Distribution in coprime residue classes of Euler's totient and the sum of divisors

Akash Singha Roy, University of Georgia
Partially based on joint work with Paul Pollack

PAlmetto Number Theory Series XXXVII

December 2023

Motivating problem: Study the distribution of arithmetic functions among residue classes to integer moduli.

Motivating problem: Study the distribution of arithmetic functions among residue classes to integer moduli.

Definition

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **uniformly distributed** (or **equidistributed**) **modulo** q if, for each integer a,

$$\frac{1}{x}\#\{n \le x : f(n) \equiv a \pmod{q}\} \to \frac{1}{q}, \quad \text{as } x \to \infty.$$

Motivating problem: Study the distribution of arithmetic functions among residue classes to integer moduli.

Definition

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **uniformly distributed** (or **equidistributed**) **modulo** q if, for each integer a,

$$\frac{1}{x}\#\{n \leq x : f(n) \equiv a \pmod{q}\} \to \frac{1}{q}, \quad \text{as } x \to \infty.$$

Example: $f(n) = n$ is equidistributed mod q for every q.

Motivating problem: Study the distribution of arithmetic functions among residue classes to integer moduli.

Definition

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **uniformly distributed** (or **equidistributed**) **modulo** q if, for each integer a,

$$\frac{1}{x}\#\{n \le x : f(n) \equiv a \pmod{q}\} \to \frac{1}{q}, \quad \text{as } x \to \infty.$$

Example: $f(n) = n$ is equidistributed mod q for every q.

Example (Pillai, Delange): $\Omega(n) = \sum_{p^k \| n} k$ is equidistributed mod q for each fixed q.

Motivating problem: Study the distribution of arithmetic functions among residue classes to integer moduli.

Definition

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **uniformly distributed** (or **equidistributed**) **modulo** q if, for each integer a,

$$\frac{1}{x}\#\{n \le x : f(n) \equiv a \pmod{q}\} \to \frac{1}{q}, \quad \text{as } x \to \infty.$$

Example: $f(n) = n$ is equidistributed mod q for every q.

Example (Pillai, Delange): $\Omega(n) = \sum_{p^k \| n} k$ is equidistributed mod q for each fixed q.

But for multiplicative functions, this is **NOT** the correct notion to consider. (Recall: f is multiplicative if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}^+$ such that $\gcd(m, n) = 1$.)

Let $\varphi(n)$ denote Euler's totient; that is, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Fact

For a fixed q, $\varphi(n) \equiv 0 \pmod{q}$ for "almost all" positive integers n:

$$\frac{1}{x}\#\{n \le x : \ \varphi(n) \equiv 0 \pmod{q}\} \to 1 \quad \text{as } x \to \infty.$$

Let $\varphi(n)$ denote Euler's totient; that is, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Fact

For a fixed q, $\varphi(n) \equiv 0 \pmod{q}$ for "almost all" positive integers n:

$$\frac{1}{x}\#\{n \le x : \ \varphi(n) \equiv 0 \pmod{q}\} \to 1 \quad \text{as } x \to \infty.$$

This means that $\varphi(n)$ is not uniformly distributed mod q for **ANY** fixed $q > 1$.

Let $\varphi(n)$ denote Euler's totient; that is, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$.

Fact

For a fixed q, $\varphi(n) \equiv 0 \pmod{q}$ for "almost all" positive integers n:

$$\frac{1}{x}\#\{n \le x : \ \varphi(n) \equiv 0 \pmod{q}\} \to 1 \quad \text{as } x \to \infty.$$

This means that $\varphi(n)$ is not uniformly distributed mod q for **ANY** fixed $q > 1$.

For multiplicative functions $f : \mathbb{N} \to \mathbb{Z}$, it makes sense to study their distribution in the multiplicative group U_q mod q. So now our sample space is $\{n : \gcd(f(n), q) = 1\}$.

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,
2. for each a coprime to q,

$$\frac{\#\{n \le x : f(n) \equiv a \pmod q\}}{\#\{n \le x : \gcd(f(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

as $x \to \infty$.

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,
2. for each a coprime to q,

$$\frac{\#\{n \leq x : f(n) \equiv a \pmod{q}\}}{\#\{n \leq x : \gcd(f(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

as $x \to \infty$.

Example: For which q is $\varphi(n)$ weakly equidistributed mod q?

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,
2. for each a coprime to q,

$$\frac{\#\{n \le x : f(n) \equiv a \pmod{q}\}}{\#\{n \le x : \gcd(f(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

as $x \to \infty$.

Example: For which q is $\varphi(n)$ weakly equidistributed mod q?

Can immediately eliminate some q's:

- $\varphi(n)$ is even for all $n > 2$, so q cannot be even.

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,
2. for each a coprime to q,

$$\frac{\#\{n \le x : f(n) \equiv a \pmod q\}}{\#\{n \le x : \gcd(f(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

   as $x \to \infty$.

Example: For which q is $\varphi(n)$ weakly equidistributed mod q?

Can immediately eliminate some q's:

- $\varphi(n)$ is even for all $n > 2$, so q cannot be even.
- Dence, Pomerance: $\varphi(n)$ is not WUD mod 3.

Definition (Narkiewicz)

Let f be an integer-valued arithmetic function and q be a positive integer. We say f is **weakly uniformly distributed** (or **weakly equidistributed** or **WUD**) **modulo** q if:

1. $\{n : \gcd(f(n), q) = 1\}$ is an infinite set,
2. for each a coprime to q,

$$\frac{\#\{n \le x : f(n) \equiv a \pmod{q}\}}{\#\{n \le x : \gcd(f(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

   as $x \to \infty$.

Example: For which q is $\varphi(n)$ weakly equidistributed mod q?

Can immediately eliminate some q's:

- $\varphi(n)$ is even for all $n > 2$, so q cannot be even.
- Dence, Pomerance: $\varphi(n)$ is not WUD mod 3. Issue is that the numbers $p - 1$, for $p \neq 3$ prime, either fail to be coprime to 3 or are "trapped" in the trivial subgroup of $(\mathbb{Z}/3\mathbb{Z})^\times$.

Thus, we can only hope for weak equidistribution modulo q when $\gcd(q, 6) = 1$.

Thus, we can only hope for weak equidistribution modulo q when $\gcd(q, 6) = 1$.

Theorem (Narkiewicz)

$\varphi(n)$ *is weakly equidistributed modulo* q *iff* $\gcd(q, 6) = 1$.

Thus, we can only hope for weak equidistribution modulo q when $\gcd(q, 6) = 1$.

Theorem (Narkiewicz)

$\varphi(n)$ is weakly equidistributed modulo q iff $\gcd(q, 6) = 1$.

A related function: $\sigma(n) = \sum_{d|n} d$.

Theorem (Śliwa)

$\sigma(n)$ is weakly equidistributed modulo q iff $6 \nmid q$.

Thus, we can only hope for weak equidistribution modulo q when $\gcd(q, 6) = 1$.

Theorem (Narkiewicz)

$\varphi(n)$ is weakly equidistributed modulo q iff $\gcd(q, 6) = 1$.

A related function: $\sigma(n) = \sum_{d|n} d$.

Theorem (Śliwa)

$\sigma(n)$ is weakly equidistributed modulo q iff $6 \nmid q$.

In all of these results, q is fixed. What if q is allowed to vary?

Question. Can we prove (weak) equidistribution theorems when q is allowed to vary with our stopping point x?

Question. Can we prove (weak) equidistribution theorems when q is allowed to vary with our stopping point x?

Model (Siegel-Walfisz Theorem). The primes $\leq x$ are weakly equidistributed mod q, uniformly for $q \leq (\log x)^K$. In other words,

$$\frac{\#\{p \leq x : p \equiv a \pmod{q}\}}{\#\{p \leq x\}} \to \frac{1}{\varphi(q)}$$

as $x \to \infty$, uniformly in $q \leq (\log x)^K$ and $a \in U_q$.

Question. Can we prove (weak) equidistribution theorems when q is allowed to vary with our stopping point x?

Model (Siegel-Walfisz Theorem). The primes $\leq x$ are weakly equidistributed mod q, uniformly for $q \leq (\log x)^K$. In other words,

$$\frac{\#\{p \leq x : p \equiv a \pmod{q}\}}{\#\{p \leq x\}} \to \frac{1}{\varphi(q)}$$

as $x \to \infty$, uniformly in $q \leq (\log x)^K$ and $a \in U_q$.

Question (made precise). Can we establish an analogue of the Siegel-Walfisz Theorem but with primes replaced by values of $\varphi(n)$ or $\sigma(n)$?

Theorem (Pollack, S. R., 2022)

Fix $K > 0$. As $x \to \infty$,

$$\frac{\#\{n \le x : \varphi(n) \equiv a \pmod q\}}{\#\{n \le x : \gcd(\varphi(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

uniformly for $q \le (\log x)^K$ satisfying $\gcd(q, 6) = 1$ and coprime residues a mod q. The same holds true for $\sigma(n)$ in place of $\varphi(n)$.

Theorem (Pollack, S. R., 2022)

Fix $K > 0$. As $x \to \infty$,

$$\frac{\#\{n \le x : \varphi(n) \equiv a \pmod{q}\}}{\#\{n \le x : \gcd(\varphi(n), q) = 1\}} \to \frac{1}{\varphi(q)},$$

uniformly for $q \le (\log x)^K$ satisfying $\gcd(q, 6) = 1$ and coprime residues a mod q. The same holds true for $\sigma(n)$ in place of $\varphi(n)$.

Principle: We don't use characters! We develop an "anatomical" method suggested by work of Banks–Harman–Shparlinski, by splitting off the largest several prime factors of n and exploiting a certain mixing phenomenon in the unit group mod q.

Shortcomings of this result:

- No good effective error term: cannot hope to understand secondary term in asymptotics of distribution.

Shortcomings of this result:

- No good effective error term: cannot hope to understand secondary term in asymptotics of distribution.
- Have not recovered the full result of Śliwa! The result when $\gcd(q, 6) \neq 1$ **cannot** be addressed by this method.

Shortcomings of this result:

- No good effective error term: cannot hope to understand secondary term in asymptotics of distribution.
- Have not recovered the full result of Śliwa! The result when $\gcd(q,6) \neq 1$ **cannot** be addressed by this method.

Theorem (Pollack, S. R., 2023)

Fix $K > 0$ and $\epsilon \in (0,1)$. We have

$$\#\{n \leq x : \varphi(n) \equiv a \pmod{q}\}$$
$$= \frac{1}{\varphi(q)} \#\{n \leq x : \gcd(\varphi(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right),$$

uniformly in moduli $q \leq (\log x)^K$ satisfying $\gcd(q,6) = 1$ and in coprime residue classes a mod q, where $\alpha = \prod_{\ell \mid q} \left(1 - \frac{1}{\ell - 1}\right)$.

Sum of divisors function

Recall: Śliwa shows that $\sigma(n)$ is WUD mod q precisely when $6 \nmid q$.

Sum of divisors function

Recall: Śliwa shows that $\sigma(n)$ is WUD mod q precisely when $6 \nmid q$.

Theorem (S. R., 2023)

Fix $K > 0$ and $\epsilon \in (0,1)$. We have

$$\begin{aligned}&\#\{n \le x : \sigma(n) \equiv a \pmod{q}\}\\ &= \frac{1}{\varphi(q)}\#\{n \le x : \gcd(\sigma(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right),\end{aligned}$$

uniformly in odd moduli $q \le (\log x)^K$ and in coprime residue classes a mod q, where $\alpha = \prod_{\ell \mid q}\left(1 - \frac{1}{\ell-1}\right)$.

Sum of divisors function

Recall: Śliwa shows that $\sigma(n)$ is WUD mod q precisely when $6 \nmid q$.

Theorem (S. R., 2023)

Fix $K > 0$ and $\epsilon \in (0,1)$. We have

$$\begin{aligned} &\#\{n \le x : \sigma(n) \equiv a \pmod q\} \\ &= \frac{1}{\varphi(q)} \#\{n \le x : \gcd(\sigma(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right), \end{aligned}$$

uniformly in odd moduli $q \le (\log x)^K$ and in coprime residue classes a mod q, where $\alpha = \prod_{\ell \mid q}\left(1 - \frac{1}{\ell - 1}\right)$.

Remark: Here and in previous result, the exponent $1/3$ is optimal for technical reasons.

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).
Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).
Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).
Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

  Example: For primes $\ell \ge 5$, the congruence $\sigma(P^2) \equiv 3 \pmod{\ell}$ is satisfied by (primes from) two *distinct* coprime residue classes mod ℓ. So if $q = 2\prod_{5 \le \ell \le Y} \ell$, then the congruence $\sigma(n) \equiv 3 \pmod{q}$ is satisfied by too many n of the form P^2 for some prime P.

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).
Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

  Example: For primes $\ell \ge 5$, the congruence $\sigma(P^2) \equiv 3 \pmod{\ell}$ is satisfied by (primes from) two *distinct* coprime residue classes mod ℓ. So if $q = 2\prod_{5 \le \ell \le Y} \ell$, then the congruence $\sigma(n) \equiv 3 \pmod{q}$ is satisfied by too many n of the form P^2 for some prime P.

Work-around:

- Analyze the behavior of $\sigma(n)$ at squares of primes.

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).

Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

  Example: For primes $\ell \ge 5$, the congruence $\sigma(P^2) \equiv 3 \pmod{\ell}$ is satisfied by (primes from) two *distinct* coprime residue classes mod ℓ. So if $q = 2\prod_{5 \le \ell \le Y} \ell$, then the congruence $\sigma(n) \equiv 3 \pmod{q}$ is satisfied by too many n of the form P^2 for some prime P.

Work-around:

- Analyze the behavior of $\sigma(n)$ at squares of primes.
- Restrict to inputs n having sufficiently many large prime factors (more precisely, sufficiently many prime factors exceeding q). Equidistribution is restored among these inputs.

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).

Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

  Example: For primes $\ell \ge 5$, the congruence $\sigma(P^2) \equiv 3 \pmod{\ell}$ is satisfied by (primes from) two *distinct* coprime residue classes mod ℓ. So if $q = 2\prod_{5 \le \ell \le Y} \ell$, then the congruence $\sigma(n) \equiv 3 \pmod{q}$ is satisfied by too many n of the form P^2 for some prime P.

Work-around:

- Analyze the behavior of $\sigma(n)$ at squares of primes.
- Restrict to inputs n having sufficiently many large prime factors (more precisely, sufficiently many prime factors exceeding q). Equidistribution is restored among these inputs.

  By previous example, need to restrict to inputs with at least four large prime factors.

Remains to consider $\sigma(n)$ mod even q (so $3 \nmid q$).
Two main difficulties:

- Sample space is very sparse: $\#\{n \le x : (\sigma(n), q) = 1\} = O(x^{1/2})$. (Reason/key observation: if $2 \nmid \sigma(n)$, then $n = m^2$ or $2m^2$.)
- $\sigma(n)$ is **not** WUD mod q, uniformly for even moduli $q \le (\log x)^K$. Inputs n without many large prime factors obstruct uniformity!

  Example: For primes $\ell \ge 5$, the congruence $\sigma(P^2) \equiv 3 \pmod{\ell}$ is satisfied by (primes from) two *distinct* coprime residue classes mod ℓ. So if $q = 2\prod_{5 \le \ell \le Y} \ell$, then the congruence $\sigma(n) \equiv 3 \pmod{q}$ is satisfied by too many n of the form P^2 for some prime P.

Work-around:

- Analyze the behavior of $\sigma(n)$ at squares of primes.
- Restrict to inputs n having sufficiently many large prime factors (more precisely, sufficiently many prime factors exceeding q). Equidistribution is restored among these inputs.

  By previous example, need to restrict to inputs with at least four large prime factors. For squarefree q, this suffices!

Let $\widetilde{\alpha} = \prod_{\substack{\ell | q \\ \ell \equiv 1 \pmod 3}} \left(1 - \frac{2}{\ell - 1}\right)$.

Theorem (S. R., 2023)

Fix $K > 0$ and $\epsilon \in (0,1)$. We have

$$\begin{aligned}\#\{n \le x : P_4(n) > q,\ \sigma(n) \equiv a \pmod q\} \\ = \frac{1}{\varphi(q)} \#\{n \le x : P_4(n) > q,\ \gcd(\sigma(n), q) = 1\} \\ + O\left(\frac{x^{1/2}}{\varphi(q)(\log x)^{1 - \widetilde{\alpha}(1/4 + \epsilon)}}\right),\end{aligned}$$

uniformly in **squarefree** *even moduli $q \le (\log x)^K$ not divisible by 3, and in coprime residues a mod q.*

Remark: Again the exponent $1/4$ is optimal.

For general q, a more subtle obstruction: "$P_4(n) > q$" is insufficient!

For general q, a more subtle obstruction: "$P_4(n) > q$" is insufficient! Certain residues mod q are over-represented by n having $P_4(n) > q$, owing to an excess in the number of lifts of solutions to certain polynomial congruences from prime moduli to prime square moduli.

For general q, a more subtle obstruction: "$P_4(n) > q$" is insufficient! Certain residues mod q are over-represented by n having $P_4(n) > q$, owing to an excess in the number of lifts of solutions to certain polynomial congruences from prime moduli to prime square moduli.

Theorem (S. R., 2023)

Fix $K > 0$ and $\epsilon \in (0,1)$. We have

$$\#\{n \le x : P_6(n) > q,\ \sigma(n) \equiv a \pmod q\} = \frac{1}{\varphi(q)}\#\{n \le x : P_6(n) > q,\ \gcd(\sigma(n), q) = 1\} + O\left(\frac{x^{1/2}}{\varphi(q)(\log x)^{1-\widetilde{\alpha}(1/4+\epsilon)}}\right),$$

uniformly in even moduli $q \le (\log x)^K$ not divisible by 3, and in coprime residues a mod q. Here $\widetilde{\alpha} = \prod_{\substack{\ell \mid q \\ \ell \equiv 1 \pmod 3}} \left(1 - \frac{2}{\ell - 1}\right)$.

Some basic principles behind the arguments

Consider the result for $\sigma(n)$ modulo odd q. Let $\alpha = \prod_{\ell | q} \left(1 - \frac{1}{\ell - 1}\right)$.

Want to show: Uniformly in odd $q \leq (\log x)^K$ and in $a \in U_q$,

$$\begin{aligned} &\#\{n \leq x : \sigma(n) \equiv a \pmod{q}\} \\ &= \frac{1}{\varphi(q)} \#\{n \leq x : \gcd(\sigma(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right). \end{aligned}$$

Some basic principles behind the arguments

Consider the result for $\sigma(n)$ modulo odd q. Let $\alpha = \prod_{\ell | q}\left(1 - \frac{1}{\ell - 1}\right)$.

Want to show: Uniformly in odd $q \le (\log x)^K$ and in $a \in U_q$,

$$\begin{aligned}&\#\{n \le x : \sigma(n) \equiv a \pmod{q}\}\\ &= \frac{1}{\varphi(q)}\#\{n \le x : \gcd(\sigma(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right).\end{aligned}$$

Instead of directly applying orthogonality, we first prune our set of inputs n to remove certain inconvenient ones:

Some basic principles behind the arguments

Consider the result for $\sigma(n)$ modulo odd q. Let $\alpha = \prod_{\ell \mid q} \left(1 - \frac{1}{\ell - 1}\right)$.

Want to show: Uniformly in odd $q \le (\log x)^K$ and in $a \in U_q$,

$$\#\{n \le x : \sigma(n) \equiv a \pmod{q}\}$$
$$= \frac{1}{\varphi(q)} \#\{n \le x : \gcd(\sigma(n), q) = 1\} + O\left(\frac{x}{\varphi(q)(\log x)^{1-\alpha(1/3+\epsilon)}}\right).$$

Instead of directly applying orthogonality, we first prune our set of inputs n to remove certain inconvenient ones: For a large parameter y, the surviving inputs n should be expressible in the form $m \cdot r$ where
(i) m is supported on primes $\le y$ (the "y-smooth" part),
(ii) r is supported on primes $> y$ (the "y-rough" part),
(iii) r is squarefree and $\Omega(r) \ge 2$.

Let $\sum_n^*$ denote the sum over these restricted inputs n.

Apply orthogonality on these restricted inputs:

$$\sum\nolimits^*_{\substack{n\le x \\ \sigma(n)\equiv a \pmod q}} 1 = \frac{1}{\varphi(q)} \sum\nolimits^*_{\substack{n\le x \\ (\sigma(n),q)=1}} 1 + \frac{1}{\varphi(q)} \sum_{\chi\ne\chi_0 \bmod q} \overline{\chi}(a) \sum\nolimits^*_{n\le x} \chi(\sigma(n)).$$

Apply orthogonality on these restricted inputs:

$$\sum^*_{\substack{n\le x\\ \sigma(n)\equiv a \pmod q}} 1 = \frac{1}{\varphi(q)}\sum^*_{\substack{n\le x\\ (\sigma(n),q)=1}} 1 + \frac{1}{\varphi(q)}\sum_{\chi\ne\chi_0 \bmod q}\overline{\chi}(a)\sum^*_{n\le x}\chi(\sigma(n)).$$

Suffices to show: $\sum_{\chi\ne\chi_0 \bmod q}\left|\sum^*_{n\le x}\chi(\sigma(n))\right|$ is negligible.

Apply orthogonality on these restricted inputs:

$$\sum\nolimits^*_{\substack{n\le x \\ \sigma(n)\equiv a \pmod q}} 1 = \frac{1}{\varphi(q)} \sum\nolimits^*_{\substack{n\le x \\ (\sigma(n),q)=1}} 1 + \frac{1}{\varphi(q)} \sum_{\chi\neq\chi_0 \bmod q} \overline{\chi}(a) \sum\nolimits^*_{n\le x} \chi(\sigma(n)).$$

Suffices to show: $\sum_{\chi\neq\chi_0 \bmod q} \left|\sum^*_{n\le x} \chi(\sigma(n))\right|$ is negligible.

as before so that

$$\sum\nolimits^*_{n\le x} \chi(\sigma(n)) = \sum_m \chi(\sigma(m)) \sum_r \chi(\sigma(r)).$$

As r is squarefree, the estimation of $\sum_r \chi(\sigma(r))$ essentially reduces to estimating sums $\sum_P \chi(P+1)$ over certain ranges of primes P.

Apply orthogonality on these restricted inputs:

$$\sum\nolimits^*_{\substack{n\le x\\ \sigma(n)\equiv a \pmod q}} 1 = \frac{1}{\varphi(q)}\sum\nolimits^*_{\substack{n\le x\\ (\sigma(n),q)=1}} 1 + \frac{1}{\varphi(q)}\sum_{\chi\ne\chi_0 \bmod q}\overline{\chi}(a)\sum\nolimits^*_{n\le x}\chi(\sigma(n)).$$

Suffices to show: $\sum_{\chi\ne\chi_0 \bmod q}\left|\sum^*_{n\le x}\chi(\sigma(n))\right|$ is negligible.

as before so that

$$\sum\nolimits^*_{n\le x}\chi(\sigma(n)) = \sum_m \chi(\sigma(m))\sum_r \chi(\sigma(r)).$$

As r is squarefree, the estimation of $\sum_r \chi(\sigma(r))$ essentially reduces to estimating sums $\sum_P \chi(P+1)$ over certain ranges of primes P.

Doable via Siegel-Walfisz, showing that $\sum_P \chi(P+1) \approx \rho_\chi \sum_P 1$, where $\rho_\chi = \frac{1}{\varphi(q)}\sum_{\substack{v \bmod q\\ (v(v+1),q)=1}} \chi(v+1)$.

After a lot of suppressed technicalities,

$$\sum\nolimits_{n\leq x}^{*} \chi(\sigma(n)) \ll |\rho_\chi|^2 \frac{x}{(\log x)^{1-|\rho_\chi|-\alpha\epsilon}} + \text{negligible terms} \qquad (1)$$

After a lot of suppressed technicalities,

$$\sum\nolimits_{n\leq x}^{*} \chi(\sigma(n)) \ll |\rho_\chi|^2 \frac{x}{(\log x)^{1-|\rho_\chi|-\alpha\epsilon}} + \text{negligible terms} \qquad (1)$$

We can explicitly evaluate the ρ_χ to see that $|\rho_\chi| \leq \alpha/3$ for all $\chi \neq \chi_0$ mod q **except** for $\chi = \psi$ mod q, where ψ mod q is induced by the nontrivial character mod 3 (occurs if $3 \mid q$).

After a lot of suppressed technicalities,

$$\sum\nolimits_{n\leq x}^{*} \chi(\sigma(n)) \ll |\rho_\chi|^2 \frac{x}{(\log x)^{1-|\rho_\chi|-\alpha\epsilon}} + \text{negligible terms} \qquad (1)$$

We can explicitly evaluate the ρ_χ to see that $|\rho_\chi| \leq \alpha/3$ for all $\chi \neq \chi_0$ mod q **except** for $\chi = \psi$ mod q, where ψ mod q is induced by the nontrivial character mod 3 (occurs if $3 \mid q$). So

$$\sum_{\chi\neq\chi_0,\psi \bmod q} \left|\sum\nolimits_{n\leq x}^{*} \chi(\sigma(n))\right| \ll \frac{x}{(\log x)^{1-\alpha(1/3+\epsilon)}}. \qquad (2)$$

After a lot of suppressed technicalities,

$$\sum\nolimits_{n\le x}^{*} \chi(\sigma(n)) \ll |\rho_\chi|^2 \frac{x}{(\log x)^{1-|\rho_\chi|-\alpha\epsilon}} + \text{negligible terms} \qquad (1)$$

We can explicitly evaluate the ρ_χ to see that $|\rho_\chi| \le \alpha/3$ for all $\chi \ne \chi_0 \bmod q$ **except** for $\chi = \psi \bmod q$, where $\psi \bmod q$ is induced by the nontrivial character mod 3 (occurs if $3 \mid q$). So

$$\sum_{\chi\ne\chi_0,\psi \bmod q} \left|\sum\nolimits_{n\le x}^{*} \chi(\sigma(n))\right| \ll \frac{x}{(\log x)^{1-\alpha(1/3+\epsilon)}}. \qquad (2)$$

Still need to deal with $\psi \bmod q$ (if $3 \mid q$). But $|\rho_\psi| = \alpha$, so applying (1) gives a worse bound than the main term!

The key is that $\rho_\psi = -\alpha$ which suggests additional cancellation.

The key is that $\rho_\psi = -\alpha$ which suggests additional cancellation. To detect this, we again write $n = m \cdot r$ and do some fancier footwork to obtain

$$\sum\nolimits^*_{n \le x} \psi(\sigma(n)) \approx \sum_{\substack{m \le x \\ P(m) \le y}} \psi(\sigma(m)) \sum_{r \le x/m} \mathbb{1}_{P^-(r) > y} \; \rho_\psi^{\Omega(r)}.$$

(Recall: $\rho_\psi^{\Omega(r)}$ is expected as $\sum_P \psi(P+1) \approx \rho_\psi \sum_P 1$.)

The key is that $\rho_\psi = -\alpha$ which suggests additional cancellation. To detect this, we again write $n = m \cdot r$ and do some fancier footwork to obtain

$$\sum\nolimits_{n \le x}^{*} \psi(\sigma(n)) \approx \sum_{\substack{m \le x \\ P(m) \le y}} \psi(\sigma(m)) \sum_{r \le x/m} \mathbb{1}_{P^{-}(r) > y}\ \rho_\psi^{\Omega(r)}.$$

(Recall: $\rho_\psi^{\Omega(r)}$ is expected as $\sum_P \psi(P+1) \approx \rho_\psi \sum_P 1$.)

The inner sum can be estimated by powerful multiplicative machinery (precisely: the Landau–Selberg–Delange method)!

The key is that $\rho_\psi = -\alpha$ which suggests additional cancellation. To detect this, we again write $n = m \cdot r$ and do some fancier footwork to obtain

$$\sum\nolimits^{*}_{n\le x} \psi(\sigma(n)) \approx \sum_{\substack{m\le x\\ P(m)\le y}} \psi(\sigma(m)) \sum_{r\le x/m} \mathbb{1}_{P^-(r)>y}\, \rho_\psi^{\Omega(r)}.$$

(Recall: $\rho_\psi^{\Omega(r)}$ is expected as $\sum_P \psi(P+1) \approx \rho_\psi \sum_P 1$.)

The inner sum can be estimated by powerful multiplicative machinery (precisely: the Landau–Selberg–Delange method)! We get

$$\sum\nolimits^{*}_{n\le x} \psi(\sigma(n)) \ll \frac{x}{(\log x)^{1-\alpha\epsilon}}.$$

The key is that $\rho_\psi = -\alpha$ which suggests additional cancellation. To detect this, we again write $n = m \cdot r$ and do some fancier footwork to obtain

$$\sum\nolimits_{n \le x}^{*} \psi(\sigma(n)) \approx \sum_{\substack{m \le x \\ P(m) \le y}} \psi(\sigma(m)) \sum_{r \le x/m} \mathbb{1}_{P^-(r) > y} \; \rho_\psi^{\Omega(r)}.$$

(Recall: $\rho_\psi^{\Omega(r)}$ is expected as $\sum_P \psi(P+1) \approx \rho_\psi \sum_P 1$.)

The inner sum can be estimated by powerful multiplicative machinery (precisely: the Landau–Selberg–Delange method)! We get

$$\sum\nolimits_{n \le x}^{*} \psi(\sigma(n)) \ll \frac{x}{(\log x)^{1-\alpha\epsilon}}.$$

Combining this with (2), our proof is complete.

The two kinds of arguments above yield general bounds on multiplicative functions taking values in the unit disk.

Theorem

Let $f\colon \mathbb{N} \to \mathbb{U}$ be a multiplicative function, and $x, y, z, M \in \mathbb{R}^+$ satisfy $M \geq 1$, $1 < z < x$ and $e^{11/2} \leq y \leq z^{1/(18 \log\log z)^2}$. Suppose there exists $\varrho \in \mathbb{U}$ such that

$$\sum_{y<p\leq Y} f(p) = \varrho(\pi(Y) - \pi(y)) + O(MY\mathcal{E}(y)),$$

for all $Y \geq y$, where $\mathcal{E}\colon \mathbb{R}^+ \to \mathbb{R}^+$ is decreasing and $\lim_{X\to\infty} \mathcal{E}(X) = 0$. Then

$$\sum_{n\leq x} f(n) \ll \frac{|\varrho| x}{\log z}\left(\frac{\log x}{\log y}\right)^{|\varrho|} \exp\left(\sum_{p\leq y}\frac{|f(p)|}{p}\right) + \Psi(x,z) + Mx(\log x)^2\left(\mathcal{E}(y) + \frac{1}{y}\right),$$

$$\sum_{n\leq x} f(n) \ll \frac{|\varrho| x}{\log z}\left(\frac{\log z}{\log y}\right)^{\mathrm{Re}(\varrho)} \exp\left(\sum_{p\leq y}\frac{|f(p)|}{p}\right)$$

$$+ \frac{x(\log y)^{1+|\varrho|}}{(\log z)^{2-\mathrm{Re}(\varrho)}} \exp\left(\sum_{p\leq y}\frac{|f(p)|}{p}\right) + \Psi(x,z) + Mx(\log x)^2\left(\mathcal{E}(y) + \frac{1}{y}\right).$$

Thank you for your attention!