

**Are there a set  $X \subseteq \mathbb{N}$  and a constructively defined integer  $n$  such that  $(\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]) \wedge$  (a constructively defined algorithm decides  $X$ )  $\wedge$  (there are many elements of  $X$ )  $\wedge$  (the infiniteness of  $X$  is conjectured and cannot be decided by any known method)  $\wedge$  ( $X$  has the simplest definition among known sets  $\mathcal{Y} \subseteq \mathbb{N}$  with the same set of known elements)?**

AGNIESZKA KOZDĘBA, APOLONIUSZ TYSZKA

ABSTRACT. Let  $f(1) = 2$ ,  $f(2) = 4$ , and let  $f(n+1) = f(n)!$  for every integer  $n \geq 2$ . 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  $\Phi$ :  $\text{card}(\mathcal{P}_{n^2+1}) < \omega \Rightarrow \mathcal{P}_{n^2+1} \subseteq [2, f(7)]$ . Let  $B$  denote the system of equations:  $\{x_i! = x_k : i, k \in \{1, \dots, 9\}\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \dots, 9\}\}$ . We write down a system  $\mathcal{U} \subseteq B$  of 9 equations which has exactly two solutions in positive integers  $x_1, \dots, x_9$ , namely  $(1, \dots, 1)$  and  $(f(1), \dots, f(9))$ . We write down a system  $\mathcal{A} \subseteq B$  of 8 equations. Let  $\Lambda$  denote the statement: *if the system  $\mathcal{A}$  has at most finitely many solutions in positive integers  $x_1, \dots, x_9$ , then each such solution  $(x_1, \dots, x_9)$  satisfies  $x_1, \dots, x_9 \leq f(9)$* . The statement  $\Lambda$  is equivalent to the statement  $\Phi$ . It heuristically proves the statement  $\Phi$ . This proof does not yield that  $\text{card}(\mathcal{P}_{n^2+1}) = \omega$ . 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 definition is constructive and currently known to us). A definition of an integer  $n$  is called *constructive*, if it provides a known algorithm with no input that returns  $n$ . 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 with no input returns the logical value of the statement  $\text{card}(X) = \omega$ .* (3) *A known algorithm for every  $k \in \mathbb{N}$  decides whether or not  $k \in X$ .* (4) *A known algorithm with no input returns an integer  $n$  satisfying  $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$ .* (5)  *$X$  has the simplest definition among known sets  $\mathcal{Y} \subseteq \mathbb{N}$  with the same set of known elements.* The set  $X = \{k \in \mathbb{N} : (f(7) < k) \Rightarrow (f(7), k) \cap \mathcal{P}_{n^2+1} \neq \emptyset\}$  satisfies conditions (1)-(4) and does not satisfy condition (5). No set  $X \subseteq \mathbb{N}$  will satisfy conditions (1)-(4) forever, if for every algorithm with no input, 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. Conditions (1)-(3) and (5) hold for  $X = \mathcal{P}_{n^2+1}$ . The statement  $\Phi$  implies that condition (4) holds for  $X = \mathcal{P}_{n^2+1}$ .

**2020 Mathematics Subject Classification:** 03D20.

**Key words and phrases:** constructively defined integer  $n$  satisfies  $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$ , constructively defined algorithm, current knowledge on a set  $X \subseteq \mathbb{N}$ , decidable and conjecturally infinite set  $X \subseteq \mathbb{N}$ , distinction between existing algorithms and known algorithms, known elements of a set  $X \subseteq \mathbb{N}$ , physical limits of computation, primes of the form  $n^2 + 1$ .

## 1. DEFINITIONS AND THE DISTINCTION BETWEEN EXISTING ALGORITHMS AND KNOWN ALGORITHMS

Algorithms always terminate. Semi-algorithms may not terminate. Examples 1–4 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 definition is constructive and currently known to us). A definition of an integer  $n$  is called *constructive*, if it provides a known algorithm with no input that returns  $n$ .

**Definition 1.** *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 with no input returns the logical value of the statement  $\text{card}(X) = \omega$ .*
- (3) *A known algorithm for every  $k \in \mathbb{N}$  decides whether or not  $k \in X$ .*
- (4) *A known algorithm with no input returns an integer  $n$  satisfying  $\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]$ .*
- (5)  *$X$  has the simplest definition among known sets  $Y \subseteq \mathbb{N}$  with the same set of known elements.*

Condition (2) implies that no known proof shows the finiteness/infiniteness of  $X$ . It seems that condition (5) implies that the set  $X$  is naturally defined, where this term has only informal meaning.

**Definition 2.** *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>. □

Edmund Landau's conjecture states that the set  $\mathcal{P}_{n^2+1}$  of primes of the form  $n^2 + 1$  is infinite, see [6]–[8]. Let  $[\cdot]$  denote the integer part function.

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

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

**Example 3.** ([1], [4], [5, p. 9]). *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*

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

*No known algorithm computes the function  $h$ .*

**Example 4.** *The set*

$$X = \begin{cases} \mathbb{N}, & \text{if the continuum hypothesis is true} \\ \emptyset, & \text{otherwise} \end{cases}$$

*is decidable. No constructively existing algorithm decides  $X$ , which holds forever.*

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

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

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

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

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

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

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

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 Open Problem 1 and Statements 2 and 3.

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

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  $[\max(X), \infty) \cap \mathbb{N}$ .

## 2. THE PHYSICAL LIMITS OF COMPUTATION INSPIRE OPEN PROBLEM 1

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

Open Problem 1 asks: Are there a set  $X \subseteq \mathbb{N}$  and a constructively defined integer  $n$  such that  $(\text{card}(X) < \omega \Rightarrow X \subseteq (-\infty, n]) \wedge$  (a constructively defined algorithm decides  $X$ )  $\wedge$  (there are many elements of  $X$ )  $\wedge$  (the infiniteness of  $X$  is conjectured and cannot be decided by any known method)  $\wedge$  ( $X$  has the simplest definition among known sets  $\mathcal{Y} \subseteq \mathbb{N}$  with the same set of known elements)?

**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). Condition (5) fails for  $X$ .

*Proof.* Condition (1) holds as  $X \supseteq \{0, \dots, \beta\}$  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 [3]. Thus condition (2) holds. Condition (3) holds trivially. Since the set

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

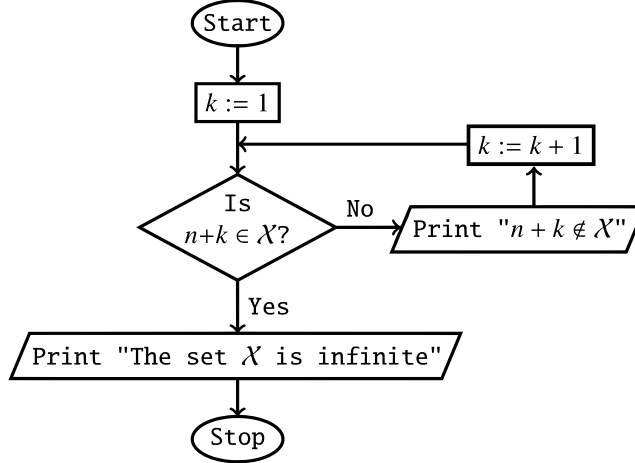
is empty or infinite, the integer  $\beta$  is a threshold number of  $X$ . Thus  $X$  satisfies condition (4). Condition (5) fails for  $X$  as the set of known elements of  $X$  equals  $\{0, \dots, \beta\}$ .  $\square$

Proving Landau's conjecture will disprove Statement 2.

**Theorem 1.** *No set  $\mathcal{X} \subseteq \mathbb{N}$  will satisfy conditions (1)–(4) forever, if for every algorithm with no input, 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)  $n + 1 \notin \mathcal{X}, n + 2 \notin \mathcal{X}, n + 3 \notin \mathcal{X}, \dots$



**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).  $\square$

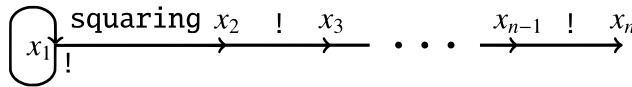
The physical limits of computation ([3]) disprove the assumption of Theorem 1.

### 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:

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

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



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

**Lemma 2.** *For every positive integer  $n$ , the system  $\mathcal{U}_n$  has exactly two solutions in positive integers, namely  $(1, \dots, 1)$  and  $(f(1), \dots, f(n))$ .*

Let  $B_n$  denote the following system of equations:

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

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  $x_1, \dots, x_n$ , then each such solution  $(x_1, \dots, x_n)$  satisfies  $x_1, \dots, x_n \leq f(n)$ .* 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 2 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  $\mathcal{S} \subseteq B_n$  has at most finitely many solutions in positive integers  $x_1, \dots, x_n$ , then for every integer  $i \in \{1, \dots, n\}$  the system  $\mathcal{S} \cup \{x_i! = x_{n+1}\}$  has at most finitely many solutions in positive integers  $x_1, \dots, x_{n+1}$ . 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 3.** *For every positive integers  $x$  and  $y$ ,  $x! \cdot y = y!$  if and only if*

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

**Lemma 4.** *(Wilson's theorem, [2, 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:

$$\left\{ \begin{array}{l} x_2! = x_3 \\ x_3! = x_4 \\ x_5! = x_6 \\ x_8! = x_9 \\ x_1 \cdot x_1 = x_2 \\ x_3 \cdot x_5 = x_6 \\ x_4 \cdot x_8 = x_9 \\ x_5 \cdot x_7 = x_8 \end{array} \right.$$

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



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

**Lemma 5.** *For every integer  $x_1 \geq 2$ , the system  $\mathcal{A}$  is solvable in positive integers  $x_2, \dots, x_9$  if and only if  $x_1^2 + 1$  is prime. In this case, the integers  $x_2, \dots, x_9$  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 3, for every integer  $x_1 \geq 2$ , the system  $\mathcal{A}$  is solvable in positive integers  $x_2, \dots, x_9$  if and only if  $x_1^2 + 1$  divides  $(x_1^2)! + 1$ . Hence, the claim of Lemma 5 follows from Lemma 4.  $\square$

**Lemma 6.** *There are only finitely many tuples  $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ , which solve the system  $\mathcal{A}$  and satisfy  $x_1 = 1$ . This is true as every such tuple  $(x_1, \dots, x_9)$  satisfies  $x_1, \dots, x_9 \in \{1, 2\}$ .*

*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  $x_7 = \frac{x_8}{x_5} \in \left\{\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{2}{2}\right\} \cap \mathbb{N} = \{1, 2\}$ .  $\square$

**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  $x_1 \geq 2$  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 5, there exists a unique tuple  $(x_2, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^8$  such that the tuple  $(x_1, x_2, \dots, x_9)$  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,

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

Conjecture 1 and the inequality  $x_9 > f(9)$  imply that the system  $\mathcal{A}$  has infinitely many solutions  $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ . According to Lemmas 5 and 6, the set  $\mathcal{P}_{n^2+1}$  is infinite.  $\square$

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

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

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

*Proof.* By Lemmas 5 and 6, if positive integers  $x_1, \dots, x_9$  solve the system  $\mathcal{A}$ , then

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

or  $x_1, \dots, x_9 \in \{1, 2\}$ . In the first case, Lemma 5 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  $x_1, \dots, x_9$ . 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 3.** *Conditions (1)–(3) and (5) hold for  $\mathcal{X} = \mathcal{P}_{n^2+1}$ . The statement  $\Phi$  implies that condition (4) holds for  $\mathcal{X} = \mathcal{P}_{n^2+1}$ .*

*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 [7]. 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  $\mathcal{P}_{n^2+1}$  is greater than  $f(7) = (((24!)!)!)! = \beta$ , see [3]. Thus condition (2) holds. Conditions (3) and (5) hold trivially. The statement  $\Phi$  implies that  $\beta$  is a threshold number of  $\mathcal{P}_{n^2+1}$ . Hence, the statement  $\Phi$  implies that condition (4) holds for  $\mathcal{X} = \mathcal{P}_{n^2+1}$ .  $\square$

Proving Landau's conjecture will disprove Statement 3.

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

## REFERENCES

- [1] J. Case and M. Ralston, *Beyond Rogers' non-constructively computable function*, in: *The nature of computation*, Lecture Notes in Comput. Sci., 7921, 45–54, Springer, Heidelberg, 2013, [http://link.springer.com/chapter/10.1007/978-3-642-39053-1\\_6](http://link.springer.com/chapter/10.1007/978-3-642-39053-1_6).
- [2] M. Erickson, A. Vazzana, D. Garth, *Introduction to number theory*, 2nd ed., CRC Press, Boca Raton, FL, 2016.
- [3] S. Lloyd, *Ultimate physical limits to computation*, Nature 406 (2000), 1047–1054, <http://doi.org/10.1038/35023282>.
- [4] 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>.
- [5] H. Rogers, Jr., *Theory of recursive functions and effective computability*, 2nd ed., MIT Press, Cambridge, MA, 1987.
- [6] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, A002496, *Primes of the form  $n^2 + 1$* , <http://oeis.org/A002496>.
- [7] 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>.
- [8] Wolfram MathWorld, *Landau's Problems*, <http://mathworld.wolfram.com/LandausProblems.html>.

Agnieszka Kozdęba

Faculty of Environmental Engineering and Land Surveying

Hugo Kołłątaj University

Balicka 253C, 30-198 Kraków, Poland

Institute of Mathematics

Jagiellonian University

Łojasiewicza 6, 30-348 Kraków, Poland

E-mail address: [Agnieszka.Kozdeba@im.uj.edu.pl](mailto:Agnieszka.Kozdeba@im.uj.edu.pl)

Apoloniusz Tyszka

Technical Faculty

Hugo Kołłątaj University

Balicka 116B, 30-149 Kraków, Poland

E-mail address: [rttyszka@cyf-kr.edu.pl](mailto:rttyszka@cyf-kr.edu.pl)