On the binary digits of $n$ and $n^2$

Pierre Popoli

joint work with Aloui, Jamet, Kaneko, Kopecki and Stoll

Université de Lorraine

Numeration 2023,
Liège, May 22-26, 2023
1 Introduction
2 Interference graph
3 Few binary digits
4 Algorithm
5 Open questions
Exponential diophantine equations

Diophantine equations with variables that appears in exponents.

Large family of problems, classically studied in number theory.
Exponential diophantine equations
Diophantine equations with variables that appears in exponents.

Large family of problems, classically studied in number theory.

- Ramanujan–Nagell equation: $2^n - 7 = x^2$.
  - Ramanujan (1913) conjectured that solutions are $n = 3, 4, 5, 7, 15$.
  - Nagell (1948) proved this conjecture.
Exponential diophantine equations

Diophantine equations with variables that appears in exponents.

Large family of problems, classically studied in number theory.

- Ramanujan–Nagell equation: $2^n - 7 = x^2$.
  - Ramanujan (1913) conjectured that solutions are $n = 3, 4, 5, 7, 15$.
  - Nagell (1948) proved this conjecture.
  - Apéry (1960) proved that the equation $2^n - D = x^2$ has at most two solutions ($D > 0, D \neq 7$).
Exponential diophantine equations

Diophantine equations with variables that appears in exponents.

Large family of problems, classically studied in number theory.

- Ramanujan–Nagell equation: $2^n - 7 = x^2$.
  - Ramanujan (1913) conjectured that solutions are $n = 3, 4, 5, 7, 15$.
  - Nagell (1948) proved this conjecture.
  - Apéry (1960) proved that the equation $2^n - D = x^2$ has at most two solutions ($D > 0, D \neq 7$).

- Generalized Ramanujan–Nagell equation: $y^n - D = x^2, D \neq 0$.
  - Beukers (2002): At most four solutions for $D < 0$.
  - Bugeaud-Mignotte-Siksek (2006): All solutions for $1 \leq D \leq 100$. 

Catalan’s conjecture (1844):

$x^a - y^b = 1, a, b > 1, x, y > 0 \Rightarrow x = b = 3, y = a = 2$.

- Mihăilescu (2003) proved this conjecture.
Exponential diophantine equations

Diophantine equations with variables that appears in exponents.

Large family of problems, classically studied in number theory.

- Ramanujan–Nagell equation: $2^n - 7 = x^2$.
  - Ramanujan (1913) conjectured that solutions are $n = 3, 4, 5, 7, 15$.
  - Nagell (1948) proved this conjecture.
  - Apéry (1960) proved that the equation $2^n - D = x^2$ has at most two solutions ($D > 0, D \neq 7$).

- Generalized Ramanujan–Nagell equation: $y^n - D = x^2$, $D \neq 0$.
  - Beukers (2002): At most four solutions for $D < 0$.
  - Bugeaud-Mignotte-Siksek (2006): All solutions for $1 \leq D \leq 100$.

- Catalan’s conjecture (1844): $x^a - y^b = 1$, $a, b > 1$, $x, y > 0$
  - $\implies x = b = 3, y = a = 2$.
  - Mihăilescu (2003) proved this conjecture.

- ....
Let \( k \geq 2 \)

\[
n^2 = 2^{a_{k-1}} + \cdots + 2^{a_1} + 1, \quad 0 < a_1 < \cdots < a_{k-1}.
\] (1)
Let $k \geq 2$

\[ n^2 = 2^{a_{k-1}} + \cdots + 2^{a_1} + 1, \quad 0 < a_1 < \cdots < a_{k-1}. \] (1)

$s(n) =$ sum of digits function in base 2, the Hamming weight.
→ $n$ satisfies (1) if and only if $s(n^2) = k$ and $n$ is odd.
Let $k \geq 2$

\[ n^2 = 2^{a_{k-1}} + \cdots + 2^{a_1} + 1, \quad 0 < a_1 < \cdots < a_{k-1}. \tag{1} \]

$s(n) =$ sum of digits function in base 2, the Hamming weight.

$\Rightarrow$ $n$ satisfies (1) if and only if $s(n^2) = k$ and $n$ is odd.

$a, b$ positive integers.

- **Subadditive**: $s(a + b) \leq s(a) + s(b)$.

- **Submultiplicative**: $s(ab) \leq s(a)s(b)$.

- **2-additive**: If $b < 2^r$, $s(a2^r + b) = s(a) + s(b)$.

\[
\begin{array}{cccc}
(a)_2 & 0 \cdots 0 & 0 \cdots 0 & = a2^r \\
+ & 0 \cdots 0 & (b)_2 & = b
\end{array}
\]

\[
\begin{array}{cccc}
(a)_2 & 0 \cdots 0 & (b)_2 & = a2^r + b.
\end{array}
\]

The sum is **non-interfering**: no interaction between the digits of $a$ and $b$. 
Expected values:

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n) = \frac{1}{2} \log_2(N) + O(1),
\]

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n^2) = \log_2(N) + O(1).
\]
Expected values:

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n) = \frac{1}{2} \log_2(N) + O(1),
\]

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n^2) = \log_2(N) + O(1).
\]

- Stolarsky (1978):
  \[
  \lim \inf \frac{s(n^2)}{s(n)} = 0,
  \]
  \[
  \lim \sup \frac{s(n^2)}{s(n)} = \infty.
  \]

- Madritsch, Stoll (2014):
  \[
  \frac{s(n^2)}{s(n)} \text{ is dense in } \mathbb{R}^+.
  \]
Expected values:

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n) = \frac{1}{2} \log_2(N) + O(1),
\]

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n^2) = \log_2(N) + O(1).
\]

- Stolarsky (1978):
  \[\lim \inf \frac{s(n^2)}{s(n)} = 0,\]
  \[\lim \sup \frac{s(n^2)}{s(n)} = \infty.\]

- Madritsch, Stoll (2014):
  \[\frac{s(n^2)}{s(n)} \text{ is dense in } \mathbb{R}^+.\]

Let \( k \geq 1 \), we study the following equation

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2) \]

→ Exceptional set of integers.
Expected values:

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n) = \frac{1}{2} \log_2(N) + O(1),
\]

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n^2) = \log_2(N) + O(1).
\]

- Stolarsky (1978):
  \[
  \lim \inf \frac{s(n^2)}{s(n)} = 0,
  \]
  \[
  \lim \sup \frac{s(n^2)}{s(n)} = \infty.
  \]

- Madritsch, Stoll (2014):
  \[
  \frac{s(n^2)}{s(n)} \text{ is dense in } \mathbb{R}^+.
  \]

Let \( k \geq 1 \), we study the following equation

\[
s(n) = s(n^2) = k, \quad n \text{ odd.}
\]  \hspace{1cm} (2)

\[\rightarrow\] Exceptionnal set of integers.

\[
91 = 1 + 2 + 8 + 16 + 64, \quad (91)_2 = 1011011, \quad s(91) = 5.
\]

\[
91^2 = 1 + 8 + 16 + 64 + 2^{13}, \quad (91^2)_2 = 10000001011001, \quad s(91^2) = 5.
\]
Expected values:

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n) = \frac{1}{2} \log_2(N) + O(1),
\]

\[
\frac{1}{N} \sum_{1 \leq n \leq N} s(n^2) = \log_2(N) + O(1).
\]

- Stolarsky (1978):
  \[
  \lim \inf \frac{s(n^2)}{s(n)} = 0,
  \]
  \[
  \lim \sup \frac{s(n^2)}{s(n)} = \infty.
  \]

- Madritsch, Stoll (2014):
  \[
  \frac{s(n^2)}{s(n)} \text{ is dense in } \mathbb{R}^+.
  \]

Let \( k \geq 1 \), we study the following equation

\[
s(n) = s(n^2) = k, \quad n \text{ odd.} \tag{2}
\]

\( \rightarrow \) Exceptionnal set of integers.

\[
91 = 1 + 2 + 8 + 16 + 64, \quad (91)_2 = 1011011, \quad s(91) = 5.
\]

\[
91^2 = 1 + 8 + 16 + 64 + 2^{13}, \quad (91^2)_2 = 10000001011001, \quad s(91^2) = 5.
\]

Q: Are there finitely or infinitely many solutions for (2)?
\( s(n) = s(n^2) = k, \quad n \text{ odd.} \) \hfill (2)

**Theorem (Hare, Laishram, Stoll, 2011)**
- If \( 1 \leq k \leq 8 \), (2) has **finitely** many solutions.
- If \( k = 12, 13 \) or \( k \geq 16 \), (2) has **infinitely** many solutions.

---

Pierre Popoli  
On the binary digits of \( n \) and \( n^2 \)
$$s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2)$$

**Theorem (Hare, Laishram, Stoll, 2011)**

- If $1 \leq k \leq 8$, (2) has **finitely** many solutions.
- If $k = 12, 13$ or $k \geq 16$, (2) has **infinitely** many solutions.

Proof by an algorithm that computes all the solutions for the first case.

*Example:* For $k = 5$, the set of solutions is $\{31, 79, 91, 157, 279\}$. 
\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \tag{2} \]

**Theorem (Hare, Laishram, Stoll, 2011)**

- If \( 1 \leq k \leq 8 \), (2) has **finitely** many solutions.
- If \( k = 12, 13 \) or \( k \geq 16 \), (2) has **infinitely** many solutions.

- Proof by an algorithm that computes all the solutions for the first case.
  
  *Example:* For \( k = 5 \), the set of solutions is \( \{31, 79, 91, 157, 279\} \).

- Give an infinite family of solutions for each \( k \) in the second case:
  \[ s(n) = s(n^2) = 12, \text{ for all } n = 111 \cdot 2^t + 111, \text{ with } t \geq 15. \]
  
  \[ (111)_2 \quad 0 \cdots 0 \quad (111)_2 = (n)_2 \]
  \[ (111^2)_2 \quad 0 \cdots 0 \quad (111^2)_2 = (n^2)_2 \]

And \( s(111) = 6, \ s(111^2) = 4. \)
\[ s(n) = s(n^2) = k, \quad n \text{ odd}. \] (2)

**Theorem (Hare, Laishram, Stoll, 2011)**

- If \( 1 \leq k \leq 8 \), (2) has **finitely** many solutions.
- If \( k = 12, 13 \) or \( k \geq 16 \), (2) has **infinitely** many solutions.

Q: What about \( 9 \leq k \leq 11 \) and \( k = 14, 15 \)?
$s(n) = s(n^2) = k$, \hspace{1cm} n odd. \hspace{1cm} (2)

**Theorem (Hare, Laishram, Stoll, 2011)**

- If $1 \leq k \leq 8$, (2) has **finitely** many solutions.
- If $k = 12, 13$ or $k \geq 16$, (2) has **infinitely** many solutions.

Q: What about $9 \leq k \leq 11$ and $k = 14, 15$?
- Previous algorithm is no longer adapted.
- No infinite family appears clearly.
\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2) \]

**Theorem (Hare, Laishram, Stoll, 2011)**

- If \(1 \leq k \leq 8\), (2) has **finitely** many solutions.
- If \(k = 12, 13\) or \(k \geq 16\), (2) has **infinitely** many solutions.

Q: What about \(9 \leq k \leq 11\) and \(k = 14, 15\)?

- Previous algorithm is no longer adapted.
- No infinite family appears clearly.

**Theorem (Aloui, Jamet, Kaneko, Kopecki, P., Stoll, 2023)**

If \(9 \leq k \leq 11\), (2) has **finitely** many solutions.

*Proof:* new combinatorial tools and algorithms.
Interference graph

\( m = 1 \)

Write \( n = 2^\ell m x_m + \cdots + 2^\ell_1 x_1 + x_0 \) such that

\[
(n)_2 = (x_m)_2 0 \cdots 0 (x_{m-1})_2 \cdots (x_1)_2 0 \cdots 0 (x_0)_2, \quad \eta_i \geq 0.
\]

→ Not unique decomposition.
Write $n = 2^\ell m x_m + \cdots + 2^\ell_1 x_1 + x_0$ such that

$$(n)_2 = (x_m)_2 0 \cdots 0 (x_{m-1})_2 \cdots (x_1)_2 0 \cdots 0 (x_0)_2, \, \eta_i \geq 0.$$ 

→ Not unique decomposition.

- For $m = 1$, $n^2 = 2^{2\ell_1} x_1^2 + 2^{\ell_1+1} x_1 x_0 + x_0^2$. 

![Diagram showing the binary representation and decomposition of $n^2$.]
Write $n = 2^\ell m x_m + \cdots + 2^\ell_1 x_1 + x_0$ such that

$$(n)_2 = (x_m)_2 0 \cdots 0 (x_{m-1})_2 \cdots (x_1)_2 0 \cdots 0 (x_0)_2, \; \eta_i \geq 0.$$  

$\rightarrow$ Not unique decomposition.

• For $m = 1$, $n^2 = 2^{2\ell_1} x_1^2 + 2^{\ell_1+1} x_1 x_0 + x_0^2$.

$|x|$ denotes the binary length of $x$.

If $\ell_1 + 1 > 2|x_0|$, no interference between $2^{\ell_1+1} x_1 x_0$ and $x_0^2$. 

$$(x_0^2)_2$$

$$(x_1 x_0)_2$$

$$(x_1^2)_2$$

$\ell_1 + 1$

$2\ell_1$
Interference graph

$m = 1$

Write $n = 2^{\ell m} x_m + \cdots + 2^{\ell_1} x_1 + x_0$ such that

$$(n)_2 = (x_m)_2 0 \cdots 0 (x_{m-1})_2 \cdots (x_1)_2 0 \cdots 0 (x_0)_2, \; \eta_i \geq 0.$$  

→ Not unique decomposition.

• For $m = 1$, $n^2 = 2^{2\ell_1} x_1^2 + 2^{\ell_1+1} x_1 x_0 + x_0^2$.

$$(x_0^2)_2$$

$$(x_1 x_0)_2$$

$$(x_1^2)_2$$

$\ell_1 + 1$

$2\ell_1$

$|x|$ denotes the binary length of $x$.

If $\ell_1 + 1 > 2|x_0|$, no interference between $2^{\ell_1+1} x_1 x_0$ and $x_0^2$.

If $2\ell_1 > \ell_1 + 1 + |x_1| + |x_0|$, no interference between $x_1^2$ and $2^{\ell_1+1} x_1 x_0$. 

Pierre Popoli

On the binary digits of $n$ and $n^2$
Write $n = 2^{\ell_0} x_m + \cdots + 2^{\ell_1} x_1 + x_0$ such that

$$(n)_2 = (x_m)_2 0 \cdots 0 (x_{m-1})_2 \cdots (x_1)_2 0 \cdots 0 (x_0)_2, \, \eta_i \geq 0.$$ 

→ Not unique decomposition.

- For $m = 1$, $n^2 = 2^{2\ell_1} x_1^2 + 2^{\ell_1+1} x_1 x_0 + x_0^2$.

$$(x_0^2)_2$$

$$(x_1 x_0)_2$$

$$(x_1^2)_2$$

$|x|$ denotes the binary length of $x$.

If $\ell_1 + 1 > 2|x_0|$, no interference between $2^{\ell_1+1} x_1 x_0$ and $x_0^2$.

If $2\ell_1 > \ell_1 + 1 + |x_1| + |x_0|$, no interference between $x_1^2$ and $2^{\ell_1+1} x_1 x_0$.

In this case, $n^2$ is composed of three independent blocks.
For $m = 2$, we have

$$n = 2^\ell_2 x_2 + 2^\ell_1 x_1 + x_0.$$  
$$n^2 = 2^{2\ell_2} x_2^2 + 2^{\ell_2 + \ell_1 + 1} x_2 x_1 + 2^{2\ell_1} x_1^2 + 2^{\ell_2 + 1} x_2 x_0 + 2^{\ell_1 + 1} x_1 x_0 + x_0^2.$$  

Potential interference **even if** $\ell_i$ large enough.
For $m = 2$, we have

$$n = 2^{\ell_2}x_2 + 2^{\ell_1}x_1 + x_0.$$  

$$n^2 = 2^{2\ell_2}x_2^2 + 2^{\ell_2 + \ell_1 + 1}x_2x_1 + 2^{2\ell_1}x_1^2 + 2^{\ell_2 + 1}x_2x_0 + 2^{\ell_1 + 1}x_1x_0 + x_0^2.$$  

Potential interference even if $\ell_i$ large enough.
Interference graph
Graphs for $m = 1$ and $m = 2$

Figure: Interference graph for $m = 1$.

Figure: Interference graph for $m = 2$. 
For $m = 3$, we have

\[
n = 2^{\ell^3} x_3 + 2^{\ell^2} x_2 + 2^{\ell^1} x_1 + x_0.
\]

\[
n^2 = 2^{2\ell^3} x_3^2 + 2^{\ell^3+\ell^2+1} x_3 x_2 + \cdots + 2^{\ell^1+1} x_1 x_0 + x_0^2.
\]

9 blocks and 5 potential interferences if $\ell_i$ large enough.

Figure: Interference graph for $m = 3$. 
Factorization lemma

For $k \geq 1$, there exists $N_k$ such that every odd integer $n \geq N_k$ with $s(n) = s(n^2) = k$ can be factorized

\[(n)_2 = (x_m)_2 \eta_m (x_{m-1})_2 \cdots (x_1)_2 \eta_1 (x_0)_2,\]

with $\min(\eta_i) > 2 \max(|x_i|) + k^2$.

Useful to
- prove that there is finitely many solutions.
- find easily infinite families of solutions.
Factorization lemma

For $k \geq 1$, there exists $N_k$ such that every odd integer $n \geq N_k$ with $s(n) = s(n^2) = k$ can be factorized

$$(n)_2 = (x_m)_20^{\eta_m}(x_{m-1})_2 \cdots (x_1)_20^{\eta_1}(x_0)_2,$$

with $\min(\eta_i) > 2 \max(|x_i|) + k^2$.

Useful to

- prove that there is finitely many solutions.
- find easily infinite families of solutions.

The bound $N_k$ is very large: $N_9 = 2^{611,669}$. 
Suppose \( n \) is such that \( s(n) = s(n^2) = 11 \) and satisfies the factorization lemma. Distribute 11 1-bits in the 3 independent blocks. For example:

\[
\begin{align*}
\text{4} & & \text{3} & & \text{4} \\
 x_1^2 & & x_1 x_0 & & x_0^2 \\
\end{align*}
\]

\[
\begin{align*}
 s(x_1) + s(x_0) &= 11, \\
 s(x_1^2) &= 4, \\
 s(x_1 x_0) &= 3, \\
 s(x_0^2) &= 4.
\end{align*}
\]
Suppose \( n \) is such that \( s(n) = s(n^2) = 11 \) and satisfies the factorization lemma. Distribute 11 1-bits in the 3 independent blocks. For example:

\[
\begin{align*}
s(x_1) + s(x_0) &= 11, \\
0 &= 4, \\
0 &= 4.
\end{align*}
\]

**Lemma (Kaneko, Stoll, 2022)**

Let \( a, b \) be odd integers, \( s(a) = \ell, s(b) = m \geq 3 \).

\[
\begin{align*}
\text{if } s(ab) = 2 & \implies ab < 2^{2\ell m - 4}, \\
\text{if } s(ab) = 3 & \implies ab < 2^{4\ell m - 13}.
\end{align*}
\]

Computer research is sufficient: \( ab < 2^{107} \).
Suppose $n$ is such that $s(n) = s(n^2) = 11$ and satisfies the factorization lemma. Distribute 11 1-bits in the 3 independent blocks. For example:

\[
\begin{align*}
3 & \quad 4 & \quad 4 \\
\text{x}_1^2 & \quad \text{x}_1 \text{x}_0 & \quad \text{x}_0^2
\end{align*}
\]

\[
\begin{align*}
s(x_1) + s(x_0) &= 11, \\
s(x_1^2) &= 3, \\
s(x_1 \text{x}_0) &= 4, \\
s(x_0^2) &= 4,
\end{align*}
\]
Suppose \( n \) is such that \( s(n) = s(n^2) = 11 \) and satisfies the factorization lemma. Distribute 11 1-bits in the 3 independent blocks. For example:

\[
\begin{align*}
3 & \quad x_1^2 \\
4 & \quad x_1 x_0 \\
4 & \quad x_0^2
\end{align*}
\]

\[
\begin{aligned}
s(x_1) + s(x_0) &= 11, \\
s(x_1^2) &= 3, \\
s(x_1 x_0) &= 4, \\
s(x_0^2) &= 4,
\end{aligned}
\]

Computer research is no longer possible for \( s(x_1 x_0) = 4 \) since

**Lemma (Kaneko, Stoll, 2022)**

For all integers \( L \geq 1 \) there exist integers \( \ell, m \geq L \) such that there are infinitely many pairs \( (a, b) \) of positive odd integers with

\[
s(a) = \ell, \ s(b) = m, \ s(ab) = 4.
\]
Suppose \( n \) is such that \( s(n) = s(n^2) = 11 \) and satisfies the factorization lemma. Distribute 11 1-bits in the 3 independent blocks. For example:

\[
\begin{align*}
3 & \quad 4 & \quad 4 \\
\begin{array}{c}
3 \quad 4 \\
\end{array} & \quad \begin{array}{c}
4 \\
\end{array} & \quad \begin{array}{c}
4 \\
\end{array}
\end{align*}
\]

\[
\begin{align*}
s(x_1) + s(x_0) &= 11, \\
s(x_1^2) &= 3, \\
s(x_1x_0) &= 4, \\
s(x_0^2) &= 4.
\end{align*}
\]

Computer research is no longer possible for \( s(x_1x_0) = 4 \) since

**Lemma (Kaneko, Stoll, 2022)**

For all integers \( L \geq 1 \) there exist integers \( \ell, m \geq L \) such that there are infinitely many pairs \((a, b)\) of positive odd integers with

\[
s(a) = \ell, \quad s(b) = m, \quad s(ab) = 4.
\]

**Focus** on solutions of \( s(n^2) = k \) for small \( k \geq 2 \).
Summary

1 Introduction

2 Interference graph

3 Few binary digits

4 Algorithm

5 Open questions
Few binary digits

Results

\[ E_k := \{ n \in \mathbb{N} : s(n^2) = k, n \text{ odd} \}. \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
</tbody>
</table>
Few binary digits

Results

\[ E_k := \{ n \in \mathbb{N} : s(n^2) = k, \text{ } n \text{ odd} \} . \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
<tr>
<td>3</td>
<td>{7, 23} \cup F, \text{ } F \text{ infinite family.}</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\( E_k := \{ n \in \mathbb{N} : s(n^2) = k, n \text{ odd} \} \).

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
<tr>
<td>3</td>
<td>{7, 23} \cup F, \text{Szalay (2002).}</td>
</tr>
<tr>
<td></td>
<td>F infinite family. for all ( n \in F, s(n) = 2 ).</td>
</tr>
<tr>
<td></td>
<td>( \rightarrow \text{Beukers result on the RN equation.} )</td>
</tr>
<tr>
<td>4</td>
<td>\text{Finite set.} Bennett, Bugeaud, Mignotte (2012).</td>
</tr>
<tr>
<td></td>
<td>( \rightarrow \text{Linear forms in logarithms.} )</td>
</tr>
</tbody>
</table>
\[ E_k := \{ n \in \mathbb{N} : s(n^2) = k, \text{n odd}\}. \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
<tr>
<td>3</td>
<td>{7, 23} \cup F, Szalay (2002).</td>
</tr>
<tr>
<td></td>
<td>( F ) infinite family. for all ( n \in F, s(n) = 2. )</td>
</tr>
<tr>
<td></td>
<td>( \rightarrow ) Beukers result on the RN equation.</td>
</tr>
<tr>
<td></td>
<td>( \rightarrow ) Linear forms in logarithms.</td>
</tr>
<tr>
<td></td>
<td>{13, 15, 47, 111} Conjecture (2012), still open.</td>
</tr>
</tbody>
</table>
Few binary digits

Results

\[ E_k := \{ n \in \mathbb{N} : s(n^2) = k, n \text{ odd} \}. \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
</tbody>
</table>
| 3 | \{7, 23\} \cup F, F \text{ infinite family.} | Szalay (2002).
| | for all \( n \in F, s(n) = 2. \) | → Beukers result on the RN equation. |
| 4 | \text{Finite set.} | Bennett, Bugeaud, Mignotte (2012).
| | \{13, 15, 47, 111\} | → Linear forms in logarithms.
| | Conjecture (2012), still open. |
| 5 | \( F_1 \cup F_2 \cup F_3 \cup E'_5, \) F\text{\textsubscript{i} infinite families,} E\text{\textsubscript{5} finite set.} | Aloui, Jamet, Kaneko, Kopecki, P., Stoll (2023)
| | for all \( n \in F_i, s(n) = 3. \) | → Combinatorial tools. |
### Results

\[ E_k := \{ n \in \mathbb{N} : s(n^2) = k, \text{ } n \text{ odd} \}. \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( E_k )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{1}</td>
</tr>
<tr>
<td>2</td>
<td>{3}</td>
</tr>
<tr>
<td>3</td>
<td>{7, 23} \cup F, \text{ } F \text{ infinite family.} \text{ } \text{Szalay (2002).} \text{ } \text{for all } n \in F, s(n) = 2. \text{ } \rightarrow \text{ Beukers result on the RN equation.}</td>
</tr>
<tr>
<td>4</td>
<td>\text{Finite set.} \text{ } \text{Bennett, Bugeaud, Mignotte (2012).} \text{ } \text{} \text{→ Linear forms in logarithms.} \text{ } \text{{13, 15, 47, 111}} \text{ } \text{Conjecture (2012), still open.}</td>
</tr>
<tr>
<td>5</td>
<td>\text{( F_1 \cup F_2 \cup F_3 \cup E'_5, \text{ } F_i \text{ infinite families,} \text{ } \text{( E'_5 \text{ finite set.} \text{ } \text{( E'_5 = {29, \ldots, 5793}. \text{ } \text{Conjecture (2023) } ) } ) } ) }</td>
</tr>
</tbody>
</table>
Few binary digits
Distribution for 11 bits: Example 2

\[
\begin{array}{c}
3 \\
\times_1^2 \\
4 \\
\times_{1x0} \\
4 \\
\times_0^2
\end{array}
\]

\[
\begin{cases}
s(x_1) + s(x_0) = 11, \\
s(x_1^2) = 3, \\
s(x_{1x0}) = 4, \\
s(x_0^2) = 4.
\end{cases}
\]

**Problem:** All solutions of \( s(x_0^2) = 4 \) are not known.
Few binary digits
Distribution for 11 bits: Example 2

\[
\begin{align*}
&3 \\
\circ & x_1^2 \quad & 4 \\
\circ & x_1 x_0 \quad & 4 \\
\circ & x_0^2
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
s(x_1) + s(x_0) &= 11, \\
s(x_1^2) &= 3, \\
s(x_1 x_0) &= 4, \\
s(x_0^2) &= 4.
\end{cases}
\end{align*}
\]

**Problem:** All solutions of \(s(x_0^2) = 4\) are not known.

But, we only need integers of \(E_4\) with **bounded** sum of digits.

\[
E_{k, \lambda} := \{n \in \mathbb{N} : s(n^2) = k, s(n) = \lambda, \ n \ \text{odd}\}, \quad E_k = \bigcup_{\lambda \geq 1} E_{k, \lambda}.
\]
Few binary digits
Distribution for 11 bits: Example 2

\[ \begin{array}{ccc}
3 & 4 & 4 \\
\circ x_1^2 & \circ x_1 x_0 & \circ x_0^2
\end{array} \]

\[ \begin{align*}
s(x_1) + s(x_0) &= 11, \\
s(x_1^2) &= 3, \\
s(x_1 x_0) &= 4, \\
s(x_0^2) &= 4.
\end{align*} \]

**Problem:** All solutions of \( s(x_0^2) = 4 \) are not known.

But, we only need integers of \( E_4 \) with **bounded** sum of digits.

\[ E_k,\lambda := \{ n \in \mathbb{N} : s(n^2) = k, s(n) = \lambda, \text{ } n \text{ odd} \}, \quad E_k = \bigcup_{\lambda \geq 1} E_k,\lambda. \]

**Theorem (Aloui, Jamet, Kaneko, Kopecki, P., Stoll, 2023)**

\[ \bigcup_{1 \leq \lambda \leq 17} E_4,\lambda = \{13, 15, 47, 111\}. \]

**Proof:** By an algorithm that constructs all possible solutions for a given weight.

Supports the conjecture \( E_4 = \{13, 15, 47, 111\} \) since \( s(111) = 6. \)
Few binary digits
Distribution for 11 bits: Example 2

\[
\begin{align*}
3 & \quad 4 & \quad 4 \\
x_1^2 & \quad x_1x_0 & \quad x_0^2
\end{align*}
\]

\[
\begin{cases}
\quad s(x_1) + s(x_0) = 11, \\
\quad s(x_1^2) = 3, \\
\quad s(x_1x_0) = 4, \\
\quad s(x_0^2) = 4.
\end{cases}
\]

\[
\implies \begin{cases}
\quad s(x_0) + s(x_1) = 11 \\
\quad x_1 \in \{7, 23\}, \text{ or } x_1 = 2^\ell + 1, \ell \geq 2. \\
\quad s(x_1x_0) = 4, \\
\quad x_0 \in \{13, 15, 47, 111\}.
\end{cases}
\]

Then \( s(x_0) + s(x_1) \leq 4 + 6 < 11 \implies \) no solution for this distribution of digits.
Few binary digits
Distribution for 11 bits: Example 3

\[ \begin{array}{ccc}
2 & 4 & 5 \\
\times_1^2 & \times_1 \times_0 & \times_0^2 \\
\end{array} \]

\[ \begin{align*}
& s(x_1) + s(x_0) = 11, \\
& s(x_1^2) = 2, \\
& s(x_1 \times_0) = 4, \\
& s(x_0^2) = 5.
\end{align*} \]

Same problem for solutions of \( s(x_0^2) = 5 \).

**Theorem (Aloui, Jamet, Kaneko, Kopecki, P., Stoll, 2023)**

\[ \bigcup_{4 \leq \lambda \leq 15} E_{5,\lambda} = \{29, 31, 51, 79, 91, 95, 157, 223, 279, 479, 727, 1471, 5793\}. \]

→ This set is the conjectured set for \( E_5' \).
Few binary digits
Distribution for 11 bits: Example 3

\[
\begin{align*}
2 & \quad 4 & \quad 5 \\
\times_1^2 & \quad \times_1 \times_0 & \quad \times_0^2
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
\quad s(x_1) + s(x_0) = 11, \\
\quad s(x_1^2) = 2, \\
\quad s(x_1 x_0) = 4, \\
\quad s(x_0^2) = 5.
\end{cases}
\end{align*}
\]

Same problem for solutions of \(s(x_0^2) = 5\).

\textbf{Theorem (Aloui, Jamet, Kaneko, Kopecki, P., Stoll, 2023)}

\[
\bigcup_{4 \leq \lambda \leq 15} E_{5,\lambda} = \{29, 31, 51, 79, 91, 95, 157, 223, 279, 479, 727, 1471, 5793\}.
\]

→ This set is the conjectured set for \(E_{5}'\).

\[
\begin{align*}
\begin{cases}
\quad s(x_0) + s(x_1) = 11, \\
\quad x_1 = 3, \\
\quad s(x_1 x_0) = 4, \\
\quad x_0 \in \{29, 31, \ldots, 1471, 5793\}.
\end{cases}
\end{align*}
\]

\[
\quad \implies \quad s(x_0) = 9 \text{ and } x_0 = 1471.
\]

Since \(s(3 \cdot 1471) = 7 > 4\), there is no solution for this distribution of digits.
Theorem (Aloui, Jamet, Kaneko, Kopecki, P., Stoll, 2023)

If $9 \leq k \leq 11$, (2) has finitely many solutions.

Proof

- Fix $k$ and consider $n$ that satisfies the factorization lemma for some $m \leq k$.
- Finite number of distribution of digits for each $m$.
- Prove that all of them leads to a contradiction.
Summary

1. Introduction
2. Interference graph
3. Few binary digits
4. Algorithm
5. Open questions
Suppose that \( n = 1 + 2^\ell y, \) \( y \) odd, \( \ell \geq 1, \) such that \( s(n^2) = 4. \)

\[
\begin{align*}
s(1 + 2^{\ell+1} y + 2^{2\ell} y^2) &= 4, \\
s(y + 2^{\ell-1} y^2) &= 3.
\end{align*}
\]
Suppose that $n = 1 + 2^\ell y$, $y$ odd, $\ell \geq 1$, such that $s(n^2) = 4$.

\[
s(1 + 2^{\ell+1} y + 2^{2\ell} y^2) = 4, \\
s(y + 2^{\ell-1} y^2) = 3.
\]
Suppose that \( n = 1 + 2^\ell y, \ y \text{ odd}, \ \ell \geq 1, \) such that \( s(n^2) = 4. \)

\[
\begin{align*}
  s(1 + 2^{\ell+1} y + 2^{2\ell} y^2) &= 4, \\
  s(y + 2^{\ell-1} y^2) &= 3.
\end{align*}
\]

Extending \( y \) with 1 does not change \( y_2. \)

For odd integers \( a, b, \)

\[
a \equiv b \pmod{2^\lambda} \implies a^2 \equiv b^2 \pmod{2^{\lambda+1}}.
\]
Suppose that \( n = 1 + 2^\ell y \), \( y \) odd, \( \ell \geq 1 \), such that \( s(n^2) = 4 \).

\[
\begin{align*}
 s(1 + 2^{\ell+1} y + 2^{2\ell} y^2) &= 4, \\
 s(y + 2^{\ell-1} y^2) &= 3.
\end{align*}
\]

Extending \( y \) with 0 does not change \( y_2 \).

For odd integers \( a, b \),

\[
a \equiv b \pmod{2^\lambda} \implies a^2 \equiv b^2 \pmod{2^{\lambda+1}}.
\]
Start from a candidate $y$ and extend $y$ on the left by
- a 1: finite number of extension since $s(y) \leq k - 1$ by hypothesis.
- a 0: not a too large block of consecutive 0, otherwise too many digits in the sum.

$\implies$ Finite number of possible extensions.

If the algorithm ends, it gives all solutions to $s(n^2) = 4$ and $s(n) = k$. 
Start from a candidate $y$ and extend $y$ on the left by
- a 1: finite number of extension since $s(y) \leq k - 1$ by hypothesis.
- a 0: not a too large block of consecutive 0, otherwise too many digits in the sum.

$\implies$ Finite number of possible extensions.

If the algorithm ends, it gives all solutions to $s(n^2) = 4$ and $s(n) = k$.

<table>
<thead>
<tr>
<th>$k$</th>
<th>Computation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1 sec</td>
</tr>
<tr>
<td>16</td>
<td>102 sec</td>
</tr>
<tr>
<td>17</td>
<td>2h50 mn</td>
</tr>
</tbody>
</table>

$\bigcup_{1 \leq \lambda \leq 17} E_{4,\lambda} = \{13, 15, 47, 111\}$.  

Pierre Popoli  On the binary digits of $n$ and $n^2$
Start from a candidate \( y \) and extend \( y \) on the left by
- a 1: finite number of extension since \( s(y) \leq k - 1 \) by hypothesis.
- a 0: not a too large block of consecutive 0, otherwise too many digits in the sum.

\[ \rightarrow \] Finite number of possible extensions.

If the algorithm ends, it gives all solutions to \( s(n^2) = 4 \) and \( s(n) = k \).

<table>
<thead>
<tr>
<th>( k )</th>
<th>Computation time</th>
<th>( \bigcup_{1 \leq \lambda \leq 17} E_{4,\lambda} = {13, 15, 47, 111} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1 sec</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>102 sec</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>2h50 mn</td>
<td></td>
</tr>
</tbody>
</table>

We also have

\[ \bigcup_{4 \leq \lambda \leq 15} E_{5,\lambda} = \{29, 31, 51, 79, 91, 95, 157, 223, 279, 479, 727, 1471, 5793\} \]
Summary

1 Introduction

2 Interference graph

3 Few binary digits

4 Algorithm

5 Open questions
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2) \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>( &lt; \infty )</td>
<td>( &lt; \infty )</td>
<td>( \infty )</td>
<td>?</td>
<td>( \infty )</td>
</tr>
</tbody>
</table>
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \] \hspace{1cm} (2)

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>(&lt; \infty)</td>
<td>(&lt; \infty)</td>
<td>(\infty)</td>
<td>?</td>
<td>(\infty)</td>
</tr>
</tbody>
</table>

“Natural” conjecture

For \( k = 14, 15 \), (2) has **infinitely** many solutions.
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2) \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>(&lt; \infty )</td>
<td>(&lt; \infty )</td>
<td>( \infty )</td>
<td>?</td>
<td>( \infty )</td>
</tr>
</tbody>
</table>

“Natural” conjecture
For \( k = 14, 15 \), (2) has infinitely many solutions.

→ Global research of every odd integer \( n \) such that \( s(n) = s(n^2) = k, \quad n \leq 2^{80} \).

Number of integers to check: \( \binom{79}{k-1} \) very large.
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad (2) \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>(&lt; \infty)</td>
<td>(&lt; \infty)</td>
<td>(\infty)</td>
<td>?</td>
<td>(\infty)</td>
</tr>
</tbody>
</table>

“Natural” conjecture

For \( k = 14, 15 \), (2) has infinitely many solutions.

→ Global research of every odd integer \( n \) such that \( s(n) = s(n^2) = k, \quad n \leq 2^{80} \).

Number of integers to check: \( \binom{79}{k-1} \) very large.

Parallelize the program.

Set up the first four nonzero bits of \( n \):

\[ n = 1 + 2^a + 2^b + 2^c + y, \quad 1 \leq a < b < c, \quad 2^c < y \leq 2^{80}. \]

Number of integers to check: \( \binom{79-c}{k-4} \) smaller but large number of cases.
\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \quad \tag{2} \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>(&lt; \infty)</td>
<td>(&lt; \infty)</td>
<td>(\infty)</td>
<td>(?)</td>
<td>(\infty)</td>
</tr>
</tbody>
</table>

→ Global research of every odd integer \( n \) such that \( s(n) = s(n^2) = k \), \( n \leq 2^{80} \).

- For \( k = 11 \), the largest solution is \( n = 35463511416833 \) of binary length 46.
- For \( k = 14, 15 \), we have solutions of binary length 80, for example:
  \[ n = 605643510452789079965697 \] satisfies \( s(n) = s(n^2) = 14 \).
  \[ n = 605642350760526229274625 \] satisfies \( s(n) = s(n^2) = 15 \).
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd}. \]  \hspace{1cm} (2)

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>(&lt; \infty)</td>
<td>(&lt; \infty)</td>
<td>(\infty)</td>
<td>?</td>
<td>(\infty)</td>
</tr>
</tbody>
</table>

→ Global research of every odd integer \( n \) such that \( s(n) = s(n^2) = k \), \( n \leq 2^{80} \).

- For \( k = 11 \), the largest solution is \( n = 35463511416833 \) of binary length 46.

- For \( k = 14, 15 \), we have solutions of binary length 80, for example:
  \[ n = 605643510452789079965697 \] satisfies \( s(n) = s(n^2) = 14 \).
  \[ n = 605642350760526229274625 \] satisfies \( s(n) = s(n^2) = 15 \).

But no obvious infinite family.

Conjecture
For \( k = 14, 15 \), (2) has finitely many solutions.
Open questions
Remaining cases of (2)

\[ s(n) = s(n^2) = k, \quad n \text{ odd.} \tag{2} \]

<table>
<thead>
<tr>
<th>( k )</th>
<th>1–8</th>
<th>9–11</th>
<th>12–13</th>
<th>14–15</th>
<th>( \geq 16 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>( &lt; \infty )</td>
<td>( &lt; \infty )</td>
<td>( \infty )</td>
<td>?</td>
<td>( \infty )</td>
</tr>
</tbody>
</table>

→ Global research of every odd integer \( n \) such that \( s(n) = s(n^2) = k, \quad n \leq 2^{80} \).

- For \( k = 11 \), the largest solution is \( n = 35463511416833 \) of binary length 46.

- For \( k = 14, 15 \), we have solutions of binary length 80, for example:
  
  \[ n = 605643510452789079965697 \text{ satisfies } s(n) = s(n^2) = 14. \]
  
  \[ n = 605642350760526229274625 \text{ satisfies } s(n) = s(n^2) = 15. \]

But no obvious infinite family.

Conjecture

For \( k = 14, 15 \), (2) has finitely many solutions.

Thank you for your attention!