UNITARY UNTOUCHABLE NUMBERS

Hee-Sung Yang
Advisor: Carl Pomerance

Dartmouth College

29 May 2012
# OUTLINE

## 1 OVERVIEW
- Introduction
- Historical context
- Here comes Erdős!
- Herman te Riele

## 2 UNITARY UNTOUCHABLE NUMBERS
- Overview of the proof
- Construction of the main theorem
- Proof of the main theorem

## 3 COMPUTATIONAL RESULTS & FUTURE DIRECTION
- Computations
- Future direction

## 4 REFERENCES
**Quick Definitions**

**Definition**

Any function $f : \mathbb{Z}_+ \to \mathbb{C}$ 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 $n$.

**Remark**

$\sigma(n)$ (sum-of-divisors function) and $\sigma^*(n)$ (sum-of-unitary-divisors function) are both multiplicative, so it suffices to define them over prime-powers.


**DEFINITION**

Any function $f : \mathbb{Z}_+ \rightarrow \mathbb{C}$ 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 $n$.

**REMARK**

$\sigma(n)$ (sum-of-divisors function) and $\sigma^*(n)$ (sum-of-unitary-divisors function) are both multiplicative, so it suffices to define them over prime-powers.
**Quick Definitions**

**Definition**

Any function $f : \mathbb{Z}_+ \rightarrow \mathbb{C}$ 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 $n$.

**Remark**

$\sigma(n)$ (sum-of-divisors function) and $\sigma^*(n)$ (sum-of-unitary-divisors function) are both multiplicative, so it suffices to define them over prime-powers.
**NOTATION**

- $p$ or $p_i$ always denotes an *odd* prime
- $\sigma(n)$: 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 $s(n) = s^*(n)$. 
### How to Study Arithmetical Functions?

How to study arithmetical functions?
How to study arithmetical functions?

- Study the distribution of the range of $f$ within $\mathbb{Z}_{\geq 0}$
HOW TO STUDY ARITHMETICAL FUNCTIONS?

- Study the distribution of the range of $f$ within $\mathbb{Z}_{\geq 0}$
- Or one can study the “non-range”, i.e., which integers are *not* in $f$’s range
HOW TO STUDY ARITHMETICAL FUNCTIONS?

- Study the distribution of the range of $f$ within $\mathbb{Z}_{\geq 0}$
- Or one can study the “non-range”, i.e., which integers are not in $f$’s range
HOW TO STUDY ARITHMETICAL FUNCTIONS?

- Study the distribution of the range of $f$ within $\mathbb{Z}_{\geq 0}$
- Or one can study the “non-range”, 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 $f(n) = m$. 
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 $\geq 9$. A few things we can learn:

- 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!
- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.


**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 $\geq 9$. A few things we can learn:

- 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!
- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.
**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 $\geq 9$. A few things we can learn:

- 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!
- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.
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 $\geq 9$. A few things we can learn:

- 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!
- Montgomery & Vaughan: The set of odd numbers not of the form $p + q + 1$ has density 0.
Here comes Erdős!

Erdős AND $s$-UNTTOUCHABLE NUMBERS

Erdős Pal (1913 – 1996)
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 $\varphi$-Funktion und vermuteten, dass für unendlich viele $m$ die Gleichung

$$n - \varphi(n) = m$$

(1)

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

$$\sigma(n) - n = m$$

(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 $n = \varphi q$, wo $\varphi$ und $q$ verschiedene ungerade Primzahlen sind. Offenbar ist

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

\(^1\) Ist $a_1 < a_2 < a_3 < \ldots$ eine unendliche Folge natürlicher Zahlen und $A(n)$ die Anzahl der $a_k \leq n$, so ist für $n \to \infty$ $\bar{\omega} = \lim A(n)/n$ die untere und $\bar{\mu} = \lim A(n)/n$ die obere Dichte der Folge. Ist $\omega = \bar{\omega} = \bar{\mu}$, so wird $\omega$ die (asymptotische) Dichte der Folge genannt.
**Theorem (Erdős, 1973)**

There is a positive proportion of $s$-untouchable numbers. Hence, there are infinitely many $s$-untouchable numbers.
**THEOREM (Erdős, 1973)**

There is a positive proportion of s-untouchable numbers. Hence, there are infinitely many s-untouchable numbers.
Theorem (Erdős, 1973)

There is a positive proportion of $s$-untouchable numbers. Hence, there are infinitely many $s$-untouchable numbers.

Proof (Sketch).

- For each fixed $d \in \mathbb{Z}_+$, $\sigma(n)$ is divisible by $d$ for “almost all” $n$. Suppose $\sigma(n)$ is divisible by many small primes.
- If $n$ has the same property, then one sees that not only is $s(n)$ divisible by those small primes, but $s(n)/n$ becomes large.
- Meaning, if $N$ is divisible by the same small primes and $s(n) = N$, then $n$ is considerably smaller than $N$.
- So such numbers $N$ divisible by those small primes are mostly $s$-untouchable.
TE RIELE AND s*-UNTACTHABLE NUMBERS

Herman te Riele (b. 1947)
In his doctoral thesis, he tried to tackle the problem: integers of the form $2^w p^r (w \geq 1, p$ an odd prime). Problematic, as there are too many $2^w p^r$'s with $s^*(2^w p^r) \leq x$ for any $x$. 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 or 1. The conjecture proved to be false.
In his doctoral thesis, he tried to tackle $s^*$-untouchables.
In his doctoral thesis, he tried to tackle $s^*$-untouchables

Problem: integers of the form $2^w p$ ($w \geq 1, p$ an odd prime)
In his doctoral thesis, he tried to tackle $s^*$-untouchables

Problem: integers of the form $2^wp$ ($w \geq 1$, $p$ an odd prime)

Problematic, as there are too many $2^wp$’s with $s^*(2^wp) \leq x$ for any $x$
In his doctoral thesis, he tried to tackle $s^*$-untouchables

Problem: integers of the form $2^wp$ ($w \geq 1$, $p$ an odd prime)

Problematic, as there are too many $2^wp$'s with $s^*(2^wp) \leq x$ for any $x$

te Riele’s astute observation: de Polignac’s conjecture true $\Rightarrow$ all even numbers $> 2$ are $s^*$-touchable
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 or 1.*
In his doctoral thesis, he tried to tackle \( s^\ast \)-untouchables.

Problem: integers of the form \( 2^wp \) (\( w \geq 1, p \) an odd prime)

Problematic, as there are too many \( 2^wp \)'s with \( s^\ast(2^wp) \leq x \) for any \( x \)

te Riele’s astute observation: de Polignac’s conjecture true \( \Rightarrow \) all even numbers > 2 are \( s^\ast \)-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 or 1.

The conjecture proved to be false.
TE RIELE AND s*-UNTOUCHABLE NUMBERS

1. In his doctoral thesis, he tried to tackle s*-untouchables.
2. Problem: integers of the form $2^wp$ ($w \geq 1$, $p$ an odd prime).
3. Problematic, as there are too many $2^wp$'s with $s^*(2^wp) \leq x$ 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 or 1.*

5. The conjecture proved to be false.
OK, CONCLUSION FIRST

Are there infinitely many unitary untouchable numbers?

Yes! In fact, a positive proportion of the integers are.
OK, CONCLUSION FIRST

Are there infinitely many unitary untouchable numbers?
OK, CONCLUSION FIRST

QUESTION
Are there infinitely many unitary untouchable numbers?

ANSWER
Yes! In fact, a positive proportion of the integers are.
Overview of the proof

Outline of our strategy

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

2. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod{4}$, i.e., $2 \mid n$
   - 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

3. We see that Cases II, III, and IV aren't that exciting.

4. However, the Erdős argument is needed for Case I.
Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^w p)$ (“Case 0”)
Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^wp)$ ("Case 0")

Now, tackle the remaining cases:
Overview of the Proof

Outline of our Strategy

1. Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^*(2^wp)$ (“Case 0”)

2. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod{4}$, i.e., $2 \mid n$
   - Case II: $n = 2^wp^a$ ($a > 1$)
   - Case III: $4 \mid n$, $n$ has more than one odd prime factor
   - Case IV: $n$ is odd
**Outline of Our Strategy**

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

2. Now, tackle the remaining cases:
   - Case I: $n \equiv 2 \pmod{4}$, i.e., $2 \mid n$
   - 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

3. We see that Cases II, III, and IV aren’t that exciting.
Derive an infinite arithmetic progression that are totally missed by the numbers of the form $s^* (2^w p)$ (“Case 0”)

Now, tackle the remaining cases:

- Case I: $n \equiv 2 \pmod{4}$, i.e., $2 \mid n$
- 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

We see that Cases II, III, and IV aren’t that exciting.

However, the Erdős argument is needed for Case I.
Case 0: \( n = 2^w p \)

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

\[
\begin{align*}
    w &\equiv 1 \pmod{2}, \quad w \equiv 1 \pmod{3} \\
    w &\equiv 2 \pmod{4}, \quad w \equiv 4 \pmod{8} \\
    w &\equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}.
\end{align*}
\]

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 \( N := s^*(2^w p) = 1 + 2^w + p \) we have:

<table>
<thead>
<tr>
<th>( m )</th>
<th>( q )</th>
<th>( 2^w \pmod{q} )</th>
<th>( N \pmod{q} )</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{3} ) or ( p = 3 )</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>( N \equiv 3 + p )</td>
<td>( N \not\equiv 0 \pmod{7} ) or ( p = 7 )</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>−1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{5} ) or ( p = 5 )</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>−1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{17} ) or ( p = 17 )</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>−4</td>
<td>( N \equiv −3 + p )</td>
<td>( N \not\equiv −3 \pmod{13} ) or ( p = 13 )</td>
</tr>
<tr>
<td>24</td>
<td>241</td>
<td>1</td>
<td>( N \equiv 2 + p )</td>
<td>( N \not\equiv 2 \pmod{241} ) or ( p = 241 )</td>
</tr>
</tbody>
</table>
CASE 0: \( n = 2^w p \)

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

\[
\begin{align*}
    w &\equiv 1 \pmod{2}, \quad w \equiv 1 \pmod{3} \\
    w &\equiv 2 \pmod{4}, \quad w \equiv 4 \pmod{8} \\
    w &\equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}.
\end{align*}
\]

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 \( N := s^*(2^wp) = 1 + 2^w + p \) we have:

<table>
<thead>
<tr>
<th>( m )</th>
<th>( q )</th>
<th>( 2^w \pmod{q} )</th>
<th>( N \pmod{q} )</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{3} ) or ( p = 3 )</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>( N \equiv 3 + p )</td>
<td>( N \not\equiv 3 \pmod{7} ) or ( p = 7 )</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>−1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{5} ) or ( p = 5 )</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>−1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{17} ) or ( p = 17 )</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>−4</td>
<td>( N \equiv −3 + p )</td>
<td>( N \not\equiv −3 \pmod{13} ) or ( p = 13 )</td>
</tr>
<tr>
<td>24</td>
<td>241</td>
<td>1</td>
<td>( N \equiv 2 + p )</td>
<td>( N \not\equiv 2 \pmod{241} ) or ( p = 241 )</td>
</tr>
</tbody>
</table>
**Case 0: \( n = 2^wp \)**

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

\[
\begin{align*}
  w &\equiv 1 \pmod{2}, \quad w \equiv 1 \pmod{3} \\
  w &\equiv 2 \pmod{4}, \quad w \equiv 4 \pmod{8} \\
  w &\equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}.
\end{align*}
\]

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 \( N := s^*(2^wp) = 1 + 2^w + p \) we have:

<table>
<thead>
<tr>
<th>( m )</th>
<th>( q )</th>
<th>( 2^w \mod q )</th>
<th>( N \mod q )</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{3} ) or ( p = 3 )</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>( N \equiv 3+p )</td>
<td>( N \not\equiv 0 \pmod{7} ) or ( p = 7 )</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>-1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{5} ) or ( p = 5 )</td>
</tr>
<tr>
<td>8</td>
<td>17</td>
<td>-1</td>
<td>( N \equiv p )</td>
<td>( N \not\equiv 0 \pmod{17} ) or ( p = 17 )</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>-4</td>
<td>( N \equiv -3+p )</td>
<td>( N \not\equiv -3 \pmod{13} ) or ( p = 13 )</td>
</tr>
<tr>
<td>24</td>
<td>241</td>
<td>1</td>
<td>( N \equiv 2+p )</td>
<td>( N \not\equiv 0 \pmod{241} ) or ( p = 241 )</td>
</tr>
</tbody>
</table>
Every \( w \in \mathbb{Z} \) satisfies at least one of the following six congruences:

\[
\begin{align*}
    w &\equiv 1 \pmod{2}, \quad w \equiv 1 \pmod{3} \\
    w &\equiv 2 \pmod{4}, \quad w \equiv 4 \pmod{8} \\
    w &\equiv 8 \pmod{12}, \quad w \equiv 0 \pmod{24}.
\end{align*}
\]

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 \( N := s^*(2^w p) = 1 + 2^w + p \) we have:

\[
\begin{array}{|c|c|c|c|c|}
\hline
 m & q & 2^w \mod q & N \mod q & \text{Conclusion} \\
\hline
 2 & 3 & 2 & N \equiv p & N \not\equiv 0 \pmod{3} \text{ or } p = 3 \\
 3 & 7 & 2 & N \equiv 3 + p & N \not\equiv 3 \pmod{7} \text{ or } p = 7 \\
 4 & 5 & -1 & N \equiv p & N \not\equiv 0 \pmod{5} \text{ or } p = 5 \\
 8 & 17 & -1 & N \equiv p & N \not\equiv 0 \pmod{17} \text{ or } p = 17 \\
12 & 13 & -4 & N \equiv -3 + p & N \not\equiv -3 \pmod{13} \text{ or } p = 13 \\
24 & 241 & 1 & N \equiv 2 + p & N \not\equiv 2 \pmod{241} \text{ or } p = 241 \\
\hline
\end{array}
\]
**Case 0: \( n = 2^wp \)**

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

\[
N \equiv 0 \pmod{3}, \quad N \equiv 3 \pmod{7} \\
N \equiv 0 \pmod{5}, \quad N \equiv 0 \pmod{17} \\
N \equiv -3 \pmod{13}, \quad N \equiv 2 \pmod{241}.
\]

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

**Lemma**

*Let \( n = 2^wp \), 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: $n = 2^wp$

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

\[
\begin{align*}
N &\equiv 0 \pmod{3}, \quad N \equiv 3 \pmod{7} \\
N &\equiv 0 \pmod{5}, \quad N \equiv 0 \pmod{17} \\
N &\equiv -3 \pmod{13}, \quad N \equiv 2 \pmod{241}.
\end{align*}
\]

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

**Lemma**

Let $n = 2^wp$, 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 \( s^*(2^w p) \):

\[
\begin{align*}
N &\equiv 0 \pmod{3}, \quad N \equiv 3 \pmod{7} \\
N &\equiv 0 \pmod{5}, \quad N \equiv 0 \pmod{17} \\
N &\equiv -3 \pmod{13}, \quad N \equiv 2 \pmod{241}.
\end{align*}
\]

This gives us \( N \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241} \). 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 $s^*(2^w p)$:

\[
\begin{align*}
N &\equiv 0 \pmod{3}, \quad N \equiv 3 \pmod{7} \\
N &\equiv 0 \pmod{5}, \quad N \equiv 0 \pmod{17} \\
N &\equiv -3 \pmod{13}, \quad N \equiv 2 \pmod{241}.
\end{align*}
\]

This gives us $N \equiv -1518780 \pmod{3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241}$. 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 $p$. 
We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and $p$ an odd prime.

But we need more: recall that the Erdős argument relied on the fact that $n$ is divisible by the product of small primes, then $s(n)/n$ is large.

In the case of $\sigma^*(n)$, we need $n$’s that have the product of small primes as unitary divisors.

At the same time, we want to have a single residue class which we can use for the Erdős argument. So, my choice of those "small primes" will be $Q_k := (2 \cdot 3 \cdots \cdot p_k)/(d, 2 \cdot 3 \cdots \cdot p_k)$.

My pick: $s^*(n) \equiv Q_k \pmod{Q_k^2}$
Quick re-visit to Erdős

- We constructed this residue class that is totally missed by $s^*(2^wp)$ for all $w \geq 1$ and $p$ an odd prime.
- But we need more: recall that the Erdős argument relied on the fact that $n$ is divisible by the product of small primes, then $s(n)/n$ is large.
- In the case of $\sigma^*(n)$, we need $n$’s that have the product of small primes as unitary divisors.
- At the same time, we want to have a single residue class which we can use for the Erdős argument. So, my choice of those "small primes" will be $Q_k := (2 \cdot 3 \cdot \cdots \cdot p_k)/(d, 2 \cdot 3 \cdot \cdots \cdot p_k)$.
- My pick: $s^*(n) \equiv Q_k \pmod{Q_k^2}$
Quick re-visit to Erdős

- We constructed this residue class that is totally missed by $s^*(2^wp)$ for all $w \geq 1$ and $p$ an odd prime.
- But we need more: recall that the Erdős argument relied on the fact that $n$ is divisible by the product of small primes, then $s(n)/n$ is large.
- In the case of $\sigma^*(n)$, we need $n$’s that have the product of small primes as unitary divisors.
- At the same time, we want to have a single residue class which we can use for the Erdős argument. So, my choice of those "small primes" will be $Q_k := (2 \cdot 3 \cdots \cdot p_k)/(d, 2 \cdot 3 \cdots \cdot p_k)$.
- My pick: $s^*(n) \equiv Q_k \pmod{Q_k^2}$
Quick re-visit to Erdős

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and $p$ an odd prime.

- But we need more: recall that the Erdős argument relied on the fact that $n$ is divisible by the product of small primes, then $s(n)/n$ is large.

- In the case of $\sigma^*(n)$, we need $n$’s that have the product of small primes as unitary divisors.

- At the same time, we want to have a single residue class which we can use for the Erdős argument. So, my choice of those "small primes" will be $Q_k := (2 \cdot 3 \cdots p_k)/(d, 2 \cdot 3 \cdots p_k)$.

- My pick: $s^*(n) \equiv Q_k \pmod{Q_k^2}$
Quick re-visit to Erdős

- We constructed this residue class that is totally missed by $s^*(2^w p)$ for all $w \geq 1$ and $p$ an odd prime.

- But we need more: recall that the Erdős argument relied on the fact that $n$ is divisible by the product of small primes, then $s(n)/n$ is large.

- In the case of $\sigma^*(n)$, we need $n$’s that have the product of small primes as unitary divisors.

- At the same time, we want to have a single residue class which we can use for the Erdős argument. So, my choice of those "small primes" will be $Q_k := (2 \cdot 3 \cdots \cdot p_k)/(d, 2 \cdot 3 \cdots \cdot p_k)$.

- My pick: $s^*(n) \equiv Q_k \pmod{Q_k^2}$
We denote $r_k$ the residue class mod $dQ_k^2$ that is both $Q_k$ mod $Q_k^2$ and $c$ mod $d$. So we shall endeavour to prove the following:

**Theorem**

Let $P_k$ be the product of first $k$ primes, and let $Q_k := P_k/(d, P_k)$. Then there exists $k_0$ such that if $k > k_0$ then the upper density of integers $s^*(n)$ satisfying

$$s^*(n) \equiv r_k \pmod{dQ_k^2}$$

is less than $1/2dQ_k^2$. That is, one can find a sufficiently large $k$ so that the lower density of unitary untouchable numbers is at least $1/2dQ_k^2$. 


We denote $r_k$ the residue class mod $dQ_k^2$ that is both $Q_k$ mod $Q_k^2$ and $c$ mod $d$. So we shall endeavour to prove the following:

**Theorem**

Let $P_k$ be the product of first $k$ primes, and let $Q_k := P_k/(d, P_k)$. Then there exists $k_0$ such that if $k > k_0$ then the upper density of integers $s^*(n)$ satisfying

$$s^*(n) \equiv r_k \pmod{dQ_k^2}$$

is less than $1/2dQ_k^2$. That is, one can find a sufficiently large $k$ so that the lower density of unitary untouchable numbers is at least $1/2dQ_k^2$. 
**Case I: \( n \equiv 2 \pmod{4} \)**

Almost all \( n \)'s have \( Q_k \mid \sigma^*(n) \). So \( n \equiv -Q_k \pmod{Q_k^2} \), i.e., \( Q_k \parallel n \).

Let \( \varepsilon > 0 \) be some fixed real number.

\[
\sigma^*(n) \geq n \prod_{q \mid Q_k \atop q \text{ prime}} \left( 1 + \frac{1}{q} \right) > n \left( 1 + \sum_{q \mid Q_k \atop q \text{ prime}} \frac{1}{q} \right) > n \left( 1 + \frac{1}{\varepsilon} \right)
\]

Note that we can choose \( k \) sufficiently large (i.e. larger than \( k_0 \), which depends on our choice of \( \varepsilon \)) so that the second inequality holds, as the sum part tends to infinity as \( k \to \infty \).
Case I: $n \equiv 2 \pmod{4}$

Almost all $n$’s have $Q_k \mid \sigma^*(n)$. So $n \equiv -Q_k \pmod{Q_k^2}$, i.e., $Q_k \parallel n$.

Let $\varepsilon > 0$ be some fixed real number.

$$\sigma^*(n) \geq n \prod_{q \mid Q_k \atop q \text{ prime}} \left( 1 + \frac{1}{q} \right) > n \left( 1 + \sum_{q \mid Q_k \atop q \text{ prime}} \frac{1}{q} \right) > n \left( 1 + \frac{1}{\varepsilon} \right)$$

Note that we can choose $k$ sufficiently large (i.e. larger than $k_0$, which depends on our choice of $\varepsilon$) so that the second inequality holds, as the sum part tends to infinity as $k \to \infty$. 
Proof of the Main Theorem

**Case I: \( n \equiv 2 \pmod{4} \)**

Almost all \( n \)'s have \( Q_k \mid \sigma^*(n) \). So \( n \equiv -Q_k \pmod{Q_k^2} \), i.e., \( Q_k \mid\mid n \).

Let \( \varepsilon > 0 \) be some fixed real number.

\[
\sigma^*(n) \geq n \prod_{\substack{q \mid Q_k \\ q \text{ prime}}} \left( 1 + \frac{1}{q} \right) > n \left( 1 + \sum_{\substack{q \mid Q_k \\ q \text{ prime}}} \frac{1}{q} \right) > n \left( 1 + \frac{1}{\varepsilon} \right)
\]

Note that we can choose \( k \) sufficiently large (i.e. larger than \( k_0 \), which depends on our choice of \( \varepsilon \)) so that the second inequality holds, as the sum part tends to infinity as \( k \to \infty \).
**Case I: \( n \equiv 2 \pmod{4} \)**

Almost all \( n \)'s have \( Q_k \mid \sigma^*(n) \). So \( n \equiv -Q_k \pmod{Q_k^2} \), i.e., \( Q_k \parallel n \).

Let \( \varepsilon > 0 \) be some fixed real number.

\[
\sigma^*(n) \geq n \prod_{\substack{q|Q_k \\ q \text{ prime}}} \left( 1 + \frac{1}{q} \right) > n \left( 1 + \sum_{\substack{q|Q_k \\ q \text{ prime}}} \frac{1}{q} \right) > n \left( 1 + \frac{1}{\varepsilon} \right)
\]

Note that we can choose \( k \) sufficiently large (i.e. larger than \( k_0 \), which depends on our choice of \( \varepsilon \)) so that the second inequality holds, as the sum part tends to infinity as \( k \to \infty \).
**Case I: \( n \equiv 2 \pmod{4} \)**

We also want \( \sigma^*(n) - n \leq x \), so it follows that

\[
\frac{1}{\varepsilon} n < \sigma^*(n) - n \leq x \Rightarrow n < \varepsilon x.
\]

But then we are only concerned with one of the residue classes mod \( dQ_k^2 \), so the number of \( n \)'s we are looking for is at most \( 1 + \varepsilon x / dQ_k^2 \).

**Lemma**

Suppose \( n \equiv 2 \pmod{4} \), i.e., \( 2 \parallel n \). Then for any \( \varepsilon > 0 \) there exists some \( k_0(\varepsilon) \) and \( x_0(\varepsilon) \) so that if \( k > k_0(\varepsilon) \), then the number of \( n \)'s satisfying the desired conditions is at most \( 1 + \varepsilon x / dQ_k^2 \) for all \( x > x_0(\varepsilon) \).
We also want $\sigma^*(n) - n \leq x$, so it follows that

$$\frac{1}{\varepsilon} n < \sigma^*(n) - n \leq x \Rightarrow n < \varepsilon x.$$

But then we are only concerned with one of the residue classes mod $dQ_k^2$, so the number of $n$’s we are looking for is at most $1 + \varepsilon x/dQ_k^2$.

**Lemma**

Suppose $n \equiv 2 \pmod{4}$, i.e., $2 \parallel n$. Then for any $\varepsilon > 0$ there exists some $k_0(\varepsilon)$ and $x_0(\varepsilon)$ so that if $k > k_0(\varepsilon)$, then the number of $n$’s satisfying the desired conditions is at most $1 + \varepsilon x/dQ_k^2$ for all $x > x_0(\varepsilon)$. 
**Proof of the main theorem**

**Case I: \( n \equiv 2 \pmod{4} \)**

We also want \( \sigma^*(n) - n \leq x \), so it follows that

\[
\frac{1}{\varepsilon} n < \sigma^*(n) - n \leq x \Rightarrow n < \varepsilon x.
\]

But then we are only concerned with one of the residue classes mod \( dQ_k^2 \), so the number of \( n \)'s we are looking for is at most \( 1 + \varepsilon x / dQ_k^2 \).

**Lemma**

Suppose \( n \equiv 2 \pmod{4} \), i.e., \( 2 \parallel n \). Then for any \( \varepsilon > 0 \) there exists some \( k_0(\varepsilon) \) and \( x_0(\varepsilon) \) so that if \( k > k_0(\varepsilon) \), then the number of \( n \)'s satisfying the desired conditions is at most \( 1 + \varepsilon x / dQ_k^2 \) for all \( x > x_0(\varepsilon) \).
We computed the number of UU’s using the following relation:

**PROPOSITION**

*For* \( j \in \mathbb{Z}_+ \) *and* \( m \) *odd,*

\[
(1) \quad s^*(2^j m) = 2^j s^*(m) + \sigma^*(m) \\
(2) \quad s^*(2^{j+1} m) = 2s^*(2^j m) - \sigma^*(m)
\]
We computed the number of UU’s using the following relation:

**Proposition**

*For* \( j \in \mathbb{Z}_+ \) *and* \( m \) *odd,*

\[
(\text{I}) \quad s^*(2^j m) = 2^j s^*(m) + \sigma^*(m)
\]

\[
(\text{II}) \quad s^*(2^{j+1} m) = 2 s^*(2^j m) - \sigma^*(m)
\]
We computed the number of UU’s using the following relation:

**Proposition**

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

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

$s^*(2^j m)$ strictly increases as $j$ increases, so we keep going until $s^*(2^j m) > N$
We computed the number of UU’s using the following relation:

**Proposition**

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

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

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 $m \geq N$
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,

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

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. Table (up to $10^8$! [not a factorial!]) next slide
### Computations of Unitary Untouchables $\leq 10^8$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$N(x)$</th>
<th>$100D$</th>
<th>$x$</th>
<th>$N(x)$</th>
<th>$100D$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000000</td>
<td>9903</td>
<td>0.9903</td>
<td>150000000</td>
<td>152930</td>
<td>1.01953</td>
</tr>
<tr>
<td>20000000</td>
<td>19655</td>
<td>0.98275</td>
<td>200000000</td>
<td>203113</td>
<td>1.01557</td>
</tr>
<tr>
<td>30000000</td>
<td>29700</td>
<td>0.99</td>
<td>300000000</td>
<td>304631</td>
<td>1.01544</td>
</tr>
<tr>
<td>40000000</td>
<td>40302</td>
<td>1.00755</td>
<td>400000000</td>
<td>405978</td>
<td>1.01495</td>
</tr>
<tr>
<td>50000000</td>
<td>50081</td>
<td>1.00162</td>
<td>500000000</td>
<td>509695</td>
<td>1.01939</td>
</tr>
<tr>
<td>60000000</td>
<td>60257</td>
<td>1.00428</td>
<td>600000000</td>
<td>615349</td>
<td>1.02558</td>
</tr>
<tr>
<td>70000000</td>
<td>70518</td>
<td>1.0074</td>
<td>700000000</td>
<td>720741</td>
<td>1.02963</td>
</tr>
<tr>
<td>80000000</td>
<td>80987</td>
<td>1.01234</td>
<td>800000000</td>
<td>821201</td>
<td>1.0265</td>
</tr>
<tr>
<td>90000000</td>
<td>91087</td>
<td>1.01208</td>
<td>900000000</td>
<td>923994</td>
<td>1.02666</td>
</tr>
<tr>
<td>100000000</td>
<td>101030</td>
<td>1.0103</td>
<td>1000000000</td>
<td>1028263</td>
<td>1.02826</td>
</tr>
</tbody>
</table>
CONJECTURE & OPEN QUESTIONS

CONJECTURE

The density of unitary untouchable numbers exists and is 0.01.

Open questions:

- (Asymptotic) Density of unitary untouchable numbers (if it exists)?
- Lower bound of the lower density of unitary untouchable numbers?
- Expansion of the table/more efficient algorithm?
List of References (partial)


- P. Erdős, *Über die Zahlen der Form σ(n) − n und n − ϕ(n)*, Elemente der Mathematik **11** (1973), 83–86.

