THE PHYSICAL LIMITS OF COMPUTATION INSPIRE AN OPEN PROBLEM THAT CONCERNS ABSTRACT COMPUTABLE SETS $\mathcal{X} \subseteq \mathbb{N}$ AND CANNOT BE FORMALIZED IN ZFC AS IT REFERS TO OUR CURRENT KNOWLEDGE ON $\mathcal{X}$

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 Φ: $\mathrm{card}(\mathcal{P}_{n^2+1}) < \omega \Rightarrow \mathcal{P}_{n^2+1} \subseteq [2, f(7)]$. Let B denote the system of equations: $\left\{x_i! = x_k:\ i,k \in \{1,\ldots,9\}\right\} \cup \left\{x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,9\}\right\}$. 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 Ψ 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 Ψ restricted to the system $\mathcal{A}$ is equivalent to the statement Φ. This heuristically proves the statement Φ. This proof does not argue that $\mathrm{card}(\mathcal{P}_{n^2+1}) = \omega$. 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 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 that computes an integer n satisfying* $\mathrm{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$. `(5)` *There is a naturally defined condition $\mathcal{C}$, which can be formalized in ZFC, such that for all except at most finitely many $k \in \mathbb{N}$, k satisfies the condition $\mathcal{C}$ if and only if $k \in \mathcal{X}$. The simplest known such condition $\mathcal{C}$ defines in $\mathbb{N}$ the set $\mathcal{X}$.* Let $[\cdot]$ denote the integer part function. The set $\mathcal{X} = \mathrm{card}(\mathcal{P}_{n^2+1})$ satisfies condition `(2)`. The set $\mathcal{X} = \begin{cases} \mathbb{N} & \text{if } [f(7)/\pi] \text{ is odd} \\ \emptyset & \text{if } [f(7)/\pi] \text{ is even} \end{cases}$ does not satisfy condition `(2)` because we know an algorithm that theoretically computes $[f(7)/\pi]$. For every set $\mathcal{X} \subseteq \mathbb{N}$, there exists an algorithm $\mathtt{Alg}(\mathcal{X})$ that returns $n = \begin{cases} 0 & \text{if } \mathrm{card}(\mathcal{X}) \in \{0,\omega\} \\ \max(\mathcal{X}) & \text{if } \mathrm{card}(\mathcal{X}) \notin \{0,\omega\} \end{cases}$. 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. These three examples explain the distinction between existing algorithms and known algorithms. 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 Φ 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 that operates on integers, at some future day, a computer will be able to execute this algorithm in 1 second or less. Physics disproves this assumption.

2020 Mathematics Subject Classification: 03D20.

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 decides 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

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 algorithm 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 that computes an integer* n *satisfying* $\mathrm{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$.

`(5)` *There is a naturally defined condition* $\mathcal{C}$*, which can be formalized in ZFC, such that for all except at most finitely many* $k \in \mathbb{N}$*,* k *satisfies the condition* $\mathcal{C}$ *if and only if* $k \in \mathcal{X}$*. The simplest known such condition* $\mathcal{C}$ *defines in* $\mathbb{N}$ *the set* $\mathcal{X}$.

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 [3]–[5]. Let $[\cdot]$ denote the integer part function. The set $\mathcal{X} = \mathrm{card}(\mathcal{P}_{n^2+1})$ satifies condition `(2)`. The set $\mathcal{X} = \begin{cases} \mathbb{N} & \text{if } [\beta/\pi] \text{ is odd} \\ \emptyset & \text{if } [\beta/\pi] \text{ is even} \end{cases}$ does not satisfy condition `(2)` because we know an algorithm that theoretically computes $[\beta/\pi]$. These two examples explain the distinction between existing algorithms and known algorithms.

Definition 3. *Let* Φ *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 Φ. In Section 4, we heuristically prove the statement Φ. 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 $\mathtt{Alg}(\mathcal{X})$ that returns

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

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. □

The proof of Statement 1 explains the distinction between existing algorithms and known algorithms. Proving the statement Φ 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 4. *We say that an integer* n *is a threshold number of a set* $\mathcal{X} \subseteq \mathbb{N}$*, if* $\mathrm{card}(\mathcal{X}) < \omega \Rightarrow \mathcal{X} \subseteq (-\infty, n]$*, cf.* [6] *and* [7].

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)`*?*

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

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 β, 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 β 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 $\max(2^\beta \cdot [n/\beta], 1)$.

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*

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

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 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 conditons `(2)-(4)` will hold forever, the semi-algorithm in Figure 1 never terminates and sequentially prints the following sentences:

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

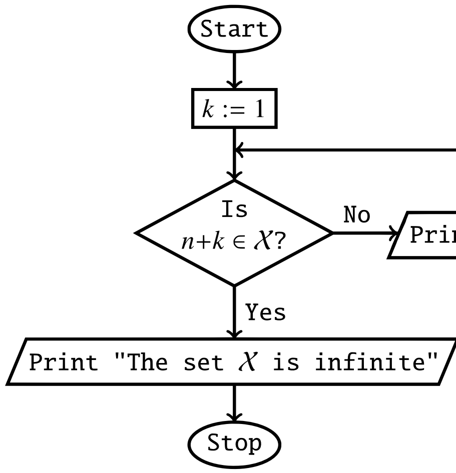

Fig. 1 Semi-algorithm that halts if and only if the set $\mathcal{X}$ is infinite

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). □

Physics disproves the assumption of Theorem 1.

3. Number-theoretic statements Ψ_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 $\mathcal{U}_n$.

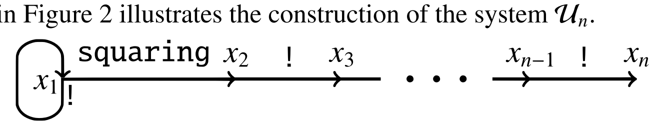

Fig. 2 Construction of the system $\mathcal{U}_n$

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:

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

For a positive integer n, let Ψ_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 Ψ_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 Ψ_1 and Ψ_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 Ψ_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 Ψ_{n+1} implies the statement Ψ_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 Ψ_{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 Ψ_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 $\mathcal{A}$.

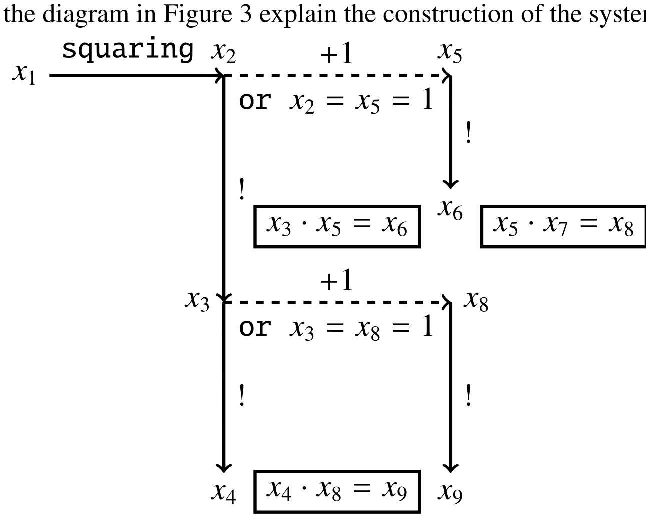

Fig. 3 Construction of the system $\mathcal{A}$

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:*

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

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 Ψ_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 Φ.*

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

Theorem 7. *The statement Φ 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 Φ 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 Φ 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 [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 $\{1\} \cup \mathcal{P}_{n^2+1}$ is greater than $f(7) = (((24!)!)!)! = \beta$, see [2]. Thus condition `(2)` holds. Condition `(3)` holds trivially. The statement Φ implies that β 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.

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

[4] 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`.

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

[6] A. A. Zenkin, *Super-induction method: logical acupuncture of mathematical infinity,* Twentieth World Congress of Philosophy, Boston, MA, August 10–15, 1998, `http://www.bu.edu/wcp/Papers/Logi/LogiZenk.htm`.

[7] A. A. Zenkin, *Superinduction: new logical method for mathematical proofs with a computer,* in: J. Cachro and K. Kijania-Placek (eds.), Volume of Abstracts, 11th International Congress of Logic, Methodology and Philosophy of Science, August 20–26, 1999, Cracow, Poland, p. 94, The Faculty of Philosophy, Jagiellonian University, Cracow, 1999.

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`