\lambda^k(x) = \#\{n \le x \text{ s.t. } \lambda(n) \ \text{ is } k\text{–free}\}$$

$\forall k \ge 3$,

$$\mathcal{S}_\lambda^k(x) = (\kappa_k + o(1)) \frac{x}{\log^{1-\alpha_k} x} \qquad (x \to +\infty)$$

k–free values of λ

✎EP, Saidak & Shparlinski (2002)

$$\mathcal{S}_\lambda^k(x) = \#\{n \le x \text{ s.t. } \lambda(n) \text{ is } k\text{–free}\}$$

$\forall k \ge 3$,

$$\mathcal{S}_\lambda^k(x) = (\kappa_k + o(1)) \frac{x}{\log^{1-\alpha_k} x} \qquad (x \to +\infty)$$

where

$$\kappa_k := \frac{2^{k+2}-1}{2^{k+2}-2} \cdot \frac{\eta_k}{e^{\gamma\alpha_k}\Gamma(\alpha_k)}, \quad \alpha_k := \prod_{l \text{ prime}} \left(1 - \frac{1}{l^{k-1}(l-1)}\right)$$

k–free values of λ

✎EP, Saidak & Shparlinski (2002)

$$\mathcal{S}_\lambda^k(x) = \#\{n \leq x \text{ s.t. } \lambda(n) \text{ is } k\text{–free}\}$$

$\forall k \geq 3$,

$$\mathcal{S}_\lambda^k(x) = (\kappa_k + o(1)) \frac{x}{\log^{1-\alpha_k} x} \qquad (x \to +\infty)$$

where

$$\kappa_k := \frac{2^{k+2}-1}{2^{k+2}-2} \cdot \frac{\eta_k}{e^{\gamma\alpha_k}\Gamma(\alpha_k)}, \quad \alpha_k := \prod_{l \text{ prime}} \left(1 - \frac{1}{l^{k-1}(l-1)}\right)$$

$$\eta_k := \lim_{T\to\infty} \frac{1}{\log^{\alpha_k} T} \prod_{\substack{l \leq T \\ l-1 \ k\text{–free}}} \log\left(1 + \frac{1}{l} + \ldots + \frac{1}{l^k}\right)$$

k–free values of λ

✎FP, Saidak & Shparlinski (2002)

$$\mathcal{S}_\lambda^k(x) = \#\{n \le x \text{ s.t. } \lambda(n) \ \text{ is } k\text{–free}\}$$

$\forall k \ge 3$,

$$\mathcal{S}_\lambda^k(x) = (\kappa_k + o(1)) \frac{x}{\log^{1-\alpha_k} x} \qquad (x \to +\infty)$$

where

$$\kappa_k := \frac{2^{k+2}-1}{2^{k+2}-2} \cdot \frac{\eta_k}{e^{\gamma\alpha_k}\Gamma(\alpha_k)}, \quad \alpha_k := \prod_{l \text{ prime}} \left(1 - \frac{1}{l^{k-1}(l-1)}\right)$$

$$\eta_k := \lim_{T\to\infty} \frac{1}{\log^{\alpha_k} T} \prod_{\substack{l \le T \\ l-1 \ k\text{–free}}} \log\left(1 + \frac{1}{l} + \ldots + \frac{1}{l^k}\right)$$

e.g. $k_2 = 0.80328\ldots$ and $\alpha_2 = 0.37395\ldots$.

Carmichael Conjecture

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

Carmichael Conjecture

✎$A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎$\mathcal{B}_\varphi(x) = \{m \leq x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \leq x\}$

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ $\mathcal{B}_\varphi(x) = \{m \leq x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \leq x\}$

✎ Ford (1998)

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ $\mathcal{B}_\varphi(x) = \{m \leq x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \leq x\}$

✎ Ford (1998)

☞ If $\mathcal{B}_\varphi(x) \neq \varnothing$ for some x, then necessarily $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0$

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ $\mathcal{B}_\varphi(x) = \{m \le x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \le x\}$

✎ Ford (1998)

- ☞ If $\mathcal{B}_\varphi(x) \neq \varnothing$ for some x, then necessarily $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0$
- ☞ Hence if $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} = 0$, Carmichael Conjecture follows

Carmichael Conjecture

✎$A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \; \forall m \in \mathbb{N}$

✎$\mathcal{B}_\varphi(x) = \{m \le x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \le x\}$

✎Ford (1998)

- ☞ If $\mathcal{B}_\varphi(x) \neq \emptyset$ for some x, then necessarily $\liminf\limits_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0$
- ☞ Hence if $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} = 0$, Carmichael Conjecture follows
- ☞ $\limsup\limits_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} < 1$

Carmichael Conjecture

✎$A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎$\mathcal{B}_\varphi(x) = \{m \leq x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \leq x\}$

✎Ford (1998)

- ☞ If $\mathcal{B}_\varphi(x) \neq \varnothing$ for some x, then necessarily $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0$
- ☞ Hence if $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} = 0$, Carmichael Conjecture follows
- ☞ $\limsup_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} < 1$
- ☞ $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} < 10^{-5000000000}$

Carmichael Conjecture

✎ $A_\varphi(m) = \#\{n \in \mathbb{N} \mid \varphi(n) = m\}$

Carmichael Conjecture: $A_\varphi(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ $\mathcal{B}_\varphi(x) = \{m \le x \mid A_\varphi(m) = 1\}$ and $\mathcal{F}(x) = \{n \in \mathbb{N} \mid \varphi(n) \le x\}$

✎ Ford (1998)

- ☞ If $\mathcal{B}_\varphi(x) \neq \emptyset$ for some x, then necessarily $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} > 0$
- ☞ Hence if $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} = 0$, Carmichael Conjecture follows
- ☞ $\limsup_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} < 1$
- ☞ $\liminf_{x\to\infty} \frac{\#\mathcal{B}_\varphi(x)}{\#\mathcal{F}(x)} < 10^{-5000000000}$
- ☞ If $A_\varphi(m) = 1$ them $m > 10^{10^{10}}$

Carmichael Conjecture for λ (1/2)

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ: $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ*:* $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ Banks, Friedlander, Luca, FP, Shparlinski (2004)

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ: $A_\lambda(m) \neq 1 \; \forall m \in \mathbb{N}$

✎ Banks, Friedlander, Luca, FP, Shparlinski (2004)

☞ $\forall n \leq x$, $A_\lambda(\lambda(n)) \geq \exp\left((\log\log x)^{10/3}\right)$ with at most $O(x/\log\log x)$ exceptions

Carmichael Conjecture for λ (1/2)

✎$A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ*:* $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

✎Banks, Friedlander, Luca, FP, Shparlinski(2004)

☞ $\forall n \leq x$, $A_\lambda(\lambda(n)) \geq \exp\left((\log\log x)^{10/3}\right)$ with at most $O(x/\log\log x)$ exceptions

☞ $\#\{n \leq x \mid A_\lambda(\lambda(n)) = 1\} \leq x \exp\left(-(\log\log x)^{0.77}\right)$.

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ*:* $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ☞ $\forall n \le x,\ A_\lambda(\lambda(n)) \ge \exp\left((\log\log x)^{10/3}\right)$ with at most $O(x/\log\log x)$ exceptions
- ☞ $\#\{n \le x \mid A_\lambda(\lambda(n)) = 1\} \le x \exp\left(-(\log\log x)^{0.77}\right)$.

  - ✉ The bound $\#\{n \le x \mid A_\varphi(\varphi(n)) = 1\} \le x \exp\left(-\log\log x + o((\log_3 x)^2)\right)$ implies Carmichael Conjecture (for φ)

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ: $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ Banks, Friedlander, Luca, FP, Shparlinski (2004)

☞ $\forall n \leq x$, $A_\lambda(\lambda(n)) \geq \exp\left((\log\log x)^{10/3}\right)$ with at most $O(x/\log\log x)$ exceptions

☞ $\#\{n \leq x \mid A_\lambda(\lambda(n)) = 1\} \leq x \exp\left(-(\log\log x)^{0.77}\right)$.

- The bound $\#\{n \leq x \mid A_\varphi(\varphi(n)) = 1\} \leq x \exp\left(-\log\log x + o((\log_3 x)^2)\right)$ implies Carmichael Conjecture (for φ)
- Non non-trivial upper bound for the above is known

Carmichael Conjecture for λ (1/2)

✎ $A_\lambda(m) = \#\{n \in \mathbb{N} \mid \lambda(n) = m\}$

Carmichael Conjecture for λ: $A_\lambda(m) \neq 1 \ \forall m \in \mathbb{N}$

✎ Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ☞ $\forall n \leq x$, $A_\lambda(\lambda(n)) \geq \exp\left((\log\log x)^{10/3}\right)$ with at most $O(x/\log\log x)$ exceptions
- ☞ $\#\{n \leq x \mid A_\lambda(\lambda(n)) = 1\} \leq x \exp\left(-(\log\log x)^{0.77}\right)$.

  - ✉ The bound $\#\{n \leq x \mid A_\varphi(\varphi(n)) = 1\} \leq x \exp\left(-\log\log x + o((\log_3 x)^2)\right)$ implies Carmichael Conjecture (for φ)
  - ✉ Non non-trivial upper bound for the above is known
  - ✉ Notion of *primitive* counter example to Carmichael Conjecture(s)

Carmichael Conjecture for λ (2/2)

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if

Carmichael Conjecture for λ (2/2)

☞ $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if

✎ $A_\varphi(\varphi(n)) = 1$;

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$
- $\#\mathcal{C}_\varphi(x) \leq x^{2/3+o(1)}$

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$
- $\#\mathcal{C}_\varphi(x) \leq x^{2/3+o(1)}$
- If $\#\mathcal{C}_\lambda(x)$ is the number of primitive counterexamples up to x to the Carmichael conjecture for λ

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$
- $\#\mathcal{C}_\varphi(x) \leq x^{2/3+o(1)}$
- If $\#\mathcal{C}_\lambda(x)$ is the number of primitive counterexamples up to x to the Carmichael conjecture for λ
- A primitive counterexample to the Carmichael conjecture for λ, if it exists, is unique. i.e.

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$
- $\#\mathcal{C}_\varphi(x) \leq x^{2/3+o(1)}$
- If $\#\mathcal{C}_\lambda(x)$ is the number of primitive counterexamples up to x to the Carmichael conjecture for λ
- A primitive counterexample to the Carmichael conjecture for λ, if it exists, is unique. i.e.

$$\boxed{\#\mathcal{C}_\lambda(x) \leq 1}$$

Carmichael Conjecture for λ (2/2)

- $n \in \mathbb{N}$ is a *primitive counterexample to Carmichael conjecture* (CCCP) if
  - $A_\varphi(\varphi(n)) = 1$;
  - $A_\varphi(\varphi(d)) \neq 1 \ \forall d \mid n, d < n$.
- $\mathcal{C}_\varphi(x) = \{n \leq x \mid n \text{ is (CCCP)}\}$
- $\#\mathcal{C}_\varphi(x) \leq x^{2/3+o(1)}$
- If $\#\mathcal{C}_\lambda(x)$ is the number of primitive counterexamples up to x to the Carmichael conjecture for λ
- A primitive counterexample to the Carmichael conjecture for λ, if it exists, is unique. i.e.

$$\boxed{\#\mathcal{C}_\lambda(x) \leq 1}$$

- All counterexamples to Carmichael conjecture for λ (if any) are multiples of the smallest one

Image of φ

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

☞A lot of work on $\mathcal{F}(x)$ (Pillai, Erdős, Hall, Maier, Pomerance, ...)

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

☞A lot of work on $\mathcal{F}(x)$ (Pillai, Erdős, Hall, Maier, Pomerance, ...)

☞Ford (1998)

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

☞A lot of work on $\mathcal{F}(x)$ (Pillai, Erdős, Hall, Maier, Pomerance, ...)

☞Ford (1998)

$$\mathcal{L}(x) = \frac{x}{\log x} \exp\left\{C(\log_3 x - \log_4 x)^2 - D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x + O(1)\right\}$$

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

☞A lot of work on $\mathcal{F}(x)$ (Pillai, Erdős, Hall, Maier, Pomerance, ...)

☞Ford (1998)

$$\mathcal{L}(x) = \frac{x}{\log x} \exp\left\{C(\log_3 x - \log_4 x)^2 - D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x + O(1)\right\}$$

where $C = 0.8178146464008363 2231\cdots$, $D = 2.1769687435594103 2173\cdots$.

Image of φ

☞Denote

$$\mathcal{F} := \{\varphi(m) \mid m \in \mathbb{N}\} \qquad \text{and} \qquad \mathcal{L} := \{\lambda(m) \mid m \in \mathbb{N}\}$$

☞for any set $\mathcal{A}$ and $x \geq 1$, set $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$

☞A lot of work on $\mathcal{F}(x)$ (Pillai, Erdős, Hall, Maier, Pomerance, ...)

☞Ford (1998)

$$\mathcal{L}(x) = \frac{x}{\log x} \exp\left\{C(\log_3 x - \log_4 x)^2 - D\log_3 x - (D + \frac{1}{2} - 2C)\log_4 x + O(1)\right\}$$

where $C = 0.8178146464008363223 1\cdots$, $D = 2.1769687435594103217 3\cdots$.

☞Could not find literature on $\mathcal{L}(x)$

Image of φ vs image of λ

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\#\left(\mathcal{L}\cap\mathcal{F}\right)(x) \ge \frac{x}{\log x}\exp\left((C+o(1))(\log\log\log x)^2\right),$$

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\#\left(\mathcal{L} \cap \mathcal{F}\right)(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),$$

where $C = 0.8178146464008363 2231 \cdots$.

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\#\left(\mathcal{L} \cap \mathcal{F}\right)(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),$$

where $C = 0.8178146464008363 2231 \cdots$.

✎ The number of integers $m \le x$ which are values of λ but not of φ satisfies

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\#\left(\mathcal{L} \cap \mathcal{F}\right)(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),$$

where $C = 0.8178146464008363\,2231\cdots$.

- ✎ The number of integers $m \le x$ which are values of λ but not of φ satisfies

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)$$

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ✎ The number of integers $m \leq x$ which are values of both λ and φ satisfies

$$\boxed{\#\left(\mathcal{L} \cap \mathcal{F}\right)(x) \geq \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),}$$

  where $C = 0.8178146464008363223 1\cdots$.

- ✎ The number of integers $m \leq x$ which are values of λ but not of φ satisfies

$$\boxed{\#(\mathcal{L} \setminus \mathcal{F})(x) \geq \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)}$$

  C as above.

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\#(\mathcal{L} \cap \mathcal{F})(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),$$

where $C = 0.8178146464008363\,2231\cdots$.

- ✎ The number of integers $m \le x$ which are values of λ but not of φ satisfies

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)$$

C as above.

- ✎ The number of integers $m \le x$ which are values of φ but not of λ satisfies

Image of φ vs image of λ

Banks, Friedlander, Luca, FP, Shparlinski (2004)

- ✎ The number of integers $m \le x$ which are values of both λ and φ satisfies

$$\boxed{\#\left(\mathcal{L} \cap \mathcal{F}\right)(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right),}$$

where $C = 0.81781464640083632231\cdots$.

- ✎ The number of integers $m \le x$ which are values of λ but not of φ satisfies

$$\boxed{\#(\mathcal{L} \setminus \mathcal{F})(x) \ge \frac{x}{\log x} \exp\left((C + o(1))(\log\log\log x)^2\right)}$$

C as above.

- ✎ The number of integers $m \le x$ which are values of φ but not of λ satisfies

$$\boxed{\#(\mathcal{F} \setminus \mathcal{L})(x) \gg \frac{x}{\log^2 x}.}$$

Image of φ vs image of λ - Numerical Examples (1/2)

Image of φ vs image of λ - Numerical Examples (1/2)

x	$\#\mathcal{F}(x)$	$\#\mathcal{L}(x)$	$\#(\mathcal{F}\cap\mathcal{L})(x)$	$\#(\mathcal{L}\setminus\mathcal{F})(x)$	$\#(\mathcal{F}\setminus\mathcal{L})(x)$
10	6	6	6	0	0
10^2	38	39	38	1	0
10^3	291	328	291	37	0
10^4	2374	2933	2369	564	5
10^5	20254	27155	20220	6935	34
10^6	180184	256158	179871	76287	313
10^7	1634372	2445343	1631666	813677	2706

Image of φ vs image of λ - Numerical Examples (1/2)

x	$\#\mathcal{F}(x)$	$\#\mathcal{L}(x)$	$\#(\mathcal{F}\cap\mathcal{L})(x)$	$\#(\mathcal{L}\setminus\mathcal{F})(x)$	$\#(\mathcal{F}\setminus\mathcal{L})(x)$
10	6	6	6	0	0
10^2	38	39	38	1	0
10^3	291	328	291	37	0
10^4	2374	2933	2369	564	5
10^5	20254	27155	20220	6935	34
10^6	180184	256158	179871	76287	313
10^7	1634372	2445343	1631666	813677	2706

Criterion. $m\in\mathcal{L} \quad\Leftrightarrow\quad m=\lambda(s)$ with $s=2\prod_{\substack{p \text{ prime}\\ (p-1)\mid m}} p^{v_p(m)+1}$

Image of φ vs image of λ - Numerical Examples (2/2)

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176.$ So $1936 \notin \mathcal{L}$

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176.$ So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936.$ So $1936 \in \mathcal{F}$

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176.$ So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936.$ So $1936 \in \mathcal{F}$

✎$m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \leq 6.113m$.

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176$. So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936$. So $1936 \in \mathcal{F}$

✎$m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \leq 6.113m$.

✎$m = 90 = \lambda(31 \cdot 19) \in \mathcal{L}$ but $90 \notin \mathcal{F}$

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176$. So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936$. So $1936 \in \mathcal{F}$

✎$m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \leq 6.113m$.

✎$m = 90 = \lambda(31 \cdot 19) \in \mathcal{L}$ but $90 \notin \mathcal{F}$

✎Contini, Croot & Shparlinski

Deciding whether a given integer m lies in $\mathcal{F}$ is *NP-complete*.

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176$. So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936$. So $1936 \in \mathcal{F}$

✎$m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \leq 6.113m$.

✎$m = 90 = \lambda(31 \cdot 19) \in \mathcal{L}$ but $90 \notin \mathcal{F}$

✎Contini, Croot & Shparlinski

Deciding whether a given integer m lies in $\mathcal{F}$ is *NP-complete*.

✎$\mathcal{L} \setminus \mathcal{F} = \{90, 174, 230, 234, 246, 290, 308, 318, 364, 390, 410, 414, 450, 510, 516, 530, 534, 572, 594, 638, 644, 666, 678, 680, 702, 714, 728, 740, 770, \ldots\}$

Image of φ vs image of λ - Numerical Examples (2/2)

✎if $m = 1936$ then $s = 33407040 = 2^6 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89$

but $\lambda(33407040) = 176.$ So $1936 \notin \mathcal{L}$

✎$\varphi((2 \cdot 11 + 1) \cdot 89) = \varphi(2047) = 1936.$ So $1936 \in \mathcal{F}$

✎$m \in \mathcal{F}(10^9)$ if and only if $m = \varphi(r)$ for some $r \leq 6.113m$.

✎$m = 90 = \lambda(31 \cdot 19) \in \mathcal{L}$ but $90 \notin \mathcal{F}$

✎Contini, Croot & Shparlinski

Deciding whether a given integer m lies in $\mathcal{F}$ is *NP-complete*.

✎$\mathcal{L} \setminus \mathcal{F} = \{90, 174, 230, 234, 246, 290, 308, 318, 364, 390, 410, 414, 450, 510, 516, 530, 534, 572, 594, 638, 644, 666, 678, 680, 702, 714, 728, 740, 770, \ldots\}$

✎$\mathcal{F} \setminus \mathcal{L} = \{1936, 3872, 6348, 7744, 9196, 15004, 15488, 18392, 20812, 21160, 22264, 30008, 35332, 36784, 38416, 41624, 42320, 44528, 51304, \ldots\}$

Proof of a weaker statement

Proof of a weaker statement

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \gg \frac{x \log\log x}{\log x}.$$

Proof of a weaker statement

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \gg \frac{x \log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x) = \{q_0 q_1 \leq x, \text{s.t.} q_0 \equiv q_1 \equiv 3 \pmod 4 \text{and} (q_0 - 1, q_1 - 1) = 2\}$$

Proof of a weaker statement

$$\#(\mathcal{L}\setminus\mathcal{F})(x) \gg \frac{x\log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x) = \{q_0 q_1 \le x, \text{s.t.} q_0 \equiv q_1 \equiv 3 \pmod 4 \text{and} (q_0 - 1, q_1 - 1) = 2\}$$

Then $\forall n \in \mathcal{P}_2(x)$

$$\lambda(n) = \tfrac{(q_0-1)(q_1-1)}{2} \equiv 2 \pmod 4.$$

Proof of a weaker statement

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \gg \frac{x \log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x) = \{q_0 q_1 \le x, \text{s.t.} q_0 \equiv q_1 \equiv 3 \pmod 4 \text{and} (q_0 - 1, q_1 - 1) = 2\}$$

Then $\forall n \in \mathcal{P}_2(x)$

$$\lambda(n) = \tfrac{(q_0-1)(q_1-1)}{2} \equiv 2 \pmod 4.$$

If $m \in \mathcal{F}$ with $m \equiv 2 \bmod 4$, then $m = 4, 2p^a, p^a$ and $p \equiv 3 \bmod 4$

Proof of a weaker statement

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \gg \frac{x \log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x) = \{q_0 q_1 \le x, \text{s.t.} q_0 \equiv q_1 \equiv 3 \pmod 4 \text{and} (q_0 - 1, q_1 - 1) = 2\}$$

Then $\forall n \in \mathcal{P}_2(x)$

$$\lambda(n) = \tfrac{(q_0-1)(q_1-1)}{2} \equiv 2 \pmod 4.$$

If $m \in \mathcal{F}$ with $m \equiv 2 \bmod 4$, then $m = 4, 2p^a, p^a$ and $p \equiv 3 \bmod 4$

If $m = \lambda(n) \in \mathcal{F}$ then $m \le 3x$

Proof of a weaker statement

$$\#(\mathcal{L} \setminus \mathcal{F})(x) \gg \frac{x \log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x) = \{q_0 q_1 \leq x, \text{s.t.} q_0 \equiv q_1 \equiv 3 \pmod 4 \text{and} (q_0 - 1, q_1 - 1) = 2\}$$

Then $\forall n \in \mathcal{P}_2(x)$

$$\lambda(n) = \tfrac{(q_0-1)(q_1-1)}{2} \equiv 2 \pmod 4.$$

If $m \in \mathcal{F}$ with $m \equiv 2 \bmod 4$, then $m = 4, 2p^a, p^a$ and $p \equiv 3 \bmod 4$

If $m = \lambda(n) \in \mathcal{F}$ then $m \leq 3x$

Hence

$$\#\{\lambda(n) \in \mathcal{F} \mid n \in \mathcal{P}_2(x)\} \leq \#\{p^a \leq 3x\} \ll \frac{x}{\log x}$$

Proof of a weaker statement

$$\#(\mathcal{L}\setminus\mathcal{F})(x) \gg \frac{x\log\log x}{\log x}.$$

Proof. Let

$$\mathcal{P}_2(x)=\{q_0q_1\le x, \text{s.t.} q_0\equiv q_1\equiv 3 \pmod 4 \text{and} (q_0-1,q_1-1)=2\}$$

Then $\forall n\in\mathcal{P}_2(x)$

$$\lambda(n)=\tfrac{(q_0-1)(q_1-1)}{2}\equiv 2 \pmod 4.$$

If $m\in\mathcal{F}$ with $m\equiv 2 \bmod 4$, then $m=4, 2p^a, p^a$ and $p\equiv 3 \bmod 4$

If $m=\lambda(n)\in\mathcal{F}$ then $m\le 3x$

Hence

$$\#\{\lambda(n)\in\mathcal{F}\mid n\in\mathcal{P}_2(x)\}\le\#\{p^a\le 3x\}\ll\frac{x}{\log x}$$

It is enough to show that there are sufficiently many elements in

$$\mathcal{L}_2(x)=\{\lambda(n): n\in\mathcal{P}_2(x)\}\subset\mathcal{L}(x)$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \quad (1)$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \qquad (1)$$

Lemma 1 *If* $Q \leq x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x)$ *with* $q_1 \leq Q\}$.

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \tag{1}$$

Lemma 1 *If* $Q \leq x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x)$ *with* $q_1 \leq Q\}$.

Then $$N_Q(x) \gg \frac{x}{\log x} \log_2 Q.$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \qquad (1)$$

Lemma 1 *If* $Q \le x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x)$ *with* $q_1 \le Q\}$.

Then $$N_Q(x) \gg \frac{x}{\log x} \log_2 Q.$$

Lemma 2 *If* $Q \le x^{1/4}$ *and*

$$S_Q(x) = \#\left\{(p_0, p_1, q_0, q_1) \text{ s.t. } {q_1 < p_1 \le Q, \quad p_0 p_1 \le x, \quad q_0 q_1 \le x, \atop (p_0 - 1)(p_1 - 1) = (q_0 - 1)(q_1 - 1)}\right\}.$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \tag{1}$$

Lemma 1 *If* $Q \le x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x) \text{ with } q_1 \le Q\}$.

Then $$N_Q(x) \gg \frac{x}{\log x} \log_2 Q.$$

Lemma 2 *If* $Q \le x^{1/4}$ *and*

$$S_Q(x) = \#\left\{(p_0, p_1, q_0, q_1) \text{ s.t. } {q_1 < p_1 \le Q, \quad p_0 p_1 \le x, \quad q_0 q_1 \le x, \atop (p_0-1)(p_1-1) = (q_0-1)(q_1-1)}\right\}.$$

Then $$S_Q(x) \ll \frac{x}{(\log x)^2} (\log Q)^3.$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \tag{1}$$

Lemma 1 *If* $Q \leq x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x)$ *with* $q_1 \leq Q\}$.

Then $$N_Q(x) \gg \frac{x}{\log x} \log_2 Q.$$

Lemma 2 *If* $Q \leq x^{1/4}$ *and*

$$S_Q(x) = \#\left\{(p_0, p_1, q_0, q_1) \ s.t. \ {}^{q_1 < p_1 \leq Q, \quad p_0 p_1 \leq x, \quad q_0 q_1 \leq x,}_{(p_0-1)(p_1-1) = (q_0-1)(q_1-1)}\right\}.$$

Then $$S_Q(x) \ll \frac{x}{(\log x)^2} (\log Q)^3.$$

$$\forall Q \qquad \#\mathcal{L}_2(x) \geq N_Q(x) - 2S_Q(x) \geq c_1 \frac{x}{\log x} \log_2 Q - c_2 \frac{x}{(\log x)^2} (\log Q)^3$$

It is enough to show that

$$\mathcal{L}_2(x) = \{\lambda(n) : n \in \mathcal{P}_2(x)\} \subset \mathcal{L}(x)$$

has sufficiently many elements. i.e.

$$\#\mathcal{L}_2(x) \gg \frac{x}{\log x} \log_2 x. \tag{1}$$

Lemma 1 *If* $Q \le x^{1/4}$ *and* $N_Q(x) = \#\{n = q_0 q_1 \in \mathcal{P}_2(x)$ *with* $q_1 \le Q\}$.

Then $$N_Q(x) \gg \frac{x}{\log x} \log_2 Q.$$

Lemma 2 *If* $Q \le x^{1/4}$ *and*

$$S_Q(x) = \#\left\{(p_0, p_1, q_0, q_1) \text{ s.t. } {}^{q_1 < p_1 \le Q, \quad p_0 p_1 \le x, \quad q_0 q_1 \le x,}_{(p_0-1)(p_1-1) = (q_0-1)(q_1-1)}\right\}.$$

Then $$S_Q(x) \ll \frac{x}{(\log x)^2} (\log Q)^3.$$

$$\forall Q \qquad \#\mathcal{L}_2(x) \ge N_Q(x) - 2S_Q(x) \ge c_1 \frac{x}{\log x} \log_2 Q - c_2 \frac{x}{(\log x)^2} (\log Q)^3$$

Take $Q = \exp\left((\log x)^{1/3}\right)$ and get (1)

Proof of Lemma 1

The contribution to $N_Q(x)$ from primes $q_1 \le Q$, $q_1 \equiv 3 \pmod 4$ is

$$\sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4}} \sum_{d \mid (\frac{q_0-1}{2}, \frac{q_1-1}{2})} \mu(d) = \sum_{d \mid (q_1-1)/2} \mu(d) \sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4 \\ q_0 \equiv 1 \pmod d}} 1.$$

Proof of Lemma 1

The contribution to $N_Q(x)$ from primes $q_1 \le Q$, $q_1 \equiv 3 \pmod 4$ is

$$\sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4}} \sum_{d | (\frac{q_0-1}{2}, \frac{q_1-1}{2})} \mu(d) = \sum_{d|(q_1-1)/2} \mu(d) \sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4 \\ q_0 \equiv 1 \pmod d}} 1.$$

Therefore
$$N_Q(x) = \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} M_q + \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q$$

Proof of Lemma 1

The contribution to $N_Q(x)$ from primes $q_1 \le Q$, $q_1 \equiv 3 \pmod 4$ is

$$\sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4}} \sum_{d | (\frac{q_0-1}{2}, \frac{q_1-1}{2})} \mu(d) = \sum_{d|(q_1-1)/2} \mu(d) \sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4 \\ q_0 \equiv 1 \pmod d}} 1.$$

Therefore $$N_Q(x) = \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} M_q + \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q$$

where

$$M_q = \frac{\mathrm{li}(x/q)}{2} \sum_{d|(q-1)/2} \frac{\mu(d)}{\varphi(d)},$$

$$R_q = \sum_{d|(q-1)/2} \mu(d) \left(\pi(x/q; 4d, a_d) - \frac{\mathrm{li}(x/q)}{2\varphi(d)} \right),$$

Proof of Lemma 1

The contribution to $N_Q(x)$ from primes $q_1 \le Q$, $q_1 \equiv 3 \pmod 4$ is

$$\sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4}} \sum_{d | (\frac{q_0-1}{2}, \frac{q_1-1}{2})} \mu(d) = \sum_{d|(q_1-1)/2} \mu(d) \sum_{\substack{q_0 \le x/q_1 \\ q_0 \equiv 3 \pmod 4 \\ q_0 \equiv 1 \pmod d}} 1.$$

Therefore
$$N_Q(x) = \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} M_q + \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q$$

where

$$M_q = \frac{\mathrm{li}(x/q)}{2} \sum_{d|(q-1)/2} \frac{\mu(d)}{\varphi(d)},$$

$$R_q = \sum_{d|(q-1)/2} \mu(d) \left(\pi(x/q; 4d, a_d) - \frac{\mathrm{li}(x/q)}{2\varphi(d)} \right),$$

and a_d is the residue class modulo $4d$ determined by the classes $3 \pmod 4$ and $1 \pmod d$.

For the sum R_q over $q \leq Q$, Bombieri–Vinogradov (since $Q \leq x^{1/4}$) implies, $\forall A > 1$,

For the sum R_q over $q \le Q$, Bombieri–Vinogradov (since $Q \le x^{1/4}$) implies, $\forall A > 1$,

$$\sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q \ll \sum_{q \le Q} \sum_{d | (q-1)/2} \left| \pi(x/q; 4d, a_d) - \frac{1}{2\varphi(d)} \operatorname{li}(x/q) \right|$$

$$\ll \sum_{q \le Q} \frac{x}{q} (\log x)^{-A} \ll x(\log x)^{1-A},$$

For the sum R_q over $q \le Q$, Bombieri–Vinogradov (since $Q \le x^{1/4}$) implies, $\forall A > 1$,

$$\sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q \ll \sum_{q \le Q} \sum_{d \mid (q-1)/2} \left| \pi(x/q; 4d, a_d) - \frac{1}{2\varphi(d)} \operatorname{li}(x/q) \right|$$

$$\ll \sum_{q \le Q} \frac{x}{q} (\log x)^{-A} \ll x(\log x)^{1-A},$$

For the sum of M_q over q

$$\sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} M_q \gg \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} \operatorname{li}(x/q) \prod_{p \mid (q-1)/2} \left(1 - \frac{1}{p-1}\right)$$

$$\gg \frac{x}{\log x} \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} \frac{\varphi(q-1)}{q(q-1)} \gg \frac{x}{\log x} \log_2 Q$$

For the sum R_q over $q \le Q$, Bombieri–Vinogradov (since $Q \le x^{1/4}$) implies, $\forall A > 1$,

$$\sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} R_q \ll \sum_{q \le Q} \sum_{d|(q-1)/2} \left| \pi(x/q; 4d, a_d) - \frac{1}{2\varphi(d)} \operatorname{li}(x/q) \right|$$

$$\ll \sum_{q \le Q} \frac{x}{q} (\log x)^{-A} \ll x (\log x)^{1-A},$$

For the sum of M_q over q

$$\sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} M_q \gg \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} \operatorname{li}(x/q) \prod_{p|(q-1)/2} \left(1 - \frac{1}{p-1}\right)$$

$$\gg \frac{x}{\log x} \sum_{\substack{q \le Q \\ q \equiv 3 \pmod 4}} \frac{\varphi(q-1)}{q(q-1)} \gg \frac{x}{\log x} \log_2 Q$$

by a classical formula (Stephens) via partial summation. $\square$

Proof of Lemma 2

Fix p_1 and q_1 and estimate S_{p_1,q_1} to $S_Q(x)$ arising.

Proof of Lemma 2

Fix p_1 and q_1 and estimate S_{p_1,q_1} to $S_Q(x)$ arising.

Then

$$S_{p_1,q_1} = \left\{ m \le \frac{x}{[p_1-1, q_1-1]} \text{ s.t. } \begin{array}{c} \text{both } \frac{p_1-1}{(p_1-1,q_1-1)} \cdot m+1 \text{ and} \\ \frac{q_1-1}{(p_1-1,q_1-1)} \cdot m+1 \text{ are prime} \end{array} \right\}.$$

Proof of Lemma 2

Fix p_1 and q_1 and estimate S_{p_1,q_1} to $S_Q(x)$ arising.

Then

$$S_{p_1,q_1} = \left\{ m \le \frac{x}{[p_1-1, q_1-1]} \text{ s.t. } \begin{array}{l} \text{both } \frac{p_1-1}{(p_1-1,q_1-1)}\cdot m+1 \text{ and} \\ \frac{q_1-1}{(p_1-1,q_1-1)}\cdot m+1 \text{ are prime} \end{array} \right\}.$$

Applying the sieve

$$\begin{aligned} S_{p_1,q_1} &\ll \frac{x}{(\log x)^2} \frac{(p_1-1, q_1-1)}{(p_1-1)(q_1-1)} \prod_{p \mid [p_1-1, q_1-1]} (1-1/p)^{-1} \\ &\le \frac{x}{(\log x)^2} \frac{(p_1-1, q_1-1)}{\varphi(p_1-1)\varphi(q_1-1)}. \end{aligned}$$

Proof of Lemma 2

Fix p_1 and q_1 and estimate S_{p_1,q_1} to $S_Q(x)$ arising.

Then

$$S_{p_1,q_1} = \left\{ m \leq \frac{x}{[p_1-1, q_1-1]} \text{ s.t. } \begin{array}{l} \text{both } \frac{p_1-1}{(p_1-1,q_1-1)} \cdot m+1 \text{ and} \\ \frac{q_1-1}{(p_1-1,q_1-1)} \cdot m+1 \text{ are prime} \end{array} \right\}.$$

Applying the sieve

$$\begin{aligned} S_{p_1,q_1} &\ll \frac{x}{(\log x)^2} \frac{(p_1-1, q_1-1)}{(p_1-1)(q_1-1)} \prod_{p \mid [p_1-1, q_1-1]} (1-1/p)^{-1} \\ &\leq \frac{x}{(\log x)^2} \frac{(p_1-1, q_1-1)}{\varphi(p_1-1)\varphi(q_1-1)}. \end{aligned}$$

Sum over $q_1 < p_1 \leq Q$, and enlarge the sum to include all integers up to Q:

Sum over $q_1 < p_1 \le Q$, and enlarge the sum to include all integers up to Q:

$$\begin{aligned}\sum_{q_1<p_1\le Q}\frac{(p_1-1,q_1-1)}{\varphi(p_1-1)\varphi(q_1-1)} &\ll \sum_{k,m\le Q}\frac{(k,m)}{\varphi(k)\varphi(m)}\\ &= \sum_{k,m\le Q}\frac{1}{\varphi(k)\varphi(m)}\sum_{\substack{d\mid k\\ d\mid m}}\varphi(d)\\ &\le \sum_{d\le Q}\frac{1}{\varphi(d)}\sum_{k,m\le Q/d}\frac{1}{\varphi(k)\varphi(m)} \ll (\log Q)^3.\end{aligned}$$

Sum over $q_1 < p_1 \leq Q$, and enlarge the sum to include all integers up to Q:

$$\begin{aligned}
\sum_{q_1 < p_1 \leq Q} \frac{(p_1 - 1, q_1 - 1)}{\varphi(p_1 - 1)\varphi(q_1 - 1)} &\ll \sum_{k,m \leq Q} \frac{(k,m)}{\varphi(k)\varphi(m)} \\
&= \sum_{k,m \leq Q} \frac{1}{\varphi(k)\varphi(m)} \sum_{\substack{d|k \\ d|m}} \varphi(d) \\
&\leq \sum_{d \leq Q} \frac{1}{\varphi(d)} \sum_{k,m \leq Q/d} \frac{1}{\varphi(k)\varphi(m)} \ll (\log Q)^3.
\end{aligned}$$

This completes the proof of the Lemma. □

Sum over $q_1 < p_1 \leq Q$, and enlarge the sum to include all integers up to Q:

$$\begin{aligned}
\sum_{q_1<p_1\leq Q} \frac{(p_1-1,q_1-1)}{\varphi(p_1-1)\varphi(q_1-1)} &\ll \sum_{k,m\leq Q} \frac{(k,m)}{\varphi(k)\varphi(m)} \\
&= \sum_{k,m\leq Q} \frac{1}{\varphi(k)\varphi(m)} \sum_{\substack{d|k\\ d|m}} \varphi(d) \\
&\leq \sum_{d\leq Q} \frac{1}{\varphi(d)} \sum_{k,m\leq Q/d} \frac{1}{\varphi(k)\varphi(m)} \ll (\log Q)^3.
\end{aligned}$$

This completes the proof of the Lemma. $\square$

And the proof of the Theorem too!!

Collision of powers of φ and λ (last topic)

Collision of powers of φ and λ (last topic)

✎ $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$

Collision of powers of φ and λ (last topic)

- ✎ $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- ✎ $\mathcal{A}_k(x) = \{n \le x \;:\; \varphi(n)^{k-1} = \lambda(n)^k\}.$

Collision of powers of φ and λ (last topic)

✎ $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$

✎ $\mathcal{A}_k(x) = \{n \leq x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}$.

✎ For $r \geq s \geq 1$

$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$

Collision of powers of φ and λ (last topic)

- ✎ $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- ✎ $\mathcal{A}_k(x) = \{n \le x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}.$
- ✎ For $r \ge s \ge 1$

$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$

- ✎ Banks, Ford, Luca, FP & Shparlinski (2004)

Collision of powers of φ and λ (last topic)

- $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- $\mathcal{A}_k(x) = \{n \le x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}.$
- For $r \ge s \ge 1$

$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$

- Banks, Ford, Luca, FP & Shparlinski (2004)
  - $\mathcal{A}_k(x) \ge x^{19/27k}$ for $k \ge 2$

Collision of powers of φ and λ (last topic)

- $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- $\mathcal{A}_k(x) = \{n \le x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}$.
- For $r \ge s \ge 1$

$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$

- Banks, Ford, Luca, FP & Shparlinski (2004)
  - $\mathcal{A}_k(x) \ge x^{19/27k}$ for $k \ge 2$
  - Dickson's k–**tuples Conjecture** implies $\#\mathcal{A}_{r,1} = \infty$

Collision of powers of φ and λ (last topic)

- $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- $\mathcal{A}_k(x) = \{n \le x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}$.
- For $r \ge s \ge 1$

$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$

- Banks, Ford, Luca, FP & Shparlinski (2004)
  - $\mathcal{A}_k(x) \ge x^{19/27k}$ for $k \ge 2$
  - Dickson's k–**tuples Conjecture** implies $\#\mathcal{A}_{r,1} = \infty$
  - Schinzel's **Hypothesis H** implies $\#\mathcal{A}_{r,1} = \infty$

Collision of powers of φ and λ (last topic)

- $\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$
- $\mathcal{A}_k(x) = \{n \le x \ : \ \varphi(n)^{k-1} = \lambda(n)^k\}.$
- For $r \ge s \ge 1$
$$\mathcal{A}_{r,s} = \{n \ : \ \varphi(n)^s = \lambda(n)^r\}$$
- Banks, Ford, Luca, FP & Shparlinski (2004)
  - $\mathcal{A}_k(x) \ge x^{19/27k}$ for $k \ge 2$
  - Dickson's k–**tuples Conjecture** implies $\#\mathcal{A}_{r,1} = \infty$
  - Schinzel's **Hypothesis H** implies $\#\mathcal{A}_{r,1} = \infty$
  - The set $\{\log\varphi(n)/\log\lambda(n)\}_{n\ge3}$ is dense in $[1,\infty)$

k–tuples Conjecture *$\forall k \geq 2$, let $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$, with*

- $a_i > 0$
- $\gcd(a_i, b_i) = 1 \ \forall i = 1, \dots, k$
- *$\forall p \leq k$ $\exists n$ such that $p \nmid \prod_{i=1}^{k}(a_i n + b_i)$*

Then $\exists \infty$-many n's such that $p_i = a_i n + b_i$ is prime $\forall i = 1, \dots, k$.

k–tuples Conjecture *$\forall k \geq 2$, let $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{Z}$, with*

- $a_i > 0$
- $\gcd(a_i, b_i) = 1 \ \forall i = 1, \ldots, k$
- *$\forall p \leq k$ $\exists n$ such that $p \nmid \prod_{i=1}^{k}(a_i n + b_i)$*

Then $\exists \infty$-many n's such that $p_i = a_i n + b_i$ is prime $\forall i = 1, \ldots, k$.

Hypothesis H *If $f_1(n), \ldots, f_r(n) \in \mathbb{Z}[x]$*

- *irreducible*
- *positive leading coefficients*
- *$\forall q$ $\exists n$ such that $q \nmid f_1(n) \ldots f_r(n)$.*

Then $f_1(n), \ldots, f_r(n)$ are simultaneously prime for ∞-many n's.