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

Hee-Sung Yang
Joint work with Carl Pomerance

Dartmouth College

11 January 2013

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 f’s range

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 f's range

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 f's range

DEFINITION

An integer m is called *f-untouchable* if there is no n such that $f(n) = m$. Equivalently, m is f-untouchable if $m \in \mathbb{N} \setminus f(\mathbb{N})$.

Detour

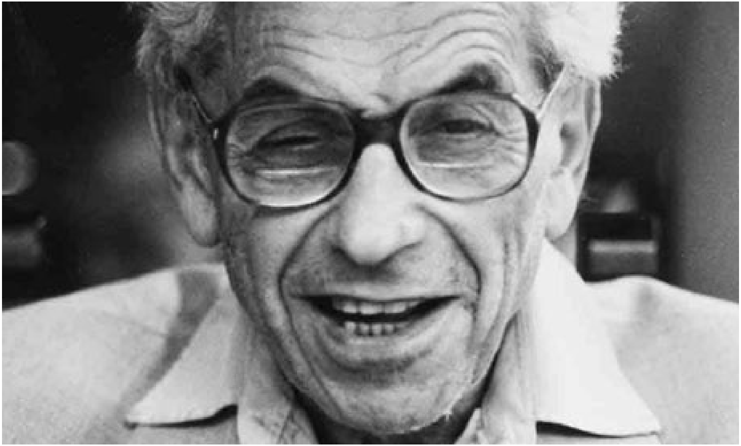
Conjecture (Goldbach)

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. A few things we can learn:

- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.
- It will be more exciting to study even numbers as far as s- (and s^*-) untouchables are concerned;
- Furthermore, examine even numbers if we want to find a positive proportion of s- (and s^*-) untouchables!

Erdős and s-untouchable numbers



Erdős Pál (1913 – 1996)

Erdős and s-untouchable 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 $a_1 < a_2 < a_3 < \ldots$ eine unendliche Folge natürlicher Zahlen und $A(n)$ die Anzahl der $a_i \le n$, so ist für $n \to \infty$ $\underline{d} = \underline{\lim}\, A(n)/n$ die untere und $\bar{d} = \overline{\lim}\, A(n)/n$ die obere Dichte der Folge. Ist $\underline{d} = \bar{d} = d$, so wird d die (asymptotische) Dichte der Folge genannt.

te Riele and s^*-untouchable numbers

Herman te Riele (b. 1947)

te Riele and s^*-untouchable numbers

1. In his doctoral thesis, he tried to tackle s^*-untouchables
2. Problem: integers of the form $2^w p$ ($w \geq 1, p$ an odd prime)
3. Problematic, as there are "too many" $2^w p$'s with $s^*(2^w p) \leq x$ for any x
4. te Riele's astute observation: de Polignac's conjecture true $\Rightarrow$ all even numbers > 2 are s^*-touchable

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.

5. The conjecture proved to be false. In fact, Erdős used the theory of covering congruences to disprove this conjecture. This gave us the starting point.

te Riele and s^*-untouchable numbers

1. In his doctoral thesis, he tried to tackle s^*-untouchables
2. Problem: integers of the form $2^w p$ ($w \geq 1, p$ an odd prime)
3. Problematic, as there are "too many" $2^w p$'s with $s^*(2^w p) \leq x$ for any x
4. te Riele's astute observation: de Polignac's conjecture true $\Rightarrow$ all even numbers > 2 are s^*-touchable

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.*

5. The conjecture proved to be false. 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 $U^* := \mathbb{N} \setminus s^*(\mathbb{N})$ *is positive.*

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. Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^w p)$ ("Case 0")

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. Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^w p)$ ("Case 0")
3. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod 4$, i..e, $2 \parallel n$
   - Case II: $n = 2^w p^a$ $(a > 1)$
   - Case III: $4 \mid n$, n has more than one odd prime factor
   - Case IV: 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. Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^w p)$ ("Case 0")
3. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod 4$, i..e, $2 \parallel n$
   - Case II: $n = 2^w p^a$ $(a > 1)$
   - Case III: $4 \mid n$, n has more than one odd prime factor
   - Case IV: n is odd
4. We see that Cases II, III, and IV aren't that exciting.

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. Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^w p)$ ("Case 0")
3. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod 4$, i..e, $2 \parallel n$
   - Case II: $n = 2^w p^a$ $(a > 1)$
   - Case III: $4 \mid n$, n has more than one odd prime factor
   - Case IV: n is odd
4. We see that Cases II, III, and IV aren't that exciting.
5. However, Case I is more interesting.

Case 0: $n = 2^w p$

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 $z := s^*(2^w p) = 1 + 2^w + p$ we have:

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

Case 0: $n = 2^w p$

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 $z := s^*(2^w p) = 1 + 2^w + p$ we have:

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

Case 0: $n = 2^w p$

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 $z := s^*(2^w p) = 1 + 2^w + p$ we have:

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

Case 0: $n = 2^w p$

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

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

This gives us $z \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. 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.

CASE 0: $n = 2^w p$

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

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

This gives us $z \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. 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.

Case 0: $n = 2^w p$

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

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

This gives us $z \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. 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.

Case 0: $n = 2^w p$

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

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

This gives us $z \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. 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.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Now what?

- 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 $s^*(n)$.
- We choose $Q := 2 \cdot 3^\alpha \cdot 5^\beta \cdot 17^\gamma$.
- Also, $c \equiv 0 \pmod{3 \cdot 5 \cdot 17}$, meaning an integer can be both $c \pmod{d}$ and has Q as a unitary divisor.
- One can see that there are 510 residue classes mod $2dQ$ that are both c mod d and 0 mod Q. Of these, $\varphi(510) = 128$ of these have Q as a unitary divisor.
- Also, there are six different ways of coverings (keeping three of them intact 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 $128 \cdot 6$.

Statement of the theorem

We shall endeavour to show the following:

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

Statement of the theorem

We shall endeavour to show the following:

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 computational remark

Remark

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

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

Proof of the main theorem

We want to consider integers n satisfying the following:

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

Almost all n's have $2dQ \mid \sigma^*(n)$. So $n \equiv -r \pmod{2dQ}$ has Q as a unitary divisor, so we have

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

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

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

Proof of the main theorem

We want to consider integers n satisfying the following:

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

Almost all n's have $2dQ \mid \sigma^*(n)$. So $n \equiv -r \pmod{2dQ}$ has Q as a unitary divisor, so we have

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

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

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

Proof of the main theorem

We want to consider integers n satisfying the following:

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

Almost all n's have $2dQ \mid \sigma^*(n)$. So $n \equiv -r \pmod{2dQ}$ has Q as a unitary divisor, so 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

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

Proof of the main theorem

We want to consider integers n satisfying the following:

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

Almost all n's have $2dQ \mid \sigma^*(n)$. So $n \equiv -r \pmod{2dQ}$ has Q as a unitary divisor, so we have

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

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

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

Proof of the main theorem

We want to consider integers n satisfying the following:

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

Almost all n's have $2dQ \mid \sigma^*(n)$. So $n \equiv -r \pmod{2dQ}$ has Q as a unitary divisor, so we have

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

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

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

Computations of U. untouchables $\leq N$

We computed the number of UU'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 U. untouchables $\leq N$

We computed the number of UU'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 U. untouchables $\leq N$

We computed the number of UU'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 $s^*(2^j m) > N$

1

Computations of U. untouchables $\leq N$

We computed the number of UU'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 U. untouchables $\leq N$

We computed the number of UU'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 $m \geq N$
3. Most recently known result: up to 10^5, by David Wilson (2001)

1

Computations of U. untouchables $\leq N$

We computed the number of UU'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 $m \geq N$
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 U. untouchables $\leq 10^8$

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 untouchable 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:
`http://www.math.ucla.edu/~hyang/publications/varianterdos.pdf`.
The paper was accepted for publication by Math. Comp.

List of References (partial)

- A. de Polignac, *Recherches novellas sur les numbers premiers*, C. R. Acad. Sci. Paris Math. **29** (1849), 397–401, 738–739.
- 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.
- H. J. J. te Riele, *A theoretical and computational study of generalized aliquot sequences*, Ph.D. thesis, Universiteit van Amsterdam, 1976.

Acknowledgements

- This work was based on my undergraduate honours thesis
- Prof. Carl Pomerance, my adviser
- Dartmouth College Mathematics Department
- Organizers of the special session for inviting me
- MAA for the financial support via MAA Travel Grant