The Physical Limits of Computation Inspire an Open Problem
That Concerns Abstract Computable Sets $X \subseteq \mathbb{N}$ and Cannot
Be Formalized in ZFC as It Refers to Our Current
Knowledge on $X$

Agnieszka Kozdéba, Apoloniusz Tyszka

Abstract. Open Problem: Is there a set $X \subseteq \mathbb{N}$ that satisfies conditions (1)-(5)?
(1) There are many elements of $X$ and it is conjectured that $X$ is infinite. (2) No
known algorithm decides the finiteness/infiniteness of $X$. (3) There is a known algo-
rithm that for every $k \in \mathbb{N}$ decides whether or not $k \in X$. (4) There is a known algo-
rithm that computes an integer $n$ satisfying $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$. (5) There is
a naturally defined condition $C$, which can be formalized in ZFC, such that for all ex-
cept at most finitely many $k \in \mathbb{N}$, $k$ satisfies the condition $C$ if and only if $k \in X$. The
simplest known such condition $C$ defines in $\mathbb{N}$ the set $X$. There is a set $X \subseteq \mathbb{N}$ that sat-
isfies conditions (1)-(5) except the requirement that $X$ is naturally defined. Let $P_{n^2+1}$
denote the set of primes of the form $n^2 + 1$. We heuristically prove the following state-
ment $\Phi$: $\text{card}(P_{n^2+1}) < \omega \Rightarrow P_{n^2+1} \subseteq (-\infty, ((24!)!)!)]$. This proof does not argue that $\text{card}(P_{n^2+1}) = \omega$. The statement $\Phi$ implies that the set $X = \{1\} \cup P_{n^2+1}$ satisfies conditions (1)-(5). If we ignore the physical limits of computation, then no set $X \subseteq \mathbb{N}$ will satisfy conditions (1)-(4) forever.

2020 Mathematics Subject Classification: 03D20.

Key words and phrases: computable set $X \subseteq \mathbb{N}$, conjecturally infinite set $X \subseteq \mathbb{N}$, cur-
rent knowledge on $X$, naturally defined set $X \subseteq \mathbb{N}$, no known algorithm decides the finite-
ness/infiniteness of $X$, physical limits of computation, primes of the form $n^2 + 1$.

1. Basic definitions

Definition 1. We say that an integer $n$ is a threshold number of a set $X \subseteq \mathbb{N}$, if $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$, cf. [6] and [7].

If a set $X \subseteq \mathbb{N}$ is empty or infinite, then any integer $n$ is a threshold number of $X$. If a set $X \subseteq \mathbb{N}$ is non-empty and finite, then the all threshold numbers of $X$ form the set $[\text{max}(X), \infty) \cap \mathbb{N}$.

Edmund Landau’s conjecture states that the set $P_{n^2+1}$ of primes of the form $n^2 + 1$ is infinite, see [3]–[5].

Definition 2. Let $\Phi$ denote the following unproven statement:

$$\text{card}(P_{n^2+1}) < \omega \Rightarrow P_{n^2+1} \subseteq (-\infty, ((24!)!)!])$$

Landau’s conjecture implies the statement $\Phi$. In Section [4] we heuristically prove the statement $\Phi$. This proof does not argue that $\text{card}(P_{n^2+1}) = \omega$.

Statement 1. No known algorithm computes an integer $k$ such that

$$\text{card}(P_{n^2+1}) < \omega \Rightarrow P_{n^2+1} \subseteq (-\infty, k]$$
Proving the statement $\Phi$ will disprove Statement 1. Statement 1 cannot be formalized in ZFC because it refers to the current mathematical knowledge. The same is true for Statements 2–4 in the next sections.

**Definition 3.** Conditions (1)–(5) concern sets $X \subseteq \mathbb{N}$.

(1) *There are many elements of $X$ and it is conjectured that $X$ is infinite.*
(2) *No known algorithm decides the finiteness/infiniteness of $X$.*
(3) *There is a known algorithm that for every $k \in \mathbb{N}$ decides whether or not $k \in X$.*
(4) *There is a known algorithm that computes an integer $n$ satisfying $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$.*
(5) *There is a naturally defined condition $C$, which can be formalized in ZFC, such that for all except at most finitely many $k \in \mathbb{N}$, $k$ satisfies the condition $C$ if and only if $k \in X$. The simplest known such condition $C$ defines in $\mathbb{N}$ the set $X$."

**Open Problem 1.** Is there a set $X \subseteq \mathbb{N}$ that satisfies conditions (1)–(5)?

Open Problem 1, which concerns abstract computable sets $X \subseteq \mathbb{N}$, represents an open problem in computability theory that cannot be formalized in ZFC and is related to fundamental concepts of arithmetic.

2. **Open Problem and the Physical Limits of Computation**

**Definition 4.** Let $\beta = (((24!)!)!)!$.

**Lemma 1.** $\log_2(\log_2(\log_2(\log_2(\log_2(\log_2(\log_2(\log_2(\beta))))))) \approx 1.42298$.

*Proof.* We ask Wolfram Alpha at [http://wolframalpha.com](http://wolframalpha.com) □

**Statement 2.** The set $X = \{ k \in \mathbb{N} : (\beta < k) \Rightarrow (\beta, k) \cap \mathcal{P}_{n^2+1} \neq \emptyset \}$

satisfies conditions (1)–(4).

*Proof.* Condition (1) holds as $X \supseteq \{0, \ldots, \beta\}$ and the set $\mathcal{P}_{n^2+1}$ is conjecturally infinite. By Lemma 1 due to known physics we are not able to confirm by a direct computation that some element of $\mathcal{P}_{n^2+1}$ is greater than $\beta$, see [2]. Thus condition (2) holds. Condition (3) holds trivially. Since the set $\{ k \in \mathbb{N} : (\beta < k) \land (\beta, k) \cap \mathcal{P}_{n^2+1} \neq \emptyset \}$ is empty or infinite, the integer $\beta$ is a threshold number of $X$. Thus condition (4) holds. □

Let $[\cdot]$ denote the integer part function. For a non-negative integer $n$, let $g(n)$ denote the greatest non-negative integer $k$ such that $2^k$ divides $\max\left\{2^\beta \cdot \left[\frac{x}{2}\right], 1\right\}$.

**Lemma 2.** The function $g : \mathbb{N} \to \mathbb{N}$ satisfies $g(0) = \ldots = g(\beta - 1) = 0$ and maps $\mathbb{N} \cap [\beta, \infty)$ onto itself taking every value in $\mathbb{N} \cap [\beta, \infty)$ infinitely many times.

**Statement 3.** The set $X = \{ n \in \mathbb{N} : g(n)^2 + 1 \text{ has no divisors greater than 1 and smaller than } g(n)^2 + 1 \}$

satisfies conditions (1)–(5) except the requirement that $X$ is naturally defined.

*Proof.* We use Lemma 2 and argue as in the proof of Statement □
Proving Landau’s conjecture will disprove Statements 2 and 3.

**Theorem 1.** No set $X \subseteq \mathbb{N}$ will satisfy conditions (1)–(4) forever, if for every algorithm with no inputs that operates on integers, at some future day, a computer will be able to execute this algorithm in 1 second or less.

**Proof.** The proof goes by contradiction. We fix an integer $n$ that satisfies condition (4). Since conditions (2)–(4) will hold forever, the semi-algorithm in Figure 1 never terminates and sequentially prints the following sentences:

\[(T) \quad n + 1 \notin X, \quad n + 2 \notin X, \quad n + 3 \notin X, \ldots\]

![Figure 1: Semi-algorithm that halts if and only if the set $X$ is infinite](image)

The sentences from the sequence (T) and our assumption imply that for every integer $m > n$ computed by a known algorithm, at some future day, a computer will be able to confirm in 1 second or less that $(n, m] \cap X = \emptyset$. Thus, at some future day, numerical evidence will support the conjecture that the set $X$ is finite, contrary to the conjecture in condition (1).

Physics disproves the assumption of Theorem 1.

3. Number-theoretic statements $\Psi_n$

Let $f(1) = 2$, $f(2) = 4$, and let $f(n + 1) = f(n)!$ for every integer $n \geq 2$. Let $\mathcal{U}_1$ denote the system of equations which consists of the equation $x_1! = x_1$. For an integer $n \geq 2$, let $\mathcal{U}_n$ denote the following system of equations:

\[
\begin{align*}
\forall i \in \{2, \ldots, n-1\} & \quad x_i! = x_{i+1} \\
x_1 \cdot x_2 & = x_3 \\
x_1 & = x_1
\end{align*}
\]
The diagram in Figure 2 illustrates the construction of the system $\mathcal{U}_n$.

**Fig. 2** Construction of the system $\mathcal{U}_n$

**Lemma 3.** For every positive integer $n$, the system $\mathcal{U}_n$ has exactly two solutions in positive integers, namely $(1, \ldots, 1)$ and $(f(1), \ldots, f(n))$.

Let $B_n$ denote the following system of equations:

$$\{x_i! = x_k : i, k \in \{1, \ldots, n\}\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$$

For a positive integer $n$, let $\Psi_n$ denote the following statement: if a system of equations $S \subseteq B_n$ has at most finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n) \leq f(n)$. The statement $\Psi_n$ says that for subsystems of $B_n$ with a finite number of solutions, the largest known solution is indeed the largest possible. The statements $\Psi_1$ and $\Psi_2$ hold trivially. There is no reason to assume the validity of the statement $\forall n \in \mathbb{N} \setminus \{0\} \Psi_n$.

**Theorem 2.** For every statement $\Psi_n$, the bound $f(n)$ cannot be decreased.

**Proof.** It follows from Lemma 3 because $\mathcal{U}_n \subseteq B_n$. □

**Theorem 3.** For every integer $n \geq 2$, the statement $\Psi_{n+1}$ implies the statement $\Psi_n$.

**Proof.** If a system $S \subseteq B_n$ has at most finitely many solutions in positive integers $x_1, \ldots, x_n$, then for every integer $i \in \{1, \ldots, n\}$ the system $S \cup \{x_i! = x_{n+1}\}$ has at most finitely many solutions in positive integers $x_1, \ldots, x_{n+1}$. The statement $\Psi_{n+1}$ implies that $x_i! = x_{n+1} \leq f(n+1) = f(n)!$. Hence, $x_i \leq f(n)$. □

**Theorem 4.** Every statement $\Psi_n$ is true with an unknown integer bound that depends on $n$.

**Proof.** For every positive integer $n$, the system $B_n$ has a finite number of subsystems. □

### 4. A conjectural solution to Open Problem 1

**Lemma 4.** For every positive integers $x$ and $y$, $x! \cdot y = y!$ if and only if

$$(x + 1 = y) \lor (x = y = 1)$$

**Lemma 5.** (Wilson’s theorem, [1, p. 89]). For every integer $x \geq 2$, $x$ is prime if and only if $x$ divides $(x - 1)! + 1$.

Let $\mathcal{A}$ denote the following system of equations:

$$\begin{align*}
x_2! &= x_3 \\
x_3! &= x_4 \\
x_5! &= x_6 \\
x_8! &= x_9 \\
x_1 \cdot x_1 &= x_2 \\
x_3 \cdot x_5 &= x_6 \\
x_4 \cdot x_8 &= x_9 \\
x_5 \cdot x_7 &= x_8
\end{align*}$$

Lemma 4 and the diagram in Figure 3 explain the construction of the system $\mathcal{A}$.
Lemma 6. For every integer $x_1 \geq 2$, the system $\mathcal{A}$ is solvable in positive integers $x_2, \ldots, x_9$ if and only if $x_1^2 + 1$ is prime. In this case, the integers $x_2, \ldots, x_9$ are uniquely determined by the following equalities:

$$
\begin{align*}
  x_2 &= x_1^2, \\
  x_3 &= (x_1^2)! \\
  x_4 &= ((x_1^2)!)! \\
  x_5 &= x_1^2 + 1 \\
  x_6 &= (x_1^2 + 1)! \\
  x_7 &= (x_1^2)! + 1 \\
  x_8 &= (x_1^2)! + 1 \quad \text{or} \quad x_3 = x_8 = 1 \\
  x_9 &= ((x_1^2)! + 1)! 
\end{align*}
$$

Proof. By Lemma 4 for every integer $x_1 \geq 2$, the system $\mathcal{A}$ is solvable in positive integers $x_2, \ldots, x_9$ if and only if $x_1^2 + 1$ divides $(x_1^2)! + 1$. Hence, the claim of Lemma 6 follows from Lemma 5. □

Lemma 7. There are only finitely many tuples $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$, which solve the system $\mathcal{A}$ and satisfy $x_1 = 1$. This is true as every such tuple $(x_1, \ldots, x_9)$ satisfies $x_1, \ldots, x_9 \in \{1, 2\}$.

Proof. The equality $x_1 = 1$ implies that $x_3 = x_1 \cdot x_1 = 1$. Hence, $x_3 = x_2 = 1$. Therefore, $x_4 = x_3 = 1$. The equalities $x_9! = x_6$ and $x_5 = 1 \cdot x_5 = x_3 \cdot x_5 = x_6$ imply that $x_5, x_6 \in \{1, 2\}$. The equalities $x_9! = x_9$ and $x_8 = 1 \cdot x_8 = x_4 \cdot x_8 = x_9$ imply that $x_8, x_9 \in \{1, 2\}$. The equality $x_3 \cdot x_7 = x_8$ implies that $x_7 = \frac{x_8}{x_5} \in \left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right\} \cap \mathbb{N} = \{1, 2\}$. □

Conjecture 1. The statement $\Psi_9$ is true when is restricted to the system $\mathcal{A}$. 

Fig. 3 Construction of the system $\mathcal{A}$
Theorem 5. Conjecture [7] proves the following implication: if there exists an integer \( x_1 \geq 2 \) such that \( x_1^2 + 1 \) is prime and greater than \( f(7) \), then the set \( P_{n+1} \) is infinite.

Proof. Suppose that the antecedent holds. By Lemma 6, there exists a unique tuple \((x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^8\) such that the tuple \((x_1, x_2, \ldots, x_9)\) solves the system \( \mathcal{A} \). Since \( x_1^2 + 1 > f(7) \), we obtain that \( x_1^2 \geq f(7) \). Hence, \( (x_1^2)! \geq f(7)! = f(8) \). Consequently,

\[
x_9 = ((x_1^2)! + 1)! > (f(8) + 1)! > f(8)! = f(9)
\]

Conjecture [1] and the inequality \( x_9 > f(9) \) imply that the system \( \mathcal{A} \) has infinitely many solutions \((x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9\). According to Lemmas 6 and 7, the set \( P_{n+1} \) is infinite. \( \square \)

Theorem 6. Conjecture [7] implies the statement \( \Phi \).

Proof. It follows from Theorem 5 and the equality \( f(7) = (((24!)!)!)! \). \( \square \)

Theorem 7. The statement \( \Phi \) implies Conjecture [7]

Proof. By Lemmas 6 and 7 if positive integers \( x_1, \ldots, x_9 \) solve the system \( \mathcal{A} \), then

\[
(x_1 \geq 2) \land (x_5 = x_1^2 + 1) \land (x_5 \text{ is prime})
\]

or \( x_1, \ldots, x_9 \in \{1, 2\} \). In the first case, Lemma 9 and the statement \( \Phi \) imply that the inequality \( x_5 \leq (((24!)!)!)! = f(7) \) holds when the system \( \mathcal{A} \) has at most finitely many solutions in positive integers \( x_1, \ldots, x_9 \). Hence, \( x_2 = x_5 - 1 < f(7) \) and \( x_3 = x_2 < f(7)! = f(8) \). Continuing this reasoning in the same manner, we can show that every \( x_i \) does not exceed \( f(9) \). \( \square \)

Statement 4. The statement \( \Phi \) implies that the set \( \mathcal{X} = \{1\} \cup P_{n+1} \) satisfies conditions (1)–(5).

Proof. The set \( P_{n+1} \) is conjecturally infinite. There are 2199894223892 primes of the form \( n^2 + 1 \) in the interval \([2, 10^{28}]\), see [4]. These two facts imply condition (1). By Lemma 1 due to known physics we are not able to confirm by a direct computation that some element of \( \{1\} \cup P_{n+1} \) is greater than \( f(7) = (((24!)!)!)! = \beta \), see [2]. Thus condition (2) holds. Condition (3) holds trivially. The statement \( \Phi \) implies that \( \beta \) is a threshold number of \( \mathcal{X} = \{1\} \cup P_{n+1} \). Thus condition (4) holds. The following condition:

\[
k - 1 \text{ is a square and } k \text{ has no divisors greater than 1 and smaller than } k
\]

defines in \( \mathbb{N} \) the set \( \{1\} \cup P_{n+1} \). This proves condition (5). \( \square \)

Proving Landau’s conjecture will disprove Statement [4]

Acknowledgment. Agnieszka Kozdęba prepared three diagrams. Apoloniusz Tyszka wrote the article.

References


Agnieszka Kozdęba
University of Agriculture
Faculty of Environmental Engineering and Land Surveying
Balicka 253C, 30-198 Kraków, Poland

Apoloniusz Tyszka
University of Agriculture
Faculty of Production and Power Engineering
Balicka 116B, 30-149 Kraków, Poland
E-mail: rttyszka@cyf-kr.edu.pl