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

Apoloniusz Tyszka

Abstract

We define computable functions \( f, g : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\} \). For a positive integer \( n \), let \( \Theta_n \) denote the following statement: if a system \( S \subseteq \{x_i! = x_k : i, k \in \{1, \ldots, n\}\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\} \) 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 \( \min(x_1, \ldots, x_n) \leq f(n) \). The statement \( \Theta_9 \) 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 \( \Theta_{16} \) 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, Richert’s theorem, twin prime conjecture.

2010 Mathematics Subject Classification: 03B30, 03D20, 11A41.

1 Introduction

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

Observation 1. If \( n \in \mathbb{N} \) and \( W \subseteq \{0, \ldots, n\} \), then we take any integer \( m \geq n \) as a threshold number for \( W \). If \( W \subseteq \mathbb{N} \) and \( W \) is infinite, then we take any non-negative integer \( m \) as a threshold number for \( W \).
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 \( \sin \left( 10^{10^{10}} \right) > 0 \). This inequality is practically undecidable, see [7].

**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 \( \Lambda \) about graphs, let \( \text{Spectrum}(\Lambda) \) denote the set of all positive integers \( n \) such that there is a graph on \( n \) vertices satisfying \( \Lambda \). By a graph on \( n \) vertices we understand a set of \( n \) elements with a binary relation which is symmetric and irreflexive.

**Theorem 1.** ([13] p. 171). If a sentence \( \Lambda \) 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 \( (2^k \cdot 4^l) - 1 \) 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 [13] p. 234].

**Corollary 3.** If an algorithm \( A_1 \) for every recursive set \( \mathcal{W} \subseteq \mathbb{N} \) finds a non-negative integer \( A_1(\mathcal{W}) \), then there exists a finite set \( M \subseteq \mathbb{N} \) such that \( M \cap [A_1(M) + 1, \infty) \neq \emptyset \).

**Corollary 4.** If an algorithm \( A_2 \) for every recursively enumerable set \( \mathcal{W} \subseteq \mathbb{N} \) finds a non-negative integer \( A_2(\mathcal{W}) \), then there exists a finite set \( M \subseteq \mathbb{N} \) such that \( M \cap [A_2(M) + 1, \infty) \neq \emptyset \).

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 \( E \) of ZFC such that

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

and

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

see [5] and [8, p. 232]. In the model \( E, K = \{0, \ldots, n + 1\} \) 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 [8, p. 188] and [8, p. 190]. GCH implies that \( K = \mathbb{N} \). Consequently, GCH implies that every non-negative integer \( n \) is a threshold number for \( K \). □

**Theorem 4.** ([2, p. 35]). There exists a polynomial \( D(x_1, \ldots, x_m) \) with integer coefficients such that if ZFC is arithmetically consistent, then the sentences

"The equation \( D(x_1, \ldots, x_m) = 0 \) is solvable in non-negative integers"

and

"The equation \( D(x_1, \ldots, x_m) = 0 \) is not solvable in non-negative integers"

are not provable in ZFC.

Let \( \Delta \) denote the set of all non-negative integers \( k \) such that the equation \( D(x_1, \ldots, x_m) = 0 \) has no solutions in \( \{0, \ldots, k\}^m \). Since the set \( \{0, \ldots, k\}^m \) is finite, the set \( \Delta \) is computable. Theorem 4 implies the following corollary.

**Corollary 5.** If ZFC is arithmetically consistent, then for every non-negative integer \( n \) the sentences

"\( n \) is a threshold number for \( \Delta \)"

and

"\( n \) is not a threshold number for \( \Delta \)"

are not provable in ZFC.
Let \( g(1) = 1 \), and let \( g(n + 1) = 2^{2g(n)} \) for every positive integer \( n \).

**Hypothesis 1.** ([20]). If a system

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

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

**Theorem 5.** ([20]). 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

\[
(W(a_1, \ldots, a_n) = 0) \land (\max(a_1, \ldots, a_n) > b)
\]

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 \( n \geq 2 \). 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 \( n \geq 3 \), let \( \mathcal{V}_n \) denote the following system of equations:

\[
\begin{align*}
x_1! & = x_1 \\
x_1 \cdot x_1 & = x_2 \\
\forall i \in \{2, \ldots, n - 1\} & \ x_i! = x_{i+1}
\end{align*}
\]

The diagram in Figure 1 illustrates the construction of the system \( \mathcal{V}_n \).

![Fig. 1 Construction of the system \( \mathcal{V}_n \)](image)

**Lemma 1.** For every positive integer \( n \), the system \( \mathcal{V}_n \) has exactly one solution in integers greater than 1, namely \( (f(1), \ldots, f(n)) \).
Let
$$H_n = \{x_i! = x_k : i, k \in \{1, \ldots, n\}\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$$

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

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

**Theorem 6.** Every statement $\Theta_n$ is true with an unknown integer bound that depends on $n$.

**Proof.** It follows from Lemma 2. $\Box$

**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 $x \geq 4$, then $\frac{(x-1)! + 1}{x} > 1$.

**Lemma 5.** (Wilson’s theorem, [6, p. 89]). For every integer $x \geq 2$, $x$ 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 [14]. It is conjectured that $x! + 1$ is a square only for $x \in \{4, 5, 7\}$, see [21, p. 297].

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

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

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

5
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:

\[
\begin{align*}
x_2 &= x_1! \\
x_3 &= (x_1)! \\
x_5 &= x_1! + 1 \\
x_6 &= (x_1! + 1)!
\end{align*}
\]

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

Proof. It follows from Lemma 3.

Theorem 7. The statement \( \Theta_6 \) 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 \( x_1 \leq f(6) \).

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 \( \Theta_6 \) implies that \( x_1 = \min(x_1, \ldots, x_6) \leq f(6) \).

Hypothesis 2. The implication in Theorem 7 is true.

Corollary 6. 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 [12, pp. 37–38]. Let \( B \) denote the following system of equations:

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

Lemma 3 and the diagram in Figure 3 explain the construction of the system \( B \).

![Fig. 3 Construction of the system \( B \)](image)

**Lemma 7.** For every integer \( x_1 \geq 2 \), the system \( B \) 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:

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

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

**Proof.** By Lemmas 3 and 4, for every integer \(x_1 \geq 2\), the system \(B\) 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. \(\square\)

**Theorem 8.** The statement \(\Theta_9\) 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 \((x_1, x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9\) such that the tuple \((x_1, x_2, \ldots, x_9)\) solves the system \(B\). Lemma 7 guarantees that \(\min(x_1, \ldots, x_9) = x_1\). Since \(B \subseteq H_9\), the statement \(\Theta_9\) and the inequality \(\min(x_1, \ldots, x_9) = x_1 > f(9)\) imply that the system \(B\) 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 \(n^2 + 1\). \(\square\)

**Hypothesis 3.** The implication in Theorem 8 is true.

**Corollary 7.** 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 8, assuming the statement \(\Theta_9\), we can infer the statement \(\forall n \in \mathbb{N} \ \Omega(n)\) from any statement \(\Omega(n)\) with \(n \geq f(9)\). A similar situation holds for inference by the so called "super-induction method", see [22]–[25]. 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 [11] p. 443 and [18]. Let $G$ denote the following system of equations:

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

Lemma 3 and the diagram in Figure 4 explain the construction of the system $G$.

**Fig. 4** Construction of the system $G$

**Lemma 8.** For every integer $x_1 \geq 2$, the system $G$ 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:

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

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

**Proof.** By Lemmas 3 and 4, for every integer \(x_1 \geq 2\), the system \(G\) 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. \(\square\)

**Theorem 9.** The statement \(\Theta_9\) 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 \(G\). Lemma 8 guarantees that \(\min(x_1, \ldots, x_9) = x_1\). Since \(G \subseteq H_9\), the statement \(\Theta_9\) and the inequality \(\min(x_1, \ldots, x_9) = x_1 > f(9)\) imply that the system \(G\) 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 \(n! + 1\). \(\square\)

**Hypothesis 4.** The implication in Theorem 9 is true.

**Corollary 8.** 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 [12, p. 39].

Let $C$ denote the following system of equations:

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

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:

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

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

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

Hence, the claim of Lemma 11 follows from Lemma 5. □
Theorem 10. The statement $\Theta_{16}$ 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 $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0, 1\})^{14}$ such that the tuple $(x_1, \ldots, x_{16})$ solves the system $C$. Lemma 11 guarantees that $\min(x_1, \ldots, x_{16}) = x_1 = x_9 - 3 > f(16)$. Since $C \subseteq H_{16}$, the statement $\Theta_{16}$ and the inequality $\min(x_1, \ldots, x_{16}) > f(16)$ imply that the system $C$ has infinitely many solutions in integers $x_1, \ldots, x_{16}$ greater than 1. According to Lemmas 9–11, there are infinitely many twin primes. $\square$

Hypothesis 5. The implication in Theorem 10 is true.

Corollary 9. (cf. [3]). 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 [11, 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 [11, p. 1].

Open Problem. ([11, 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 [10, p. 23].

Theorem 11. ([19]). An unproven inequality stated in [19] implies that $2^{2^n} + 1$ is composite for every integer $n \geqslant 5$.

Lemma 12. ([11, 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 10. Since $k \cdot 2^{2^n} + 1 + 1 \geqslant 2^n + 1 + 1 \geqslant n + 3$, 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

$$G_n = \left\{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \right\} \cup \left\{ 2^{2^n} = x_k : i, k \in \{1, \ldots, n\} \right\}$$
Lemma 13. The following subsystem of $G_n$

\[
\begin{aligned}
& x_1 \cdot x_1 = x_1 \\
& \forall i \in \{1, \ldots, n-1\} \quad 2^{2^x_i} = x_{i+1}
\end{aligned}
\]

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

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

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

Theorem 12. Every statement $\Psi_n$ 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 $2^{2^b} \cdot 2^b = 2^c$.

Theorem 13. The statement $\Psi_{13}$ 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

\[ (x + 1)(y + 1) = 2^z + 1 \quad (1) \]

in positive integers. By Lemma 15, we can transform equation (1) into an equivalent system $\mathcal{F}$ which has 13 variables $(x, y, z, \text{and 10 other variables})$ and which consists of equations of the forms $\alpha \cdot \beta = \gamma$ and $2^{2^\alpha} = \gamma$, see the diagram in Figure 6.
Assume that $2^{n^2} + 1$ is composite for some integer $n > g(13)$. By this and Corollary 10, equation (11) 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 $F$ 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 $\Psi_{13}$ implies that the system $F$ has infinitely many solutions in positive integers. Therefore, there are infinitely many positive integers $n$ such that $2^{n^2} + 1$ is composite. \hfill \Box

Hypothesis 6. The implication in Theorem 13 is true.
Corollary 11. 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 A computer-assisted proof that a certain subset of $\mathbb{N} \setminus \{0\}$ is cofinite

The following lemma is known as Richert’s lemma or Richert’s theorem.

**Lemma 16.** ([14], [16], [17, p. 152]). Let $\{m_i\}_{i=1}^{\infty}$ be an increasing sequence of positive integers such that for some positive integer $k$ the inequality $m_{i+1} \leq 2m_i$ holds for all $i > k$. Suppose there exists a non-negative integer $b$ such that the numbers $b + 1$, $b + 2$, $b + 3$, $\ldots$, $b + m_{k+1}$ are all expressible as sums of one or more distinct elements of the set $\{m_1, \ldots, m_k\}$. Then every integer greater than $b$ is expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$.

**Corollary 12.** If the sequence $\{m_i\}_{i=1}^{\infty}$ is computable and the algorithm in Flowchart 1 terminates, then almost all positive integers are expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$. 
Input the smallest integer $k \geq 2$ such that the inequality $m_i + 1 \leq 2m_i$ holds for all $i > k$.

$k := k + 1$

$A := \{m_1, \ldots, m_k\}$

$B := \{m_1\}$

$i := 2$

$B := B \cup \{m_i\} \cup \{B[j] + m_i : j \in \{1, \ldots, \text{card}(B)\}\}$

Order the set $B$

$i := i + 1$

Is $i = k + 1$?

Does $B$ contain $m_k + 1$ consecutive integers?

Yes

Print "Almost all positive integers are expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$".

No

Stop

Flowchart 1

For a large class of sequences $\{m_i\}_{i=1}^{\infty}$ the converse is true: if almost all positive integers are expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$, then the algorithm in Flowchart 1 terminates, see [9, Theorem 2.3].
Let \([\cdot]\) denote the integer part function. For a positive integer \(i\), let \(t_i = \frac{(i + 19)^{i + 19}}{(i + 19)! \cdot 2^{i + 19}}\), and let \(m_i = [t_i]\). Let \(\mathcal{T}\) denote the set of all positive integers which are expressible as a sum of one or more distinct elements of the set \(\{m_i : i \in \mathbb{N} \setminus \{0\}\}\).

**Lemma 17.** The inequality \(m_{i+1} \leq 2m_i\) holds for every positive integer \(i\).

**Proof.** For every positive integer \(i\),

\[
\frac{m_i}{m_{i+1}} = \frac{[t_i]}{[t_{i+1}]} > \frac{t_i - 1}{t_{i+1}} = \left(\frac{t_i}{t_{i+1}}\right) - \left(\frac{1}{t_{i+1}}\right) \geq \left(\frac{t_i}{t_{i+1}}\right) - \left(\frac{1}{t_2}\right) =
\]

\[
2 \cdot \frac{i + 20}{i + 19} \cdot \left(1 - \frac{1}{i + 20}\right)^{i + 20} - \left(\frac{21! \cdot 2^{21}}{2^{21}}\right) > 2 \cdot \left(1 - \frac{1}{21}\right)^{21} - \left(\frac{21! \cdot 2^{21}}{2^{21}}\right) =
\]

\[
\frac{4087158528447152485120000}{5842587018385982521381124421}
\]

The above fraction was computed by MuPAD and is greater than \(\frac{1}{2}\). \(\square\)

**Theorem 14.** The algorithm in Flowchart 1 terminates for the sequence \(\{m_i\}_{i=1}^\infty\). 2761 is the largest integer which does not belong to \(\mathcal{T}\).

**Proof.** By Lemma 17 we take \(k = 2\) as the initial value of \(k\). The first 15 lines of the MuPAD code below describe the algorithm in Flowchart 1. It follows from the fact that MuPAD automatically orders every finite set of integers.

**MuPAD code**

```
TEXTWIDTH:=80:
k:=2:
repeat
C:={floor((i+19)^((i+19)/((i+19)!*2^(i+19))) $i=1..k+1}:
A:={floor((i+19)^((i+19)/((i+19)!*2^(i+19))) $i=1..k}:
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:
G:={y $y=B[1]-1..B[nops(B)]+1} minus B:
H:={G[n+1]-G[n] $n=1..nops(G)-1}:
k:=k+1:
until H[nops(H)]>C[nops(C)] end_repeat:
print(Unquoted, "Almost all positive integers are expressible as a sum of"):
```
\textbf{Output}

Almost all positive integers are expressible as a sum of
one or more distinct elements of the set \(\{m_1, m_2, m_3, \ldots\}\)

\begin{align*}
15 \\
\{41, 54, 72, 96, 128, 170, 227, 303, 404, 540, 722, 966, 1293, 1730, 2317, 3105\} \\
\{2761\} \\
\{\} 
\end{align*}

The output indicates that the algorithm in Flowchart 1 terminates and 15 is the smallest value of \(k\) which satisfies the condition of Lemma 16. The last three instructions list the following sets:

\begin{align*}
\{m_i : i \in \{1, \ldots, 16\}\}, \\
\{2761\} \setminus B, \\
\{2761 + 1, \ldots, 2761 + m_{16}\} \setminus B,
\end{align*}

where \(B\) denotes the set of all positive integers which are expressible as a sum of one or more distinct elements of the set \(\{m_i : i \in \{1, \ldots, 15\}\}\). Since the set \(\{2761\}\) equals \(\{2761\} \setminus B\), we conclude that \(2761 \not\in B\). By this and the inequality \(m_{16} = 3105 > 2761\), we conclude that \(2761 \not\in T\).

Since the empty set \(\{\}\) equals

\[\{2761 + 1, \ldots, 2761 + m_{16}\} \setminus B\]

we conclude that each of the integers

\[2761 + 1, 2761 + 2, 2761 + 3, \ldots, 2761 + m_{16}\]

belongs to \(B\). Consequently, in virtue of Lemma 17, we can apply Lemma 16 with \(k = 15\) and \(b = 2761\) to confirm that every integer greater than 2761 belongs to \(T\). \(\square\)
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](https://doi.org/10.1090/S0025-5718-01-01315-1).


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