Variant of a theorem of Erdős on the sum-of-proper-divisors function

Heesung Yang
Joint work with Carl Pomerance

Dalhousie University

25 November 2019

Outline

How to study arithmetical functions?

How to study arithmetical functions?

- Study the distribution of the range of f

HOW TO STUDY ARITHMETICAL FUNCTIONS?

- Study the distribution of the range of f
- Or, study the "non-range" of f, i.e., which integers are *not* in the range of f

How to study arithmetical functions?

- Study the distribution of the range of f
- Or, study the "non-range" of f, i.e., which integers are *not* in the range of f
- Specifically, we are interested when $f(n) = s^*(n) := \sigma^*(n) - n$ which we will define shortly.

How to study arithmetical functions?

- Study the distribution of the range of f
- Or, study the "non-range" of f, i.e., which integers are *not* in the range of f
- Specifically, we are interested when $f(n) = s^*(n) := \sigma^*(n) - n$ which we will define shortly.

Quick definitions

Definition

Any function $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic* or *arithmetical* function. Additionally, if $f(mn) = f(m)f(n)$ for all $(m,n) = 1$, then f is *multiplicative*.

Definition

An integer d is called a *unitary divisor of n* if $d \mid n$ and $(d, n/d) = 1$. We write $d \parallel n$ if d is a unitary divisor of n.

Definition

$\sigma(n)$ denotes the sum of all the divisors of n. $\sigma^*(n)$ denotes the sum of all the unitary divisors of n. Note that both $\sigma(n)$ and $\sigma^*(n)$ are multiplicative.

Quick definitions

Definition

Any function $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic* or *arithmetical* function. Additionally, if $f(mn) = f(m)f(n)$ for all $(m, n) = 1$, then f is *multiplicative*.

Definition

An integer d is called a *unitary divisor of* n if $d \mid n$ and $(d, n/d) = 1$. We write $d \parallel n$ if d is a unitary divisor of n.

Definition

$\sigma(n)$ denotes the sum of all the divisors of n. $\sigma^*(n)$ denotes the sum of all the unitary divisors of n. Note that both $\sigma(n)$ and $\sigma^*(n)$ are multiplicative.

Quick definitions

Definition

Any function $f : \mathbb{N} \to \mathbb{C}$ is called an *arithmetic* or *arithmetical* function. Additionally, if $f(mn) = f(m)f(n)$ for all $(m, n) = 1$, then f is *multiplicative*.

Definition

An integer d is called a *unitary divisor of* n if $d \mid n$ and $(d, n/d) = 1$. We write $d \parallel n$ if d is a unitary divisor of n.

Definition

$\sigma(n)$ denotes the sum of all the divisors of n. $\sigma^*(n)$ denotes the sum of all the unitary divisors of n. Note that both $\sigma(n)$ and $\sigma^*(n)$ are multiplicative.

Quick definitions

- $\sigma(n)$: Sum of divisors of n ($\sigma(p^a) = 1 + p + \cdots + p^a$)
- $s(n)$: Sum of proper divisors of n (= $\sigma(n) - n$)
- $\sigma^*(n)$: Sum of unitary divisors of n ($\sigma^*(p^a) = 1 + p^a$)
- $s^*(n)$: Sum of proper unitary divisors of n (= $\sigma^*(n) - n$)
- Quick comment: if n is square-free, then $\sigma(n) = \sigma^*(n)$ and $s(n) = s^*(n)$.
- We will let $U := \mathbb{N} \setminus s(\mathbb{N})$ and $U^* := \mathbb{N} \setminus s^*(\mathbb{N})$ throughout this talk.

Definition

If $n \in U$, then n is said to be a *nonaliquot number*. We shall call n a *unitary nonaliquot number* if $n \in U^*$.

Detour

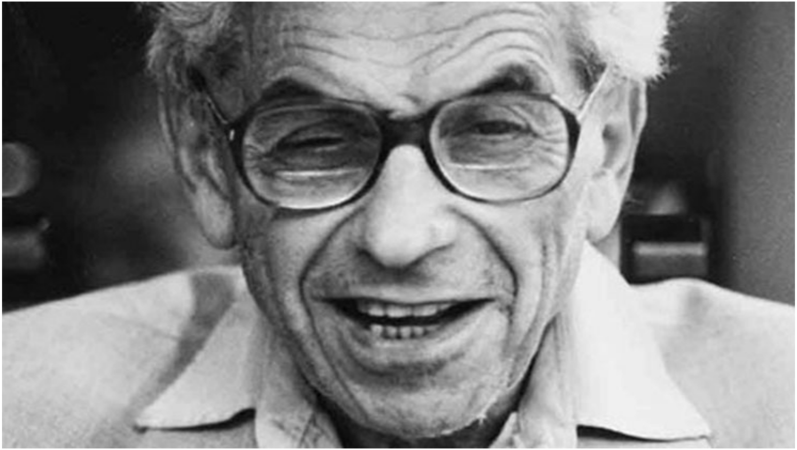
Conjecture (Goldbach)

Every even number greater than or equal to 8 can be written as a sum of two distinct primes.

According to this, we can deduce that $s(pq) = s^*(pq) = p + q + 1$, where p and q are distinct odd primes, will cover all the odd integers ≥ 9.

- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.
- It will be more exciting to focus on even numbers as far as $\mathbb{N} \setminus s^*(\mathbb{N})$ is concerned.

Erdős and nonaliquot numbers



Erdős Pál (1913 – 1996)

Erdős and nonaliquot numbers

Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$

Dem Andenken von Waclaw Sierpiński gewidmet

Ich traf Professor Sierpiński zuerst im August 1955 bei einer mathematischen Tagung in Prag. Sierpiński war damals schon mehr an der elementaren Zahlentheorie interessiert als an der Mengenlehre. Wir diskutierten über die Eulersche φ-Funktion und vermuteten, dass für unendlich viele m die Gleichung

$$n - \varphi(n) = m \tag{1}$$

unlösbar ist. Diese Vermutung ist noch immer unentschieden, ich werde aber zeigen, dass für unendlich viele Werte von m

$$\sigma(n) - n = m \tag{2}$$

unlösbar ist. Wir beweisen einen etwas stärkeren

Satz I. Die untere Dichte[1]) der Zahlen m, für welche (2) unlösbar ist, ist positiv.

Bevor wir unseren Satz beweisen, wollen wir einige Besonderheiten unserer Vermutung besprechen. Es sei $n = pq$, wo p und q verschiedene ungerade Primzahlen sind. Offenbar ist

$$n - \varphi(n) = p + q - 1 \,.$$

[1]) Ist $a_1 < a_2 < a_3 < \dots$ eine unendliche Folge natürlicher Zahlen und $A(n)$ die Anzahl der $a_i \leq n$, so ist für $n \to \infty$ $\underline{d} = \underline{\lim}\, A(n)/n$ die untere und $\overline{d} = \overline{\lim}\, A(n)/n$ die obere Dichte der Folge. Ist $\underline{d} = \overline{d} = d$, so wird d die (asymptotische) Dichte der Folge genannt.

Erdős and nonaliquot numbers

Theorem (Erdős, 1973)

There is a positive proportion of nonaliquot numbers.

Proof (Sketch).

- Let P_k be the product of first k primes. We will show that positive proportion of integers that are 0 mod P_k must be nonaliquot numbers.
- Assume $s(n) \le x$ and $s(n) \equiv 0 \pmod{P_k}$.
- If n is odd or $2 \mid n$ but $n \not\equiv 0 \pmod{P_k}$, then the density of n satisfying the two conditions is 0.
- So we may assume $P_k \mid n$ in order for us to have $P_k \mid s(n)$.

Erdős and nonaliquot numbers

Theorem (Erdős, 1973)

There is a positive proportion of nonaliquot numbers.

Proof (Sketch).

Note that we have $\sigma(n) \geq n \prod(1 + p_i^{-1})$, so for any $\varepsilon > 0$ we can choose sufficiently large k such that

$$\sigma(n) \geq n \prod_{i=1}^{k} \left(1 + \frac{1}{p_i}\right) > n \left(1 + \frac{1}{\varepsilon}\right).$$

Observe we can choose such k since the sum of reciprocals of the primes diverges. Thus, the number of n satisfying the desired conditions is strictly less than $\varepsilon x / P_k$ for all sufficiently large x.

Erdős and nonaliquot numbers

Theorem (Erdős, 1973)

There is a positive proportion of nonaliquot numbers.

Proof (Sketch).

So if $0 < \varepsilon < 1$, and k and x are appropriately chosen, the upper density of aliquot numbers that are multiple of P_k is at most ε/P_k. But since the density of numbers that are multiple of P_k is $1/P_k$, the lower density of nonaliquot numbers divisible by P_k must be positive. □

te Riele and unitary nonaliquot numbers

Herman te Riele (b. 1947)

te Riele and unitary nonaliquot numbers

- In his doctoral thesis, he tried to tackle unitary nonaliquot numbers
- Problem: integers of the form $2^w p$ $(w \geq 1, p$ an odd prime)
- Problematic, as there are "too many" $2^w p$'s with $s^*(2^w p) \leq x$ for any x. Let's examine further what this means.
- If $s^*(2^w p) = 2^w + p + 1 \leq x$, then $2^w \leq x$ and $p \leq x$, so there are $O(\log x)$ choices for 2^w and $O(x/\log x)$ choices for p thanks to the prime number theorem. Thus there are $O(x)$ numbers of the form $2^w p$ to consider, which doesn't help us in finding the density of U^*.

te Riele and unitary nonaliquot numbers

Conjecture (de Polignac, 1849)

Every odd number greater than 1 can be written in the form $2^k + p$, where $k \in \mathbb{Z}_+$ and p an odd prime (or $p = 1$).

- te Riele's astute observation: if de Polignac's conjecture were true, then all even numbers > 2 are in $s^*(\mathbb{N})$. So the density of U^* would be 0, and we would be done.
- The conjecture proved to be false, (independently) by Erdős and van der Corput. In fact, Erdős used the theory of covering congruences to disprove this conjecture. This gave us the starting point.

te Riele and unitary nonaliquot numbers

Conjecture (de Polignac, 1849)

Every odd number greater than 1 can be written in the form $2^k + p$, where $k \in \mathbb{Z}_+$ and p an odd prime (or $p = 1$).

- te Riele's astute observation: if de Polignac's conjecture were true, then all even numbers > 2 are in $s^*(\mathbb{N})$. So the density of U^* would be 0, and we would be done.
- The conjecture proved to be false, (independently) by Erdős and van der Corput. In fact, Erdős used the theory of covering congruences to disprove this conjecture. This gave us the starting point.

Main result

Main result

Theorem (Pomerance-Y., 2012)

The lower density of the set U^* is positive, and the upper density of U^* is smaller than $\frac{1}{2}$.

Main result

Theorem (Pomerance-Y., 2012)

The lower density of the set U^* is positive, and the upper density of U^* is smaller than $\frac{1}{2}$.

Remark

It is not known if the set U has upper density smaller than $\frac{1}{2}$.

Outline of our strategy

1. The set of positive lower density that we identify will be a subset of the integers that are 2 mod 4.

Outline of our strategy

1. The set of positive lower density that we identify will be a subset of the integers that are 2 mod 4.
2. First, we will get rid of the following three cases that are not too interesting.
   - Case I: $n = 2^w p^a$ $(a > 1)$
   - Case II: $4 \mid n$, n has more than one odd prime factor
   - Case III: n is odd

Outline of our strategy

1. The set of positive lower density that we identify will be a subset of the integers that are 2 mod 4.
2. First, we will get rid of the following three cases that are not too interesting.
   - Case I: $n = 2^w p^a$ $(a > 1)$
   - Case II: $4 \mid n$, n has more than one odd prime factor
   - Case III: n is odd
3. Now, tackle the remaining case:
   - First, we shall derive an infinite arithmetic progression that is totally missed by the numbers of the form $s^*(2^w p)$ using covering congruences.
   - Now show that the constructed residue class has a positive proportion of integers not of the form $s^*(n)$ for any $n \equiv 2 \pmod 4$.

Uninteresting cases

Lemma

Suppose that $n > 1$ satisfies one of the following:

1. *n is odd*
2. *n is divisible by 4 and also by at least two distinct odd primes.*

Then $s^*(n) \not\equiv 2 \pmod 4$.

Proof.

Suppose n is odd, and that $p^a \parallel n$. Then p is odd, and $\sigma^*(p^a) = 1 + p^a$, which is even. Thus $\sigma^*(n)$ is even, so $s^*(n)$ is odd. Now suppose n is divisible by 4 and by at least two distinct odd primes (say p and q). Then $4 \mid \sigma^*(p)\sigma^*(q) \mid \sigma^*(n)$, so $4 \mid s^*(n)$ as well. The claim follows. □

Uninteresting cases

Lemma

The set of integers of the form $s^*(2^w p^a)$ where p is an odd prime and $a \geq 2$ has asymptotic density 0.

Proof.

Suppose $s^*(2^w p^a) \leq x$. Note $s^*(2^w p^a) = 1 + 2^w + p^a$, so

$$2^w \leq x \text{ and } p^a \leq x.$$

So there are $O(\log x)$ choices for 2^w. As for p^a, since $a \geq 2$, there are $O(\sqrt{x}/\log x)$ choices. In total, there are $O(\sqrt{x})$ numbers satisfying $s^*(2^w p^a) \leq x$, from which the claim follows. □

The $n = 2^w p$ case

Every $w \in \mathbb{Z}$ satisfies at least one of the following six congruences:

$$\begin{aligned} w &\equiv 1 \pmod{2}, & w &\equiv 1 \pmod{3} \\ w &\equiv 2 \pmod{4}, & w &\equiv 4 \pmod{8} \\ w &\equiv 8 \pmod{12}, & w &\equiv 0 \pmod{24}. \end{aligned}$$

Now, for each modulus $m \in \{2, 3, 4, 8, 12, 24\}$, we find a prime q so that $2^m \equiv 1 \pmod{q}$. For $\ell := s^*(2^w p) = 1 + 2^w + p$ we have:

m	q	$2^w \bmod q$	$\ell \bmod q$	Conclusion
2	3	2	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{3}$ or $p = 3$
3	7	2	$\ell \equiv 3 + p$	$\ell \not\equiv 3 \pmod{7}$ or $p = 7$
4	5	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{5}$ or $p = 5$
8	17	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{17}$ or $p = 17$
12	13	-4	$\ell \equiv -3 + p$	$\ell \not\equiv -3 \pmod{13}$ or $p = 13$
24	241	1	$\ell \equiv 2 + p$	$\ell \not\equiv 2 \pmod{241}$ or $p = 241$

The $n = 2^w p$ case

Every $w \in \mathbb{Z}$ satisfies at least one of the following six congruences:

$$\begin{aligned} w &\equiv 1 \pmod{2}, & w &\equiv 1 \pmod{3} \\ w &\equiv 2 \pmod{4}, & w &\equiv 4 \pmod{8} \\ w &\equiv 8 \pmod{12}, & w &\equiv 0 \pmod{24}. \end{aligned}$$

Now, for each modulus $m \in \{2, 3, 4, 8, 12, 24\}$, we find a prime q so that $2^m \equiv 1 \pmod{q}$. For $\ell := s^*(2^w p) = 1 + 2^w + p$ we have:

m	q	$2^w \bmod q$	$\ell \bmod q$	Conclusion
2	3	2	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{3}$ or $p = 3$
3	7	2	$\ell \equiv 3 + p$	$\ell \not\equiv 3 \pmod{7}$ or $p = 7$
4	5	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{5}$ or $p = 5$
8	17	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{17}$ or $p = 17$
12	13	-4	$\ell \equiv -3 + p$	$\ell \not\equiv -3 \pmod{13}$ or $p = 13$
24	241	1	$\ell \equiv 2 + p$	$\ell \not\equiv 2 \pmod{241}$ or $p = 241$

The $n = 2^w p$ case

Every $w \in \mathbb{Z}$ satisfies at least one of the following six congruences:

$$w \equiv 1 \pmod 2, \quad w \equiv 1 \pmod 3$$
$$w \equiv 2 \pmod 4, \quad w \equiv 4 \pmod 8$$
$$w \equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}.$$

Now, for each modulus $m \in \{2, 3, 4, 8, 12, 24\}$, we find a prime q so that $2^m \equiv 1 \pmod q$. For $\ell := s^*(2^w p) = 1 + 2^w + p$ we have:

m	q	$2^w \bmod q$	$\ell \bmod q$	Conclusion
2	3	2	$\ell \equiv p$	$\ell \not\equiv 0 \pmod 3$ or $p = 3$
3	7	2	$\ell \equiv 3 + p$	$\ell \not\equiv 3 \pmod 7$ or $p = 7$
4	5	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod 5$ or $p = 5$
8	17	-1	$\ell \equiv p$	$\ell \not\equiv 0 \pmod{17}$ or $p = 17$
12	13	-4	$\ell \equiv -3 + p$	$\ell \not\equiv -3 \pmod{13}$ or $p = 13$
24	241	1	$\ell \equiv 2 + p$	$\ell \not\equiv 2 \pmod{241}$ or $p = 241$

THE $n = 2^w p$ CASE

Applying the Chinese remainder theorem to the following six congruences give us which the residue class whose member cannot be of the form $s^*(2^w p)$:

$$\ell \equiv 0 \pmod 3, \quad \ell \equiv 3 \pmod 7$$
$$\ell \equiv 0 \pmod 5, \quad \ell \equiv 0 \pmod{17}$$
$$\ell \equiv -3 \pmod{13}, \quad \ell \equiv 2 \pmod{241}.$$

This gives us $\ell \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. Let $c = -1518780$ and $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 = 5592405$. We established the following lemma:

LEMMA

Let $n = 2^w p$, with $w \geq 1$ and p an odd prime. Then there exist c and odd d such that $s^*(n) \not\equiv c \pmod d$ for any w and p.

The $n = 2^w p$ case

Applying the Chinese remainder theorem to the following six congruences give us which the residue class whose member cannot be of the form $s^*(2^w p)$:

$$\ell \equiv 0 \pmod 3, \quad \ell \equiv 3 \pmod 7$$
$$\ell \equiv 0 \pmod 5, \quad \ell \equiv 0 \pmod{17}$$
$$\ell \equiv -3 \pmod{13}, \quad \ell \equiv 2 \pmod{241}.$$

This gives us $\ell \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. Let $c = -1518780$ and $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 = 5592405$. We established the following lemma:

Lemma

Let $n = 2^w p$, with $w \geq 1$ and p an odd prime. Then there exist c and odd d such that $s^*(n) \not\equiv c \pmod d$ for any w and p.

The $n = 2^w p$ case

Applying the Chinese remainder theorem to the following six congruences give us which the residue class whose member cannot be of the form $s^*(2^w p)$:

$$\ell \equiv 0 \pmod 3, \quad \ell \equiv 3 \pmod 7$$
$$\ell \equiv 0 \pmod 5, \quad \ell \equiv 0 \pmod{17}$$
$$\ell \equiv -3 \pmod{13}, \quad \ell \equiv 2 \pmod{241}.$$

This gives us $\ell \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. Let $c = -1518780$ and $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 = 5592405$. We established the following lemma:

Lemma

Let $n = 2^w p$, with $w \geq 1$ and p an odd prime. Then there exist c and odd d such that $s^*(n) \not\equiv c \pmod d$ for any w and p.

THE $n = 2^w p$ CASE

Applying the Chinese remainder theorem to the following six congruences give us which the residue class whose member cannot be of the form $s^*(2^w p)$:

$$\begin{aligned} \ell &\equiv 0 \pmod 3, & \ell &\equiv 3 \pmod 7 \\ \ell &\equiv 0 \pmod 5, & \ell &\equiv 0 \pmod{17} \\ \ell &\equiv -3 \pmod{13}, & \ell &\equiv 2 \pmod{241}. \end{aligned}$$

This gives us $\ell \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. Let $c = -1518780$ and $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241 = 5592405$. We established the following lemma:

LEMMA

Let $n = 2^w p$, with $w \geq 1$ and p an odd prime. Then there exist c and odd d such that $s^*(n) \not\equiv c \pmod d$ for any w and p.

PROOF OF THE MAIN THEOREM

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q, since $\operatorname{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

Proof of the main theorem

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q, since $\operatorname{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

Proof of the main theorem

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q, since $\mathrm{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

PROOF OF THE MAIN THEOREM

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q, since $\text{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

Proof of the main theorem

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q, since $\mathrm{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

Proof of the main theorem

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and p an odd prime.
- Recall that we are interested in finding a subset of integers 2 mod 4 that are not in the range of $s^*(n)$.
- Let $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and have Q as its unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both $c \bmod d$ and $0 \bmod Q$, since $\operatorname{lcm}(d, Q) = dQ/255$. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (fixing the three red-coloured congruences so that c remains divisible by 255). Thus, we can compute the lower density for an arbitrary residue class satisfying the desirable conditions, and multiply it by $128 \cdot 6$.

Proof of the main theorem

Suppose that $r \pmod{2dQ}$ is one of the 128 congruence classes we are interested in. We shall consider integers n satisfying the following:

$$s^*(n) \le x$$
$$s^*(n) \equiv r \pmod{2dQ}.$$

As Cases I, II, and III show, we may assume that $n \equiv 2 \pmod 4$ or n is of the form $2^w p$ where $w \ge 2$. But $s^*(2^w p) \not\equiv c \pmod d$, so we may assume $n \equiv 2 \pmod 4$.

Since 2 is a unitary divisor of n, it follows $n < 2x$. A theorem by E. J. Scourfield implies that almost all n's have $2dQ \mid \sigma^*(n)$. Thus, we may assume $n \equiv -r \pmod{2dQ}$, so Q is a unitary divisor of n.

Proof of the main theorem

Suppose that $r \pmod{2dQ}$ is one of the 128 congruence classes we are interested in. We shall consider integers n satisfying the following:

$$s^*(n) \leq x$$
$$s^*(n) \equiv r \pmod{2dQ}.$$

As Cases I, II, and III show, we may assume that $n \equiv 2 \pmod 4$ or n is of the form $2^w p$ where $w \geq 2$. But $s^*(2^w p) \not\equiv c \pmod d$, so we may assume $n \equiv 2 \pmod 4$.

Since 2 is a unitary divisor of n, it follows $n < 2x$. A theorem by E. J. Scourfield implies that almost all n's have $2dQ \mid \sigma^*(n)$. Thus, we may assume $n \equiv -r \pmod{2dQ}$, so Q is a unitary divisor of n.

Proof of the main theorem

Suppose that $r \pmod{2dQ}$ is one of the 128 congruence classes we are interested in. We shall consider integers n satisfying the following:

$$s^*(n) \leq x$$
$$s^*(n) \equiv r \pmod{2dQ}.$$

As Cases I, II, and III show, we may assume that $n \equiv 2 \pmod 4$ or n is of the form $2^w p$ where $w \geq 2$. But $s^*(2^w p) \not\equiv c \pmod d$, so we may assume $n \equiv 2 \pmod 4$.

Since 2 is a unitary divisor of n, it follows $n < 2x$. A theorem by E. J. Scourfield implies that almost all n's have $2dQ \mid \sigma^*(n)$. Thus, we may assume $n \equiv -r \pmod{2dQ}$, so Q is a unitary divisor of n.

Proof of the main theorem

Suppose that $r \pmod{2dQ}$ is one of the 128 congruence classes we are interested in. We shall consider integers n satisfying the following:

$$s^*(n) \leq x$$
$$s^*(n) \equiv r \pmod{2dQ}.$$

As Cases I, II, and III show, we may assume that $n \equiv 2 \pmod 4$ or n is of the form $2^w p$ where $w \geq 2$. But $s^*(2^w p) \not\equiv c \pmod d$, so we may assume $n \equiv 2 \pmod 4$.
Since 2 is a unitary divisor of n, it follows $n < 2x$. A theorem by E. J. Scourfield implies that almost all n's have $2dQ \mid \sigma^*(n)$. Thus, we may assume $n \equiv -r \pmod{2dQ}$, so Q is a unitary divisor of n.

Proof of the main theorem

It follows that we have

$$s^*(n) = \sigma^*(n) - n = \sigma^*(Q)\sigma^*(n/Q) - n \geq (s^*(Q)/Q)n.$$

It follows that $n \leq (Q/s^*(Q))x$, so the number of n's we are looking for is

$$\frac{Q}{s^*(Q)} \cdot \frac{x}{2dQ} + o(x) \text{ as } x \to \infty.$$

This shows that the lower density of U^* is at least $(1 - Q/s^*(Q))/(2dQ)$, within $r \pmod{2dQ}$. There are 128 possible r's. Also, fixing $1 \pmod 2, 2 \pmod 4, 4 \pmod 8$, we can pick six different choices for the three remaining congruence classes. In conclusion, the lower density of U^* within $c \pmod d$ is

$$\left(1 - \frac{Q}{s^*(Q)}\right)\frac{384}{dQ}.$$

Proof of the main theorem

It follows that we have

$$s^*(n) = \sigma^*(n) - n = \sigma^*(Q)\sigma^*(n/Q) - n \geq (s^*(Q)/Q)n.$$

It follows that $n \leq (Q/s^*(Q))x$, so the number of n's we are looking for is

$$\frac{Q}{s^*(Q)} \cdot \frac{x}{2dQ} + o(x) \text{ as } x \to \infty.$$

This shows that the lower density of U^* is at least $(1 - Q/s^*(Q))/(2dQ)$, within $r \pmod{2dQ}$. There are 128 possible r's. Also, fixing $1 \pmod 2, 2 \pmod 4, 4 \pmod 8$, we can pick six different choices for the three remaining congruence classes. In conclusion, the lower density of U^* within $c \pmod d$ is

$$\left(1 - \frac{Q}{s^*(Q)}\right)\frac{384}{dQ}.$$

Proof of the main theorem

It follows that we have

$$s^*(n) = \sigma^*(n) - n = \sigma^*(Q)\sigma^*(n/Q) - n \geq (s^*(Q)/Q)n.$$

It follows that $n \leq (Q/s^*(Q))x$, so the number of n's we are looking for is

$$\frac{Q}{s^*(Q)} \cdot \frac{x}{2dQ} + o(x) \text{ as } x \to \infty.$$

This shows that the lower density of U^* is at least $(1 - Q/s^*(Q))/(2dQ)$, within $r \pmod{2dQ}$. There are 128 possible r's. Also, fixing $1 \pmod 2, 2 \pmod 4, 4 \pmod 8$, we can pick six different choices for the three remaining congruence classes. In conclusion, the lower density of U^* within $c \pmod d$ is

$$\left(1 - \frac{Q}{s^*(Q)}\right)\frac{384}{dQ}.$$

Statement of the theorem

Theorem (Pomerance-Y., 2012)

Let

$$Q := 2 \cdot 3^{\alpha} \cdot 5^{\beta} \cdot 17^{\gamma},$$

where α, β, γ *are positive integers. If* $s^*(Q)/Q > 1$ *then the set of the numbers in* U^* *which have* Q *as a unitary divisor has lower density at least*

$$\left(1 - \frac{Q}{s^*(Q)}\right)\frac{384}{dQ},$$

where $d = 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241.$

Quick remarks

Remark

Let $Q = 2 \cdot 3 \cdot 5 \cdot 17$. Then this theorem implies that the lower density of U^* must be at least

$$\left(1 - \frac{85}{131}\right) \frac{384}{5592405 \cdot 510} > 4.727 \cdot 10^{-8}.$$

Remark

As for the upper density of U^*, consider numbers of the form $s^*(2^w p) = 2^w + p + 1$. The lower density of numbers of the form $s^*(2^w p)$ is equal to the lower density of number of the form $2^w + p$. Habsieger and Roblot (and Lü and Pintz, each independently) showed that the lower density is at least 0.09368. Hence the upper density of U^* is at most $0.5 - 0.09368 = 0.40632$.

QUICK REMARKS

REMARK

Let $Q = 2 \cdot 3 \cdot 5 \cdot 17$. Then this theorem implies that the lower density of U^* must be at least

$$\left(1 - \frac{85}{131}\right) \frac{384}{5592405 \cdot 510} > 4.727 \cdot 10^{-8}.$$

REMARK

As for the upper density of U^*, consider numbers of the form $s^*(2^w p) = 2^w + p + 1$. The lower density of numbers of the form $s^*(2^w p)$ is equal to the lower density of number of the form $2^w + p$. Habsieger and Roblot (and Lü and Pintz, each independently) showed that the lower density is at least 0.09368. Hence the upper density of U^* is at most $0.5 - 0.09368 = 0.40632$.

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2s^*(2^j m) - \sigma^*(m)$

1

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2 s^*(2^j m) - \sigma^*(m)$

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2s^*(2^j m) - \sigma^*(m)$

1. $s^*(2^j m)$ strictly increases as j increases, so we keep going until $s^*(2^j m) > N$

1

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2s^*(2^j m) - \sigma^*(m)$

1. $s^*(2^j m)$ strictly increases as j increases, so we keep going until $s^*(2^j m) > N$
2. Move on to the next odd integer until $m \geq N$

1

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2 s^*(2^j m) - \sigma^*(m)$

1. $s^*(2^j m)$ strictly increases as j increases, so we keep going until $s^*(2^j m) > N$
2. Move on to the next odd integer until $m \geq N$
3. Most recently known result: up to 10^5, by David Wilson (2001)

1

Computations of unitary nonaliquots up to N

We computed the number of UNA's using the following relation:

Proposition

For $j \in \mathbb{Z}_+$ and m odd,

(I) $s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)$

(II) $s^*(2^{j+1} m) = 2 s^*(2^j m) - \sigma^*(m)$

1. $s^*(2^j m)$ strictly increases as j increases, so we keep going until $s^*(2^j m) > N$
2. Move on to the next odd integer until $m \geq N$
3. Most recently known result: up to 10^5, by David Wilson (2001)
4. Table (up to 10^8![1]) next slide

[1] 'Here the "!" symbol is merely an exclamation mark, and not a factorial sign!' – Roger Heath-Brown, arXiv:1002.3754

Computations of unitary nonaliquots up to 10^8

x	$N(x)$	$100D(x)$	x	$N(x)$	$100D(x)$
1000000	9903	0.99030	15000000	152930	1.01953
2000000	19655	0.98275	20000000	203113	1.01557
3000000	29700	0.99000	30000000	304631	1.01544
4000000	40302	1.00755	40000000	405978	1.01495
5000000	50081	1.00162	50000000	509695	1.01939
6000000	60257	1.00428	60000000	615349	1.02558
7000000	70518	1.00740	70000000	720741	1.02963
8000000	80987	1.01234	80000000	821201	1.02650
9000000	91087	1.01208	90000000	923994	1.02666
10000000	101030	1.01030	100000000	1028263	1.02826

Conjecture & open questions

Conjecture

The density of U^* exists and is about 0.01.

Open questions:

- (Asymptotic) Density of unitary nonaliquot numbers (if it exists)?
- Better lower bound of the lower density of unitary untouchable numbers?
- Expansion of the table/more efficient algorithm?

For more information

If you are interested, you can read the preprint in my website. Preprint is available at:
https://www.heesungyang.com/papers/varianterdos.pdf.
The paper was accepted for publication by Math. Comp.

C. Pomerance and H. Yang, *Variant of a theorem of Erdős on the sum-of-proper-divisors function*, Math. Comp. **83** (2014), 1903–1913.

List of References (partial)

- P. Erdős, *On the integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123.
- P. Erdős, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$*, Elemente der Mathematik **11** (1973), 83–86.
- Richard K. Guy, *Unsolved Problems in Number Theory*, Springer, 2004.
- H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.
- E. J. Scourfield, *Non-divisibility of some multiplicative functions*, Acta Arith. *22* (1973), 287–314.
- H. J. J. te Riele, *A theoretical and computational study of generalized aliquot sequences*, Ph.D. thesis, Universiteit van Amsterdam, 1976.