# On an informal condition $\Gamma(\mathcal{X})$ that refers to the current knowledge on a set $\mathcal{X} \subseteq \mathbb{N}$ and conjecturally holds for $\mathcal{X}$ being the set of primes of the form $n^2+1$, although the statement $\exists\, \mathcal{X} \subseteq \mathbb{N}\ \Gamma(\mathcal{X})$ (whose validity is unknown) is false for every subject which knows the output of every deterministic algorithm with no inputs

AGNIESZKA KOZDĘBA, APOLONIUSZ TYSZKA

Abstract. Let $f(1)=2$, $f(2)=4$, and let $f(n+1)=f(n)!$ for every integer $n \geqslant 2$. Edmund Landau's conjecture states that the set $\mathcal{P}_{n^2+1}$ of primes of the form $n^2+1$ is infinite. Landau's conjecture implies the following unproven statement $\Phi$: $\mathrm{card}(\mathcal{P}_{n^2+1}) < \omega \Rightarrow \mathcal{P}_{n^2+1} \subseteq (-\infty, f(7)]$. Let $B$ denote the system of equations: $\{x_i! = x_k :\ i,k \in \{1,\ldots,9\}\} \cup \{x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,9\}\}$. We write down a system $\mathcal{U} \subseteq B$ of 9 equations which has exactly two solutions in positive integers, namely $(1,\ldots,1)$ and $(f(1),\ldots,f(9))$. Let $\Psi$ denote the statement: *if a system $\mathcal{S} \subseteq B$ has at most finitely many solutions in positive integers $x_1,\ldots,x_9$, then each such solution $(x_1,\ldots,x_9)$ satisfies $x_1,\ldots,x_9 \leqslant f(9)$.* We write down a system $\mathcal{A} \subseteq B$ of 8 equations. The statement $\Psi$ restricted to the system $\mathcal{A}$ is equivalent to the statement $\Phi$. It heuristically proves the statement $\Phi$. This proof does not argue that $\mathrm{card}(\mathcal{P}_{n^2+1}) = \omega$. All algorithms are deterministic. Algorithms always terminate. We explain the distinction between *existing algorithms* (i.e. algorithms whose existence is provable in $ZFC$) and *known algorithms* (i.e. algorithms whose existence is constructive and currently known to us). Open Problem: *Is there a set $\mathcal{X} \subseteq \mathbb{N}$ that satisfies conditions* (1)-(5)*?* (1) *There are many elements of $\mathcal{X}$ and it is conjectured that $\mathcal{X}$ is infinite.* (2) *No known algorithm with no inputs decides the finiteness/infiniteness of $\mathcal{X}$. In particular, no known proof shows the finiteness/infiniteness of $\mathcal{X}$.* (3) *There is a known algorithm that for every $k \in \mathbb{N}$ decides whether or not $k \in \mathcal{X}$.* (4) *There is a known algorithm with no inputs that computes an integer $n$ satisfying* $\mathrm{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$. (5) *There is a known and 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 $k \in \mathcal{X}$. The simplest known such condition $C$ defines in $\mathbb{N}$ the set $\mathcal{X}$.* Condition (5) strengthens the condition that $\mathcal{X}$ is naturally defined. We define a set $\mathcal{X} \subseteq \mathbb{N}$. The set $\mathcal{X}$ satisfies conditions (1)-(5) except the requirement that $\mathcal{X}$ is naturally defined. The statement $\Phi$ implies that the set $\mathcal{X} = \{1\} \cup \mathcal{P}_{n^2+1}$ satisfies conditions (1)-(5). Proving Landau's conjecture will disprove the last two statements. No set $\mathcal{X} \subseteq \mathbb{N}$ will satisfy conditions (1)-(4) forever, if for every algorithm with no inputs, at some future day, a computer will be able to execute this algorithm in 1 second or less. The physical limits of computation disprove this assumption. The conjunction of conditions (1)-(5) is the condition $\Gamma(\mathcal{X})$ from the title.

**Key words and phrases:** computable set $\mathcal{X} \subseteq \mathbb{N}$, conjecturally infinite set $\mathcal{X} \subseteq \mathbb{N}$, current knowledge on $\mathcal{X}$, existing algorithms, known algorithms, naturally defined set $\mathcal{X} \subseteq \mathbb{N}$, no known algorithm with no inputs decides the finiteness/infiniteness of $\mathcal{X}$, no known proof shows the finiteness/infiniteness of $\mathcal{X}$, physical limits of computation, primes of the form $n^2+1$.

## 1. Definitions and the distinction between existing algorithms and known algorithms

All algorithms are deterministic. Algorithms always terminate. Semi-algorithms may not terminate.

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

(1) *There are many elements of* $\mathcal{X}$ *and it is conjectured that* $\mathcal{X}$ *is infinite.*

(2) *No known proof shows the finiteness/infiniteness of* $\mathcal{X}$. *No known algorithm with no inputs decides the finiteness/infiniteness of* $\mathcal{X}$.

(3) *There is a known algorithm that for every* $k \in \mathbb{N}$ *decides whether or not* $k \in \mathcal{X}$.

(4) *There is a known algorithm with no inputs that computes an integer* $n$ *satisfying* $\mathrm{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$.

(5) *There is a known and 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* $k \in \mathcal{X}$. *The simplest known such condition* $C$ *defines in* $\mathbb{N}$ *the set* $\mathcal{X}$.

Condition (5) strengthens the condition that $\mathcal{X}$ is naturally defined.

**Definition 2.** *Let* $\beta = (((24!)!)!)!$.

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

*Proof.* We ask Wolfram Alpha at `http://wolframalpha.com`. □

Edmund Landau's conjecture states that the set $\mathcal{P}_{n^2+1}$ of primes of the form $n^2 + 1$ is infinite, see [4]–[6]. Let $[\cdot]$ denote the integer part function.

**Example 1.** *The set* $\mathcal{X} = \mathcal{P}_{n^2+1}$ *satifies condition* (2).

**Example 2.** *The set* $\mathcal{X} = \begin{cases} \mathbb{N}, & \text{if } [\frac{\beta}{\pi}] \text{ is odd} \\ \emptyset, & \text{otherwise} \end{cases}$ *does not satisfy condition* (2) *because we know an algorithm with no inputs that computes* $[\frac{\beta}{\pi}]$.

**Example 3.** *(*[3]*). The function*

$$\mathbb{N} \ni n \xrightarrow{h} \begin{cases} 1, & \text{if the decimal expansion of } \pi \text{ contains } n \text{ consecutive zeros} \\ 0, & \text{otherwise} \end{cases}$$

*is computable because* $h = \mathbb{N} \times \{1\}$ *or there exists* $k \in \mathbb{N}$ *such that*

$$h = (\{0, \ldots, k\} \times \{1\}) \cup (\{k+1,\ k+2,\ k+3,\ \ldots\} \times \{0\})$$

*No known algorithm computes the function h.*

Examples 1–3 and the proof of Statement 1 explain the distinction between *existing algorithms* (i.e. algorithms whose existence is provable in $ZFC$) and *known algorithms* (i.e. algorithms whose existence is constructive and currently known to us).

**Definition 3.** *Let* $\Phi$ *denote the following unproven statement:*

$$\mathrm{card}(\mathcal{P}_{n^2+1}) < \omega \Rightarrow \mathcal{P}_{n^2+1} \subseteq (-\infty, \beta]$$

Landau's conjecture implies the statement $\Phi$. In Section 4, we heuristically prove the statement $\Phi$. This proof does not argue that $\mathrm{card}(\mathcal{P}_{n^2+1}) = \omega$.

**Statement 1.** *Condition* `(4)` *fails for* $\mathcal{X} = \mathcal{P}_{n^2+1}$.

*Proof.* For every set $\mathcal{X} \subseteq \mathbb{N}$, there exists an algorithm $\mathtt{Alg}(\mathcal{X})$ with no inputs that returns

$$n = \begin{cases} 0, & \text{if } \operatorname{card}(\mathcal{X}) \in \{0, \omega\} \\ \max(\mathcal{X}), & \text{otherwise} \end{cases}$$

This $n$ satisfies the implication in condition `(4)`, but the algorithm $\mathtt{Alg}(\mathcal{P}_{n^2+1})$ is unknown for us because its definition is ineffective. □

Proving the statement $\Phi$ will disprove Statement 1. Statement 1 cannot be formalized in mathematics because it refers to the current mathematical knowledge. The same is true for Statements 2–4 in the next sections.

**Definition 4.** *We say that an integer $n$ is a threshold number of a set $\mathcal{X} \subseteq \mathbb{N}$, if* $\operatorname{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$.

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

## 2. The physical limits of computation inspire Open Problem 1

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

**Statement 2.** *The set*

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

*satisfies conditions* `(1)-(4)`.

*Proof.* Condition `(1)` holds as $\mathcal{X} \supseteq \{0, \ldots, \beta\}$ 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

$$\{k \in \mathbb{N} : (\beta < k) \wedge (\beta, k) \cap \mathcal{P}_{n^2+1} \neq \emptyset\}$$

is empty or infinite, the integer $\beta$ is a threshold number of $\mathcal{X}$. Thus condition `(4)` holds. □

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

**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*

$$\mathcal{X} = \left\{n \in \mathbb{N} : g(n)^2 + 1 \textit{ has no divisors greater than } 1 \textit{ and smaller than } g(n)^2 + 1\right\}$$

*satisfies conditions* `(1)-(5)` *except the requirement that $\mathcal{X}$ is naturally defined.*

*Proof.* We use Lemma 2 and argue as in the proof of Statement 2. □

Proving Landau's conjecture will disprove Statements 2 and 3.

**Theorem 1.** *No set $\mathcal{X} \subseteq \mathbb{N}$ will satisfy conditions* (1)-(4) *forever, if for every algorithm with no inputs, 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 conditons (2)-(4) will hold forever, the semi-algorithm in Figure 1 never terminates and sequentially prints the following sentences:

(T) $$n+1 \notin \mathcal{X},\ n+2 \notin \mathcal{X},\ n+3 \notin \mathcal{X},\ \ldots$$

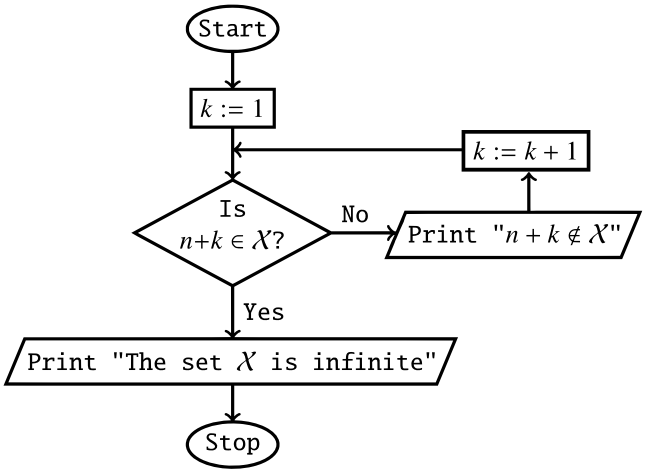


**Fig. 1** Semi-algorithm that terminates if and only if the set $\mathcal{X}$ is infinite

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 $(n, m] \cap \mathcal{X} = \emptyset$. Thus, at some future day, numerical evidence will support the conjecture that the set $\mathcal{X}$ is finite, contrary to the conjecture in condition (1). □

The physical limits of computation ([2]) disprove the assumption of Theorem 1. The conjunction of conditions (1)-(5) is the condition $\Gamma(\mathcal{X})$ from the article title.

## 3. Number-theoretic statements $\Psi_n$

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

$$\begin{cases} x_1! &= x_1 \\ x_1 \cdot x_1 &= x_2 \\ \forall i \in \{2, \ldots, n-1\}\ x_i! &= x_{i+1} \end{cases}$$

The diagram in Figure 2 illustrates the construction of the system $\mathcal{U}_n$.

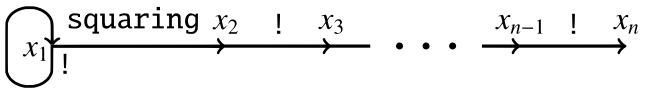


**Fig. 2** Construction of the system $\mathcal{U}_n$

**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:

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

For a positive integer $n$, let $\Psi_n$ denote the following statement: *if a system of equations $\mathcal{S} \subseteq B_n$ has at most finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leqslant f(n)$.* 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 $n \geqslant 2$, the statement $\Psi_{n+1}$ implies the statement $\Psi_n$.*

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

**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*

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

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

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

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

Lemma 4 and the diagram in Figure 3 explain the construction of the system $\mathcal{A}$.

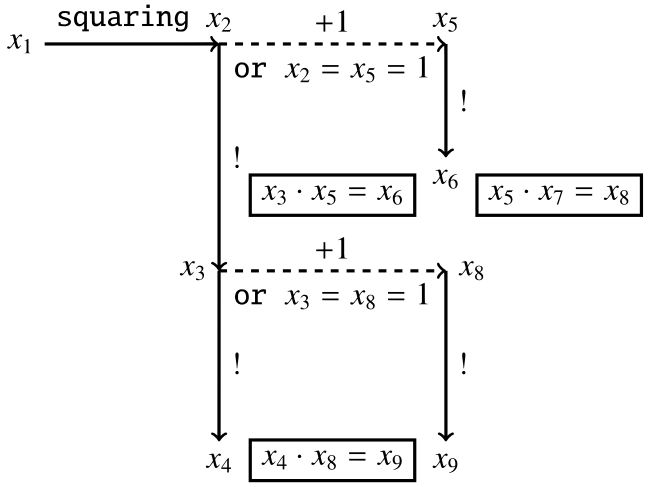


**Fig. 3** Construction of the system $\mathcal{A}$

**Lemma 6.** *For every integer $x_1 \geqslant 2$, 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:*

$$\begin{aligned}
x_2 &= x_1^2 \\
x_3 &= (x_1^2)! \\
x_4 &= ((x_1^2)!)! \\
x_5 &= x_1^2 + 1 \\
x_6 &= (x_1^2 + 1)! \\
x_7 &= \frac{(x_1^2)! + 1}{x_1^2 + 1} \\
x_8 &= (x_1^2)! + 1 \\
x_9 &= ((x_1^2)! + 1)!
\end{aligned}$$

*Proof.* By Lemma 4, for every integer $x_1 \geqslant 2$, 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 $x_2 = x_1 \cdot x_1 = 1$. Hence, $x_3 = x_2! = 1$. Therefore, $x_4 = x_3! = 1$. The equalities $x_5! = x_6$ 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 $x_8! = x_9$ 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 $x_5 \cdot x_7 = x_8$ implies that $x_7 = \frac{x_8}{x_5} \in \left\{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{2}{2}\right\} \cap \mathbb{N} = \{1, 2\}$. □

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

**Theorem 5.** *Conjecture 1 proves the following implication: if there exists an integer $x_1 \geqslant 2$ such that $x_1^2 + 1$ is prime and greater than $f(7)$, then the set $\mathcal{P}_{n^2+1}$ 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 $x_1^2 \geqslant f(7)$. Hence, $(x_1^2)! \geqslant f(7)! = f(8)$. Consequently,

$$x_9 = ((x_1^2)! + 1)! \geqslant (f(8) + 1)! > f(8)! = f(9)$$

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 $\mathcal{P}_{n^2+1}$ is infinite. □

**Theorem 6.** *Conjecture 1 implies the statement $\Phi$.*

*Proof.* It follows from Theorem 5 and the equality $f(7) = (((24!)!)!)!$. □

**Theorem 7.** *The statement $\Phi$ implies Conjecture 1.*

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

$$(x_1 \geqslant 2) \wedge (x_5 = x_1^2 + 1) \wedge (x_5 \text{ is prime})$$

or $x_1, \ldots, x_9 \in \{1, 2\}$. In the first case, Lemma 6 and the statement $\Phi$ imply that the inequality $x_5 \leqslant (((24!)!)!)! = f(7)$ 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 $f(9)$. □

**Statement 4.** *The statement $\Phi$ implies that the set $\mathcal{X} = \{1\} \cup \mathcal{P}_{n^2+1}$ satisfies conditions* `(1)-(5)`.

*Proof.* The set $\mathcal{P}_{n^2+1}$ is conjecturally infinite. There are 2199894223892 primes of the form $n^2 + 1$ in the interval $[2, 10^{28})$, see [5]. 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 $\{1\} \cup \mathcal{P}_{n^2+1}$ 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 $\mathcal{X} = \{1\} \cup \mathcal{P}_{n^2+1}$. Thus condition `(4)` holds. The following condition:

$$k - 1 \textit{ is a square and } k \textit{ has no divisors greater than } 1 \textit{ and smaller than } k$$

defines in $\mathbb{N}$ the set $\{1\} \cup \mathcal{P}_{n^2+1}$. This proves condition `(5)`. □

Proving Landau's conjecture will disprove Statement 4.

**Acknowledgement.** Agnieszka Kozdęba prepared three diagrams. Apoloniusz Tyszka wrote the article.

## References

[1] M. Erickson, A. Vazzana, D. Garth, *Introduction to number theory,* 2nd ed., CRC Press, Boca Raton, FL, 2016.

[2] S. Lloyd, *Ultimate physical limits to computation,* Nature 406 (2000), 1047–1054, http://doi.org/10.1038/35023282.

[3] R. Reitzig, *How can it be decidable whether $\pi$ has some sequence of digits?*, http://cs.stackexchange.com/questions/367/how-can-it-be-decidable-whether-pi-has-some-sequence-of-digits.

[4] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002496, Primes of the form $n^2 + 1$,* http://oeis.org/A002496.

[5] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A083844, Number of primes of the form $x^2 + 1 < 10^n$,* http://oeis.org/A083844.

[6] Wolfram MathWorld, *Landau's Problems,* http://mathworld.wolfram.com/LandausProblems.html.

Agnieszka Kozdęba
Institute of Mathematics
Jagiellonian University
Łojasiewicza 6, 30-348 Kraków, Poland
E-mail: Agnieszka.Kozdeba@im.uj.edu.pl

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 116B, 30-149 Kraków, Poland
E-mail: rttyszka@cyf-kr.edu.pl