On sets $\mathcal{W} \subseteq \mathbb{N}$ whose infinity follows from the existence in $\mathcal{W}$ of an element which is greater than a threshold number computed for $\mathcal{W}$

Apoloniusz Tyszka

Abstract

We define computable functions $f, g \colon \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$. For a positive integer n, let Θ_n denote the following statement: if a system $\mathcal{S} \subseteq \Big\{x_i! = x_k : i, k \in \{1, \ldots, n\}\Big\} \cup \Big\{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\Big\}$ has only finitely many solutions in integers $x_1, \ldots, x_n$ greater than 1, then each such solution $(x_1, \ldots, x_n)$ satisfies $\min(x_1, \ldots, x_n) \leqslant f(n)$. The statement Θ_9 proves that if there exists an integer $x > f(9)$ such that $x^2 + 1$ (alternatively, $x! + 1$) is prime, then there are infinitely many primes of the form $n^2 + 1$ (respectively, $n! + 1$). The statement Θ_{16} proves that if there exists a twin prime greater than $f(16) + 3$, then there are infinitely many twin primes. We formulate a statement which proves that if $2^{2^n} + 1$ is composite for some integer $n > g(13)$, then $2^{2^n} + 1$ is composite for infinitely many positive integers n.

Key words and phrases: Brocard's problem, Brocard-Ramanujan equation, composite Fermat numbers, composite numbers of the form $2^{2^n} + 1$, prime numbers of the form $n^2 + 1$, prime numbers of the form $n! + 1$, Richert's lemma, twin prime conjecture.

2010 Mathematics Subject Classification: 03B30, 11U09.

1 Introduction

The following observation concerns the theme described in the title of the article.

Observation 1. *If $n \in \mathbb{N}$ and $\mathcal{W} \subseteq \mathbb{N} \cap [0, n]$, then we take any integer $m \geqslant n$ as a threshold number for $\mathcal{W}$. If $\mathcal{W} \subseteq \mathbb{N}$ and W is infinite, then we take any non-negative integer m as a threshold number for $\mathcal{W}$.*

We define the set $\mathcal{U} \subseteq \mathbb{N}$ by declaring that a non-negative integer n belongs to $\mathcal{U}$ if and only if $\sin\left(10^{10^{10^{10}}}\right) > 0$. This inequality is practically undecidable, see [5].

Corollary 1. *The set $\mathcal{U}$ equals $\emptyset$ or $\mathbb{N}$. The statement "$\mathcal{U} = \emptyset$" remains unproven and the statement "$\mathcal{U} = \mathbb{N}$" remains unproven. Every non-negative integer m is a threshold number for $\mathcal{U}$. For every non-negative integer k, the sentence "$k \in \mathcal{U}$" is only theoretically decidable.*

The first-order language of graph theory contains two relation symbols of arity 2: $\sim$ and $=$, respectively for adjacency and equality of vertices. The term first-order imposes the condition that the variables represent vertices and hence the quantifiers apply to vertices only. For a first-order sentence Λ about graphs, let $\text{Spectrum}(\Lambda)$ denote the set of all positive integers n such that there is a graph on n vertices satisfying Λ. By a graph on n vertices we understand a set of n elements with a binary relation which is symmetric and irreflexive.

Theorem 1. *([12, p. 171]). If a sentence Λ in the language of graph theory has the form $\exists x_1 \ldots x_k \, \forall y_1 \ldots y_l \, \Upsilon(x_1, \ldots, x_k, y_1, \ldots, y_l)$, where $\Upsilon(x_1, \ldots, x_k, y_1, \ldots, y_l)$ is quantifier-free, then either* $\text{Spectrum}(\Lambda) \subseteq [1, (2^k \cdot 4^l) - 1]$ *or* $\text{Spectrum}(\Lambda) \supseteq [k + l, \infty) \cap \mathbb{N}$.

Corollary 2. *The number* $\left(2^k \cdot 4^l\right) - 1$ *is a threshold number for* $\text{Spectrum}(\Lambda)$.

The classes of the infinite recursively enumerable sets and of the infinite recursive sets are not recursively enumerable, see [10, p. 234].

Corollary 3. *If an algorithm $\texttt{Al}_1$ for every recursive set $\mathcal{W} \subseteq \mathbb{N}$ finds a non-negative integer $\texttt{Al}_1(\mathcal{W})$, then there exists a finite set $\mathcal{M} \subseteq \mathbb{N}$ such that $\mathcal{M} \cap [\texttt{Al}_1(\mathcal{M}) + 1, \infty) \neq \emptyset$.*

Corollary 4. *If an algorithm $\texttt{Al}_2$ for every recursively enumerable set $\mathcal{W} \subseteq \mathbb{N}$ finds a non-negative integer $\texttt{Al}_2(\mathcal{W})$, then there exists a finite set $\mathcal{M} \subseteq \mathbb{N}$ such that $\mathcal{M} \cap [\texttt{Al}_2(\mathcal{M}) + 1, \infty) \neq \emptyset$.*

Let $K = \{j \in \mathbb{N} : \, 2^{\aleph_j} = \aleph_{j+1}\}$.

Theorem 2. *If ZFC is consistent, then for every non-negative integer n the sentence* "`n is a threshold number for K`" *is not provable in ZFC.*

Proof. There exists a model $\mathcal{E}$ of ZFC such that

$$\forall i \in \{0, \ldots, n + 1\} \, \mathcal{E} \models 2^{\aleph_i} = \aleph_{i+1}$$

and

$$\forall i \in \{n + 2, n + 3, n + 4, \ldots\} \, \mathcal{E} \models 2^{\aleph_i} = \aleph_{i+2}$$

see [3] and [6, p. 232]. In the model $\mathcal{E}$, $K = \{0, \ldots, n + 1\}$ and n is not a threshold number for K. □

Theorem 3. *If ZFC is consistent, then for every non-negative integer n the sentence* "`n is not a threshold number for K`" *is not provable in ZFC.*

Proof. The Generalized Continuum Hypothesis (GCH) is consistent with ZFC, see [6, p. 188] and [6, p. 190]. GCH implies that $K = \mathbb{N}$. Consequently, GCH implies that every non-negative integer n is a threshold number for K. □

Let $g(1) = 1$, and let $g(n+1) = 2^{2^{g(n)}}$ for every positive integer n.

Hypothesis 1. *([18]). If a system*

$$\mathcal{S} \subseteq \{x_i \cdot x_j = x_k : \ i, j, k \in \{1, \ldots, n\}\} \cup \{x_i + 1 = x_k : \ i, k \in \{1, \ldots, n\}\}$$

has only finitely many solutions in non-negative integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leqslant g(2n)$.

Theorem 4. *([18]). Hypothesis 1 implies that for every $W(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ we can compute a threshold number $b \in \mathbb{N} \setminus \{0\}$ such that any non-negative integers $a_1, \ldots, a_n$ which satisfy*

$$(W(a_1, \ldots, a_n) = 0) \wedge (\max(a_1, \ldots, a_n) > b)$$

guarantee that the equation $W(x_1, \ldots, x_n) = 0$ has infinitely many solutions in non-negative integers.

2 Basic lemmas

Let $f(1) = 2$, $f(2) = 4$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 2$. Let $\mathcal{V}_1$ denote the system of equations $\{x_1! = x_1\}$, and let $\mathcal{V}_2$ denote the system of equations $\{x_1! = x_1, \ x_1 \cdot x_1 = x_2\}$. For an integer $n \geqslant 3$, let $\mathcal{V}_n$ 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 1 illustrates the construction of the system $\mathcal{V}_n$.

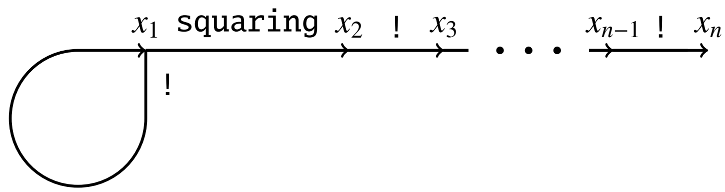

Fig. 1 Construction of the system $\mathcal{V}_n$

Lemma 1. *For every positive integer n, the system $\mathcal{V}_n$ has exactly one solution in integers greater than* 1*, namely* $\big(f(1), \dots, f(n)\big)$.

Let

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

For a positive integer n, let Θ_n denote the following statement: if a system $\mathcal{S} \subseteq H_n$ has at most finitely many solutions in integers $x_1, \dots, x_n$ greater than 1, then each such solution $(x_1, \dots, x_n)$ satisfies $\min(x_1, \dots, x_n) \leqslant f(n)$. The assumption $\min(x_1, \dots, x_n) \leqslant f(n)$ is weaker than the assumption $\max(x_1, \dots, x_n) \leqslant f(n)$ suggested by Lemma 1.

Lemma 2. *For every positive integer n, the system H_n has a finite number of subsystems.*

Theorem 5. *Every statement Θ_n is true with an unknown integer bound that depends on n.*

Proof. It follows from Lemma 2. □

Lemma 3. *For every integers x and y greater than* 1*,* $x! \cdot y = y!$ *if and only if* $x + 1 = y$.

Lemma 4. *If* $x \geqslant 4$*, then* $\dfrac{(x-1)!+1}{x} > 1$.

Lemma 5. *(Wilson's theorem, [4, p. 89]). For every integer $x \geqslant 2$, x is prime if and only if x divides* $(x-1)!+1$.

3 Brocard's problem

A weak form of Szpiro's conjecture implies that there are only finitely many solutions to the Brocard-Ramanujan equation $x! + 1 = y^2$, see [11]. It is conjectured that $x! + 1$ is a square only for $x \in \{4, 5, 7\}$, see [19, p. 297].

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

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

Lemma 3 and the diagram in Figure 2 explain the construction of the system $\mathcal{A}$.

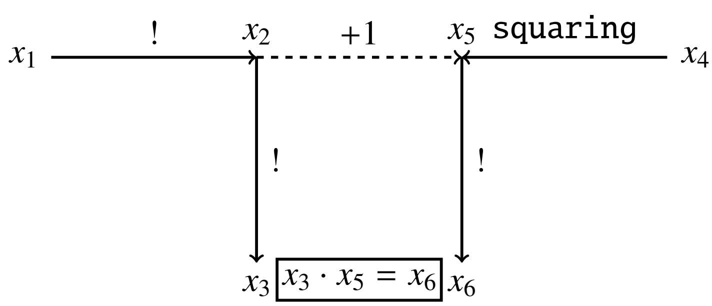

Fig. 2 Construction of the system $\mathcal{A}$

Lemma 6. *For every integers x_1 and x_4 greater than 1, the system $\mathcal{A}$ is solvable in integers x_2, x_3, x_5, x_6 greater than 1 if and only if $x_1! + 1 = x_4^2$. In this case, the integers x_2, x_3, x_5, x_6 are uniquely determined by the following equalities:*

$$\begin{aligned} x_2 &= x_1! \\ x_3 &= (x_1!)! \\ x_5 &= x_1! + 1 \\ x_6 &= (x_1! + 1)! \end{aligned}$$

and $x_1 = \min(x_1, \ldots, x_6)$.

Proof. It follows from Lemma 3. □

Theorem 6. *The statement Θ_6 proves the following implication: if the equation $x_1! + 1 = x_4^2$ has only finitely many solutions in positive integers, then each such solution (x_1, x_4) satisfies $x_1 \leqslant f(6)$.*

Proof. Let positive integers x_1 and x_4 satisfy $x_1! + 1 = x_4^2$. Then, $x_1, x_4 \in \mathbb{N} \setminus \{0, 1\}$. By Lemma 6, there exists a unique tuple $(x_2, x_3, x_5, x_6) \in (\mathbb{N} \setminus \{0, 1\})^4$ such that the tuple $(x_1, \ldots, x_6)$ solves the system $\mathcal{A}$. Lemma 6 guarantees that $x_1 = \min(x_1, \ldots, x_6)$. By the antecedent and Lemma 6, the system $\mathcal{A}$ has only finitely many solutions in integers $x_1, \ldots, x_6$ greater than 1. Therefore, the statement Θ_6 implies that $x_1 = \min(x_1, \ldots, x_6) \leqslant f(6)$. □

Hypothesis 2. *The implication in Theorem 6 is true.*

Corollary 5. *Assuming Hypothesis 2, a single query to an oracle for the halting problem decides the problem of the infinitude of the solutions of the equation* $x! + 1 = y^2$.

4 Are there infinitely many prime numbers of the form $n^2 + 1$?

Edmund Landau's conjecture states that there are infinitely many primes of the form $n^2 + 1$, see [9, pp. 37–38]. Let $\mathcal{B}$ 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 3 and the diagram in Figure 3 explain the construction of the system $\mathcal{B}$.

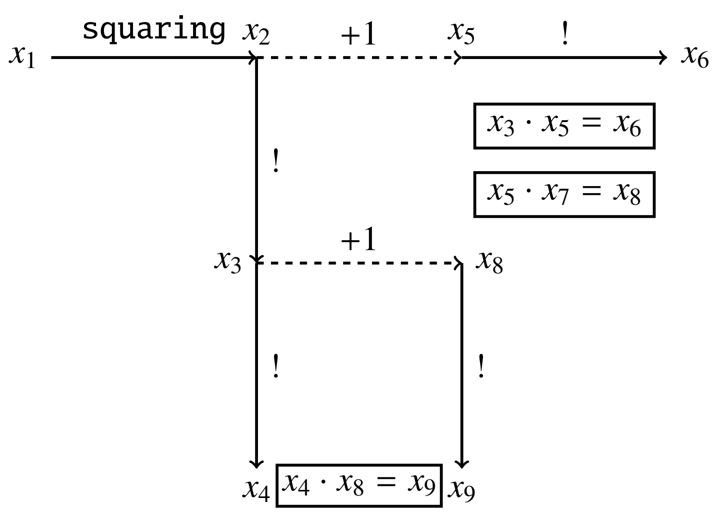

Fig. 3 Construction of the system $\mathcal{B}$

Lemma 7. *For every integer* $x_1 \geqslant 2$*, the system* $\mathcal{B}$ *is solvable in integers* $x_2, \ldots, x_9$ *greater than* 1 *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:*

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

and $\min(x_1, \ldots, x_9) = x_1$.

Proof. By Lemmas 3 and 4, for every integer $x_1 \geqslant 2$, the system $\mathcal{B}$ is solvable in integers $x_2, \ldots, x_9$ greater than 1 if and only if $x_1^2 + 1$ divides $(x_1^2)! + 1$. Hence, the claim of Lemma 7 follows from Lemma 5. □

Theorem 7. *The statement* Θ_9 *proves the following implication: if there exists an integer* $x_1 > f(9)$ *such that* $x_1^2 + 1$ *is prime, then there are infinitely many primes of the form* $n^2 + 1$.

Proof. Assume that an integer x_1 is greater than $f(9)$ and $x_1^2 + 1$ is prime. By Lemma 7, there exists a unique tuple $(x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^8$ such that the tuple $(x_1, x_2, \ldots, x_9)$ solves the system $\mathcal{B}$. Lemma 7 guarantees that $\min(x_1, \ldots, x_9) = x_1$. Since $\mathcal{B} \subseteq H_9$, the statement Θ_9 and the inequality $\min(x_1, \ldots, x_9) = x_1 > f(9)$ imply that the system $\mathcal{B}$ has infinitely many solutions $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9$. According to Lemma 7, there are infinitely many primes of the form $n^2 + 1$. □

Hypothesis 3. *The implication in Theorem 7 is true.*

Corollary 6. *Assuming Hypothesis 3, a single query to an oracle for the halting problem decides the problem of the infinitude of primes of the form* $n^2 + 1$.

Let $\mathcal{P}$ denote the set of prime numbers. For a non-negative integer n, let $\Omega(n)$ denote the following statement: $\exists m \in \mathbb{N} \cap (n, \infty)\ m^2 + 1 \in \mathcal{P}$. By Theorem 7, assuming the statement Θ_9, we can infer the statement $\forall n \in \mathbb{N}\ \Omega(n)$ from any statement $\Omega(n)$ with $n \geqslant f(9)$. A similar situation holds for inference by the so called *"super-induction method"*, see [20]–[23]. In section 8, we present a theorem whose computer-assisted proof is based on the super-induction method.

5 Are there infinitely many prime numbers of the form $n! + 1$?

It is conjectured that there are infinitely many primes of the form $n! + 1$, see [1, p. 443] and [15]. Let $\mathcal{G}$ denote the following system of equations:

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

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

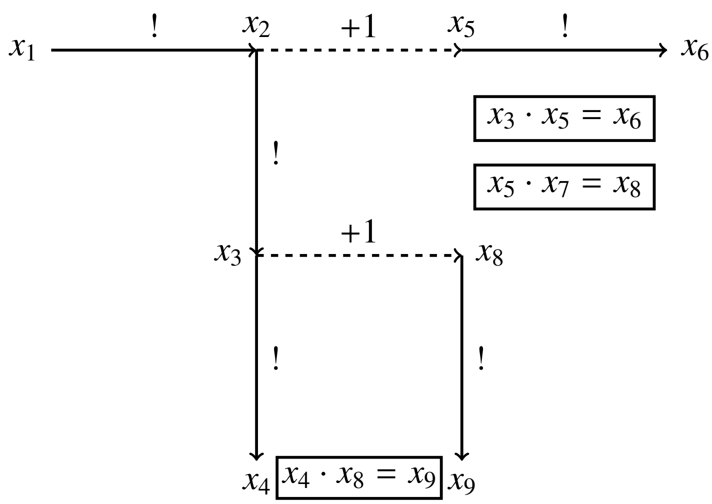

Fig. 4 Construction of the system $\mathcal{G}$

Lemma 8. *For every integer $x_1 \geqslant 2$, the system $\mathcal{G}$ is solvable in integers $x_2, \ldots, x_9$ greater than* 1 *if and only if $x_1! + 1$ is prime. In this case, the integers $x_2, \ldots, x_9$ are uniquely determined by the following equalities:*

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

and $\min(x_1, \ldots, x_9) = x_1$.

Proof. By Lemmas 3 and 4, for every integer $x_1 \geqslant 2$, the system $\mathcal{G}$ is solvable in integers $x_2, \ldots, x_9$ greater than 1 if and only if $x_1! + 1$ divides $(x_1!)! + 1$. Hence, the claim of Lemma 8 follows from Lemma 5. □

Theorem 8. *The statement Θ_9 proves the following implication: if there exists an integer $x_1 > f(9)$ such that $x_1! + 1$ is prime, then there are infinitely many primes of the form $n! + 1$.*

Proof. Assume that an integer x_1 is greater than $f(9)$ and $x_1! + 1$ is prime. By Lemma 8, there exists a unique tuple $(x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^8$ such that the tuple $(x_1, x_2, \ldots, x_9)$ solves the system $\mathcal{G}$. Lemma 8 guarantees that $\min(x_1, \ldots, x_9) = x_1$. Since $\mathcal{G} \subseteq H_9$, the statement Θ_9 and the inequality $\min(x_1, \ldots, x_9) = x_1 > f(9)$ imply that the system $\mathcal{G}$ has infinitely many solutions $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9$. According to Lemma 8, there are infinitely many primes of the form $n! + 1$. □

Hypothesis 4. *The implication in Theorem 8 is true.*

Corollary 7. *Assuming Hypothesis 4, a single query to an oracle for the halting problem decides the problem of the infinitude of primes of the form $n! + 1$.*

6 The twin prime conjecture

A twin prime is a prime number that is either 2 less or 2 more than another prime number. The twin prime conjecture states that there are infinitely many twin primes, see [9, p. 39].

Let C denote the following system of equations:

$$\begin{cases} x_1! & = & x_2 \\ x_2! & = & x_3 \\ x_4! & = & x_5 \\ x_6! & = & x_7 \\ x_7! & = & x_8 \\ x_9! & = & x_{10} \\ x_{12}! & = & x_{13} \\ x_{15}! & = & x_{16} \\ x_2 \cdot x_4 & = & x_5 \\ x_5 \cdot x_6 & = & x_7 \\ x_7 \cdot x_9 & = & x_{10} \\ x_4 \cdot x_{11} & = & x_{12} \\ x_3 \cdot x_{12} & = & x_{13} \\ x_9 \cdot x_{14} & = & x_{15} \\ x_8 \cdot x_{15} & = & x_{16} \end{cases}$$

Lemma 3 and the diagram in Figure 5 explain the construction of the system C.

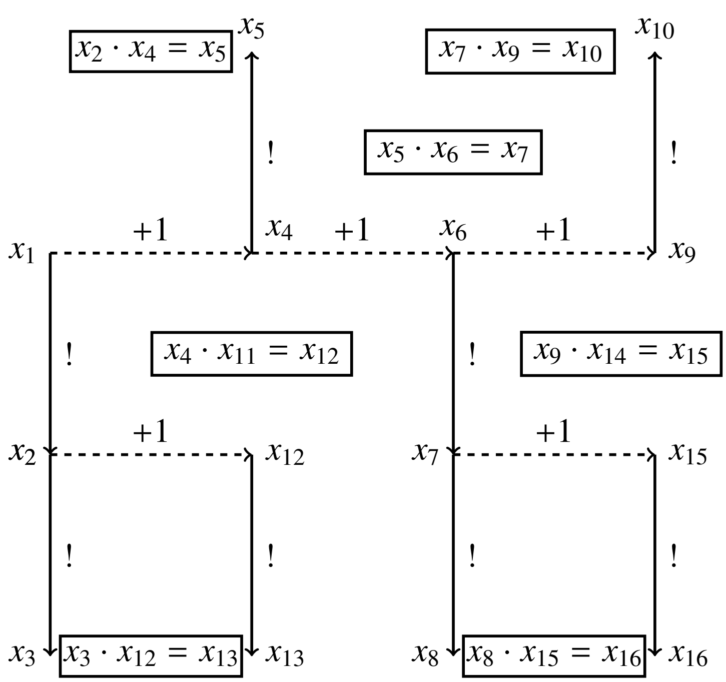

Fig. 5 Construction of the system C

Lemma 9. *If $x_4 = 2$, then the system C has no solutions in integers $x_1, \ldots, x_{16}$ greater than* 1.

Proof. The equality $x_2 \cdot x_4 = x_5 = x_4!$ and the equality $x_4 = 2$ imply that $x_2 = 1$. □

Lemma 10. *If $x_4 = 3$, then the system C has no solutions in integers $x_1, \ldots, x_{16}$ greater than* 1.

Proof. The equality $x_4 \cdot x_{11} = x_{12} = (x_4 - 1)! + 1$ and the equality $x_4 = 3$ imply that $x_{11} = 1$. □

Lemma 11. *For every $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$ and for every $x_9 \in \mathbb{N} \setminus \{0, 1\}$, the system C is solvable in integers x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16} greater than* 1 *if and only if x_4 and x_9 are prime and $x_4 + 2 = x_9$. In this case, the integers x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16} are uniquely determined by the following equalities:*

$$\begin{aligned}
x_1 &= x_4 - 1 \\
x_2 &= (x_4 - 1)! \\
x_3 &= ((x_4 - 1)!)! \\
x_5 &= x_4! \\
x_6 &= x_9 - 1 \\
x_7 &= (x_9 - 1)! \\
x_8 &= ((x_9 - 1)!)! \\
x_{10} &= x_9! \\
x_{11} &= \frac{(x_4 - 1)! + 1}{x_4} \\
x_{12} &= (x_4 - 1)! + 1 \\
x_{13} &= ((x_4 - 1)! + 1)! \\
x_{14} &= \frac{(x_9 - 1)! + 1}{x_9} \\
x_{15} &= (x_9 - 1)! + 1 \\
x_{16} &= ((x_9 - 1)! + 1)!
\end{aligned}$$

and $\min(x_1, \ldots, x_{16}) = x_1 = x_9 - 3$.

Proof. By Lemmas 3 and 4, for every $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$ and for every $x_9 \in \mathbb{N} \setminus \{0, 1\}$, the system C is solvable in integers x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16} greater than 1 if and only if

$$\Big(x_4 + 2 = x_9\Big) \wedge \Big(x_4 | (x_4 - 1)! + 1\Big) \wedge \Big(x_9 | (x_9 - 1)! + 1\Big)$$

Hence, the claim of Lemma 11 follows from Lemma 5. □

Theorem 9. *The statement Θ_{16} proves the following implication: if there exists a twin prime greater than $f(16) + 3$, then there are infinitely many twin primes.*

Proof. Assume that the antecedent holds. Then, there exist prime numbers x_4 and x_9 such that $x_9 = x_4 + 2 > f(16) + 3$. Hence, $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$. By Lemma 11, there exists a unique tuple $(x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0, 1\})^{14}$ such that the tuple $(x_1, \dots, x_{16})$ solves the system C. Lemma 11 guarantees that $\min(x_1, \dots, x_{16}) = x_1 = x_9 - 3 > f(16)$. Since $C \subseteq H_{16}$, the statement Θ_{16} and the inequality $\min(x_1, \dots, x_{16}) > f(16)$ imply that the system C has infinitely many solutions in integers $x_1, \dots, x_{16}$ greater than 1. According to Lemmas 9–11, there are infinitely many twin primes. □

Hypothesis 5. *The implication in Theorem 9 is true.*

Corollary 8. *(cf. [2]). Assuming Hypothesis 5, a single query to an oracle for the halting problem decides the twin prime problem.*

7 Are there infinitely many composite Fermat numbers?

Primes of the form $2^{2^n} + 1$ are called Fermat primes, as Fermat conjectured that every integer of the form $2^{2^n} + 1$ is prime, see [8, p. 1]. Fermat correctly remarked that $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, and $2^{2^4} + 1 = 65537$ are all prime, see [8, p. 1].

Open Problem. ([8, p. 159]). *Are there infinitely many composite numbers of the form $2^{2^n} + 1$?*

Most mathematicians believe that $2^{2^n} + 1$ is composite for every integer $n \geqslant 5$, see [7, p. 23].

Theorem 10. *([17]). An unproven inequality stated in [17] implies that $2^{2^n} + 1$ is composite for every integer $n \geqslant 5$.*

Lemma 12. *([8, p. 38]). For every positive integer n, if a prime number p divides $2^{2^n} + 1$, then there exists a positive integer k such that $p = k \cdot 2^{n+1} + 1$.*

Corollary 9. *Since $k \cdot 2^{n+1} + 1 \geqslant 2^{n+1} + 1 \geqslant n + 3$, for every positive integers x, y, and n, the equality $(x + 1)(y + 1) = 2^{2^n} + 1$ implies that $\min(n, x, x + 1, y, y + 1) = n$.*

Let

$$G_n = \left\{x_i \cdot x_j = x_k :\ i, j, k \in \{1, \dots, n\}\right\} \cup \left\{2^{2^{x_i}} = x_k :\ i, k \in \{1, \dots, n\}\right\}$$

Lemma 13. *The following subsystem of G_n*

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

has exactly one solution $(x_1, \dots, x_n) \in (\mathbb{N} \setminus \{0\})^n$, namely $(g(1), \dots, g(n))$.

For a positive integer n, let Ψ_n denote the following statement: if a system $S \subseteq G_n$ has at most finitely many solutions in positive integers $x_1, \dots, x_n$, then each such solution $(x_1, \dots, x_n)$ satisfies $\min(x_1, \dots, x_n) \leqslant g(n)$. The assumption $\min(x_1, \dots, x_n) \leqslant g(n)$ is weaker than the assumption $\max(x_1, \dots, x_n) \leqslant g(n)$ suggested by Lemma 13.

Lemma 14. *For every positive integer n, the system G_n has a finite number of subsystems.*

Theorem 11. *Every statement Ψ_n is true with an unknown integer bound that depends on n.*

Proof. It follows from Lemma 14. □

Lemma 15. *For every non-negative integers b and c, $b + 1 = c$ if and only if $2^{2^b} \cdot 2^{2^b} = 2^{2^c}$.*

Theorem 12. *The statement Ψ_{13} proves the following implication: if $2^{2^n} + 1$ is composite for some integer $n > g(13)$, then $2^{2^n} + 1$ is composite for infinitely many positive integers n.*

Proof. Let us consider the equation

$$(x + 1)(y + 1) = 2^{2^z} + 1 \tag{1}$$

in positive integers. By Lemma 15, we can transform equation (1) into an equivalent system $\mathcal{F}$ which has 13 variables (x, y, z, and 10 other variables) and which consists of equations of the forms $\alpha \cdot \beta = \gamma$ and $2^{2^\alpha} = \gamma$, see the diagram in Figure 6.

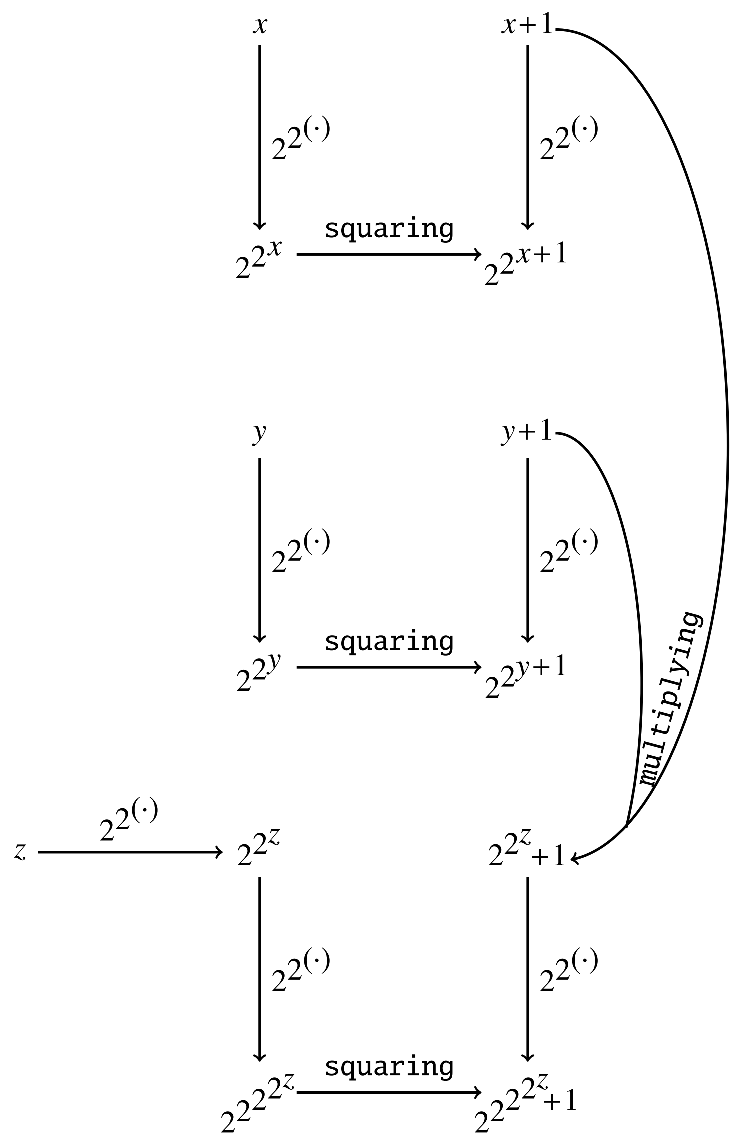

Fig. 6 Construction of the system $\mathcal{F}$

Assume that $2^{2^n} + 1$ is composite for some integer $n > g(13)$. By this and Corollary 9, equation (1) has a solution $(x, y, z) \in (\mathbb{N} \setminus \{0\})^3$ such that $z = n$ and $z = \min(z, x, x + 1, y, y + 1)$. Hence, the system $\mathcal{F}$ has a solution in positive integers such that $z = n$ and n is the smallest number in the solution sequence. Since $n > g(13)$, the statement Ψ_{13} implies that the system $\mathcal{F}$ has infinitely many solutions in positive integers. Therefore, there are infinitely many positive integers n such that $2^{2^n} + 1$ is composite. □

Hypothesis 6. *The implication in Theorem 12 is true.*

Corollary 10. *Assuming Hypothesis 6, a single query to an oracle for the halting problem decides whether or not the set of composite Fermat numbers is infinite.*

8 Every integer greater than 248 is expressible as a sum of distinct squares greater than 4

Lemma 16. *([13], [14, p. 152]). Let $\{m_i\}_{i=1}^{\infty}$ be an increasing sequence of positive integers such that for some positive integer k the inequality $m_{i+1} \leqslant 2m_i$ holds for all $i > k$. Suppose there exists a non-negative integer a such that the numbers $a+1$, $a+2$, $a+3$, $\ldots$, $a+m_{k+1}$ are all expressible as sums of distinct elements of the set $\{m_1, \ldots, m_k\}$. Then every integer greater than a is expressible as a sum of distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$.*

Every positive integer greater than 128 can be expressed as a sum of distinct squares, see [16].

Theorem 13. 248 *is the largest integer which is not expressible as a sum of distinct squares greater than* 4*. Every positive integer except* 100 *numbers is expressible as a sum of distinct squares greater than* 4*.*

Proof. The execution of the following *MuPAD* code

```
A:={n^2 $n=3..13}:
B:={A[1]}:
for i from 2 to nops(A) do
B:=B union {A[i]} union {B[j]+A[i] $j=1..nops(B)}:
end_for:
{248} minus B;
{m $m=248+1..248+14^2} minus B;
nops({m $m=1..248} minus B);
```

gives the following output

```
{248}

{}

100
```

The set {248} on the output indicates that 248 is not expressible as a sum of distinct squares greater than 4. The number 100 on the output indicates that 100 integers in the interval $[1, 248]$ are not expressible as a sum of distinct squares greater than 4. The empty set {} on the output indicates that each of the integers

$$248 + 1,\ 248 + 2,\ 248 + 3,\ \ldots,\ 248 + 14^2$$

is expressible as a sum of distinct elements of the set $\{3^2,\ 4^2,\ 5^2,\ \ldots,\ 13^2\}$. Thus, if we apply Lemma 16 with $m_i = (i + 2)^2$, $k = 11$, and $a = 248$, we conclude that every integer greater than 248 is expressible as a sum of distinct squares greater than 4. □

MuPAD is a general-purpose computer algebra system. The commercial version of *MuPAD* is no longer available as a stand-alone product, but only as the *Symbolic Math Toolbox* of *MATLAB*. Fortunately, the presented code can be executed by *MuPAD Light*, which was offered for free for research and education until autumn 2005.

References

[1] C. K. Caldwell and Y. Gallot, *On the primality of* $n! \pm 1$ *and* $2 \times 3 \times 5 \times \cdots \times p \pm 1$, Math. Comp. 71 (2002), no. 237, 441–448, `https://doi.org/10.1090/S0025-5718-01-01315-1`.

[2] F. G. Dorais, *Can the twin prime problem be solved with a single use of a halting oracle?* July 23, 2011, `https://mathoverflow.net/questions/71050`.

[3] W. B. Easton, *Powers of regular cardinals,* Ann. Math. Logic 1 (1970), 139–178.

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

[5] J. van der Hoeven, *Undecidability versus undecidability,* Bull. Symbolic Logic 5 (1999), no. 1, 75, `https://dx.doi.org/10.2307/421141`.

[6] T. Jech, *Set theory,* Springer, Berlin, 2003.

[7] J.-M. De Koninck and F. Luca, *Analytic number theory: Exploring the anatomy of integers,* American Mathematical Society, Providence, RI, 2012.

[8] M. Křížek, F. Luca, L. Somer, *17 lectures on Fermat numbers: from number theory to geometry,* Springer, New York, 2001.

[9] W. Narkiewicz, *Rational number theory in the 20th century: From PNT to FLT,* Springer, London, 2012.

[10] P. Odifreddi, *Classical recursion theory: the theory of functions and sets of natural numbers,* North-Holland, Amsterdam, 1989.

[11] M. Overholt, *The Diophantine equation* $n! + 1 = m^2$, Bull. London Math. Soc. 25 (1993), no. 2, 104, `https://doi.org/10.1112/blms/25.2.104`.

[12] O. Pikhurko and O. Verbitsky, *Logical complexity of graphs: a survey;* in: *Model theoretic methods in finite combinatorics,* Contemp. Math. 558, 129–179, Amer. Math. Soc., Providence, RI, 2011, `https://dx.doi.org/10.1090/conm/558`.

[13] H.-E. Richert, *Über Zerlegungen in paarweise verschiedene Zahlen,* Norsk Mat. Tidsskr. 31 (1949), 120–122.

[14] W. Sierpiński, *Elementary theory of numbers,* 2nd ed. (ed. A. Schinzel), PWN – Polish Scientific Publishers and North-Holland, Warsaw-Amsterdam, 1987.

[15] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002981, Numbers* n *such that* $n! + 1$ *is prime,* `https://oeis.org/A002981`.

[16] R. Sprague, *Über Zerlegungen in ungleiche Quadratzahlen,* Math. Z. 51 (1948), 289–290.

[17] A. Tyszka, *Is there a computable upper bound for the height of a solution of a Diophantine equation with a unique solution in positive integers?,* Open Comput. Sci. 7 (2017), no. 1, 17–23, `https://doi.org/10.1515/comp-2017-0003`.

[18] A. Tyszka, *A hypothetical upper bound on the heights of the solutions of a Diophantine equation with a finite number of solutions,* Open Comput. Sci. 8 (2018), in online printing, `https://www.cyf-kr.edu.pl/~rttyszka/ocs.pdf`.

[19] E. W. Weisstein, *CRC Concise Encyclopedia of Mathematics,* 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2002.

[20] A. A. Zenkin, *Superinduction: a new method for proving general mathematical statements with a computer,* Dokl. Math. 55 (1997), no. 3, 410–413.

[21] A. A. Zenkin, *Superinduction method: logical acupuncture of mathematical infinity* (in Russian), in: *Infinity in mathematics: philosophical and historical aspects* (ed. A. G. Barabashev), Janus-K, Moscow, 1997, 152–168, 173–176.

[22] A. A. Zenkin, *The generalized Waring problem: estimation of the function $G(m, r)$ in terms of the function $g(m-1, r)$ by the superinduction method,* Dokl. Math. 56 (1997), no. 1, 597–600.

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

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