On ZFC-formulae $\varphi(x)$ for which we know a non-negative integer $n$ such that $\{x \in \mathbb{N} : \varphi(x)\} \subseteq \{x \in \mathbb{N} : x \leq n - 1\}$ if the set $\{x \in \mathbb{N} : \varphi(x)\}$ is finite

Apoloniusz Tyszka

Abstract

Let $g(3) = 4$, and let $g(n + 1) = g(n)!$ for every integer $n \geq 3$. For an integer $n \in \{3, \ldots, 16\}$, let $\Psi_n$ denote the following statement: if a system of equations $S \subseteq \{x_i = x_k : (i, k) \in \{1, \ldots, n\} \land (i \neq k)\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leq g(n)$. For every statement $\Psi_n$, the bound $g(n)$ cannot be decreased. The author’s hypothesis says that the statements $\Psi_3, \ldots, \Psi_{16}$ hold true. We say that a non-negative integer $m$ is a threshold number of a set $X \subseteq \mathbb{N}$, if $X$ is infinite if and only if $X$ contains an element greater than $m$. The following problem is open: define a set $X \subseteq \mathbb{N}$ that satisfies the following conditions: (1) the relation $n \in X$ is simple and has the same intuitive meaning for every $n \in \mathbb{N}$, (2) a known algorithm for every $n \in \mathbb{N}$ decides whether or not $n \in X$, (3) a known algorithm returns a threshold number of $X$, (4) new elements of $X$ are still discovered, (5) we do not know any algorithm deciding the finiteness of $X$. We define a set $X \subseteq \mathbb{N}$ that satisfies conditions (2)-(5). The statement $\Psi_3$ implies that the set of primes of the form $n^2 + 1$ solves the problem and the set of primes of the form $n! + 1$ solves the problem. The statement $\Psi_{16}$ implies that the set of twin primes solves the problem.

Key words and phrases: Brocard-Ramanujan equation $x! + 1 = y^2$, composite Fermat numbers, decidability in the limit, finiteness of a set, incompleteness of ZFC, infiniteness of a set, prime numbers of the form $n^2 + 1$, prime numbers of the form $n! + 1$, single query to an oracle for the halting problem, twin primes.

2010 Mathematics Subject Classification: 03D20, 11A41.

1 Introduction

The phrase "we know a non-negative integer $n$" in the title means that we know an algorithm which returns $n$. The title cannot be formalised in ZFC because the phrase "we know a non-negative integer $n$" refers to currently known non-negative integers $n$ with some property. A formally stated title may look like this: On ZFC-formulae $\varphi(x)$ for which there exists a non-negative integer $n$ such that ZFC proves that

$$\text{card}(\{x \in \mathbb{N} : \varphi(x)\}) < \infty \iff \{x \in \mathbb{N} : \varphi(x)\} \subseteq \{x \in \mathbb{N} : x \leq n - 1\}$$

Unfortunately, this formulation admits formulae $\varphi(x)$ without any known non-negative integer $n$ such that ZFC proves the above implication.

Lemma 1. For every non-negative integer $n$, $\text{card}(\{x \in \mathbb{N} : x \leq n - 1\}) = n$.

Corollary 1. The title altered to "On ZFC-formulae $\varphi(x)$ for which we know a non-negative integer $n$ such that $\text{card}(\{x \in \mathbb{N} : \varphi(x)\}) \leq n$ if the set $\{x \in \mathbb{N} : \varphi(x)\}$ is finite" involves a weaker assumption on $\varphi(x)$.
2 Subsets of \( \mathbb{N} \) and their threshold numbers

We say that a non-negative integer \( m \) is a threshold number of a set \( X \subseteq \mathbb{N} \), if \( X \) is infinite if and only if \( X \) contains an element greater than \( m \), cf. [28] and [29]. If a set \( X \subseteq \mathbb{N} \) is empty or infinite, then any non-negative integer \( m \) 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 \( \{ \max(X), \max(X) + 1, \max(X) + 2, \ldots \} \).

It is conjectured that the set of prime numbers of the form \( n^2 + 1 \) is infinite, see [17] pp. 37–38. It is conjectured that the set of prime numbers of the form \( n! + 1 \) is infinite, see [3] p. 443. A twin prime is a prime number that differs from another prime number by 2. The twin prime conjecture states that the set of twin primes is infinite, see [17] p. 39. It is conjectured that the set of composite numbers of the form \( 2^{2^n} + 1 \) is infinite, see [12] p. 23 and [13] pp. 158–159. A prime \( p \) is said to be a Sophie Germain prime if both \( p \) and \( 2p + 1 \) are prime, see [26]. It is conjectured that the set of Sophie Germain primes is infinite, see [20] p. 330. For each of these sets, we do not know any threshold number.

The following statement: for every non-negative integer \( n \) there exist prime numbers \( p \) and \( q \) such that \( p + 2 = q \) and \( p \in [10^n, 10^{n+1}] \). (T)
is a \( \Pi_1 \) statement which strengthens the twin prime conjecture, see [4] p. 43]. C. H. Bennett claims that most mathematical conjectures can be settled indirectly by proving stronger \( \Pi_1 \) statements, see [1]. The statement (T) is equivalent to the non-halting of a Turing machine. If a set \( X \subseteq \mathbb{N} \) is computable and we know a threshold number of \( X \), then the infinity of \( X \) is equivalent to the halting of a Turing machine.

The height of a rational number \( \frac{p}{q} \) is denoted by \( H(\frac{p}{q}) \) and equals \( \max(|p|,|q|) \) provided \( \frac{p}{q} \) is written in lowest terms. The height of a rational tuple \( (x_1, \ldots, x_n) \) is denoted by \( H(x_1, \ldots, x_n) \) and equals \( \max(H(x_1), \ldots, H(x_n)) \).

**Proposition 1.** The equation \( x^5 - x = y^2 - y \) has only finitely many rational solutions, see [16] p. 212. The known rational solutions are \((x, y) = (-1, 0), (-1, 1), (0, 0), (0, 1), (1, 0), (1, 1), (2, -5), (2, 6), (3, -15), (3, 16), (30, -4929), (30, 4930), (\frac{1}{16}, \frac{15}{16}), (\frac{1}{16}, \frac{17}{16}), (-\frac{15}{16}, -\frac{185}{16}), (-\frac{15}{16}, \frac{1209}{16}), \) and the existence of other solutions is an open question, see [21] pp. 223–224.

**Corollary 2.** The set \( T = \{ n \in \mathbb{N} : \text{the equation } x^5 - x = y^2 - y \text{ has a rational solution of height } n \} \) is finite. We know an algorithm which for every \( n \in \mathbb{N} \) decides whether or not \( n \in T \). We do not know any algorithm which returns a threshold number of \( T \).

**Open Problem 1.** (cf. Corollary [3]) Define a set \( X \subseteq \mathbb{N} \) that satisfies the following conditions:

1. the relation \( n \in X \) is simple and has the same intuitive meaning for every \( n \in \mathbb{N} \),
2. a known algorithm for every \( n \in \mathbb{N} \) decides whether or not \( n \in X \),
3. a known algorithm returns a threshold number of \( X \),
4. new elements of \( X \) are still discovered,
5. we do not know any algorithm deciding the finiteness of \( X \).

Let \( L \) denote the following system of equations:

\[
\begin{align*}
x^2 + y^2 &= s^2 \\
x^2 + z^2 &= t^2 \\
y^2 + z^2 &= u^2 \\
x^2 + y^2 + z^2 &= v^2
\end{align*}
\]

Let \( T \) denote the set

\[
\{ k \in \mathbb{N} \setminus \{0\} : \left( \text{the system } L \text{ has no solutions in } \{1, \ldots, k\} \right) \land \\
\left( \text{the system } L \text{ has a solution in } \{1, \ldots, k+1\} \right) \}
\]

2
Let $\mathcal{P}$ denote the set of prime numbers, and let $\mathcal{Z}$ denote the set

$$\{k \in \mathbb{N} \setminus \{0\} : \text{the system } \mathcal{L} \text{ has a solution in } \{1, \ldots, k\}^7\}$$

A perfect cuboid is a cuboid having integer side lengths, integer face diagonals, and an integer space diagonal.

**Proposition 2.** ([25]) No perfect cuboids are known.

**Corollary 3.** (cf. Open Problem 1) The set $\mathcal{Z} \cup (\left\lbrack 2, 99999 \right\rbrack \cap \mathcal{P})$ satisfies conditions (2)-(5).

**Corollary 4.** We know an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in \mathcal{F}$. ZFC proves that $\text{card}(\mathcal{F}) \in \{0, 1\}$. We do not know any algorithm which returns $\text{card}(\mathcal{F})$. We do not know any algorithm which returns a threshold number of $\mathcal{F}$.

Let

$$\mathcal{H} = \begin{cases} \mathbb{N}, & \text{if } \sin\left(\frac{99999}{99999}\right) < 0 \\ \mathbb{N} \cap \left\lbrack \frac{99999}{99999} \cdot 99999 \right\rbrack, & \text{otherwise} \end{cases}$$

We do not know whether or not the set $\mathcal{H}$ is finite.

**Proposition 3.** The number $99999$ is a threshold number of $\mathcal{H}$. We know an algorithm which decides the equality $\mathcal{H} = \mathbb{N}$. If $\mathcal{H} \neq \mathbb{N}$, then the set $\mathcal{H}$ consists of all integers from 0 to a non-negative integer which can be computed by a known algorithm. We know an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in \mathcal{H}$.

Let

$$\mathcal{K} = \begin{cases} \{n\}, & \text{if } (n \in \mathbb{N}) \land \left(2^{\aleph_0} = \aleph_{n+1}\right) \\ \{0\}, & \text{if } 2^{\aleph_0} > \aleph_\omega \end{cases}$$

**Theorem 1.** ZFC proves that $\text{card}(\mathcal{K}) = 1$. If ZFC is consistent, then for every $n \in \mathbb{N}$ the sentences "$n$ is a threshold number of $\mathcal{K}$" and "$n$ is not a threshold number of $\mathcal{K}$" are not provable in ZFC. If ZFC is consistent, then for every $n \in \mathbb{N}$ the sentences "$n \in \mathcal{K}$" and "$n \notin \mathcal{K}$" are not provable in ZFC.

**Proof.** It suffices to observe that $2^{\aleph_0}$ can attain every value from the set $\{\aleph_1, \aleph_2, \aleph_3, \ldots\}$, see [8] and [11, p. 232].

**3 A Diophantine equation whose non-solvability expresses the consistency of ZFC**

Gödel’s second incompleteness theorem and the Davis-Putnam-Robinson- Matiyasevich theorem imply the following theorem.

**Theorem 2.** ([6, 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.

**Remark 1.** ([5, 17 p. 53]) The polynomial $D(x_1, \ldots, x_m)$ is very complicated.
Let \( \mathcal{Y} \) 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, there exists an algorithm which for every \( n \in \mathbb{N} \) decides whether or not \( n \in \mathcal{Y} \). Theorem 3 implies the next theorem.

**Theorem 3.** For every \( n \in \mathbb{N} \), ZFC proves that \( n \in \mathcal{Y} \). If ZFC is arithmetically consistent, then the sentences "\( \mathcal{Y} \) is finite" and "\( \mathcal{Y} \) is infinite" are not provable in ZFC. If ZFC is arithmetically consistent, then for every \( n \in \mathbb{N} \) the sentences "\( n \) is a threshold number of \( \mathcal{Y} \)" and "\( n \) is not a threshold number of \( \mathcal{Y} \)" are not provable in ZFC.

Let \( \mathcal{E} \) denote the set of all non-negative integers \( k \) such that the equation \( D(x_1, \ldots, x_m) = 0 \) has a solution in \( \{0, \ldots, k\}^m \). Since the set \( \{0, \ldots, k\}^m \) is finite, there exists an algorithm which for every \( n \in \mathbb{N} \) decides whether or not \( n \in \mathcal{E} \). Theorem 3 implies the next theorem.

**Theorem 4.** The set \( \mathcal{E} \) is empty or infinite. In both cases, every non-negative integer \( n \) is a threshold number of \( \mathcal{E} \). If ZFC is arithmetically consistent, then the sentences "\( \mathcal{E} \) is empty", "\( \mathcal{E} \) is not empty", "\( \mathcal{E} \) is finite", and "\( \mathcal{E} \) is infinite" are not provable in ZFC.

Let \( \mathcal{V} \) denote the set

\[
\{ k \in \mathbb{N} : \text{(the polynomial } D(x_1, \ldots, x_m) \text{ has no solutions in } \{0, \ldots, k\}^m) \land \\
\text{(the polynomial } D(x_1, \ldots, x_m) \text{ has a solution in } \{0, \ldots, k \cdot 1\}^m) \}.
\]

Since the sets \( \{0, \ldots, k\}^m \) and \( \{0, \ldots, k \cdot 1\}^m \) are finite, there exists an algorithm which for every \( n \in \mathbb{N} \) decides whether or not \( n \in \mathcal{V} \). According to Remark 1, at present we are not able to write a computer program that realizes such an algorithm. Theorem 5 implies the next theorem.

**Theorem 5.** (6) ZFC proves that \( \text{card}(\mathcal{V}) \in \{0, 1\} \). (7) For every \( n \in \mathbb{N} \), ZFC proves that \( n \notin \mathcal{V} \). (8) ZFC does not prove the emptiness of \( \mathcal{V} \), if ZFC is arithmetically consistent. (9) For every \( n \in \mathbb{N} \), the sentence "\( n \) is a threshold number of \( \mathcal{V} \)" is not provable in ZFC, if ZFC is arithmetically consistent. (10) For every \( n \in \mathbb{N} \), the sentence "\( n \) is not a threshold number of \( \mathcal{V} \)" is not provable in ZFC, if ZFC is arithmetically consistent.

**Open Problem 2.** Define a simple algorithm \( A \) such that \( A \) returns 0 or 1 on every input \( k \in \mathbb{N} \) and the set

\[
\mathcal{V} = \{ k \in \mathbb{N} : \text{the program } A \text{ returns 1 on input } k \}
\]

satisfies conditions (6)–(10).

## 4 Basic lemmas

**Lemma 2.** For every positive integers \( x \) and \( y \), \( x! \cdot y! = y! \cdot x! \) if and only if

\[
(x + 1 = y) \lor (x = y = 1)
\]

Let \( \Gamma(k) \) denote \( (k - 1)! \).

**Lemma 3.** For every positive integers \( x \) and \( y \), \( x \cdot \Gamma(x) = \Gamma(y) \) if and only if

\[
(x + 1 = y) \lor (x = y = 1)
\]

**Lemma 4.** For every non-negative integers \( b \) and \( c \), \( b + 1 = c \) if and only if

\[
2^{2^b} \cdot 2^{2^b} = 2^{2^c}
\]

**Lemma 5.** (Wilson’s theorem, [9, p. 89]). For every positive integer \( x \), \( x \) divides \( (x - 1)! + 1 \) if and only if \( x = 1 \) or \( x \) is prime.
5 Hypothetical statements $\Psi_3, \ldots, \Psi_{16}$

For an integer $n \geq 3$, let $U_n$ denote the following system of equations:

$$\begin{align*}
\forall i \in \{1, \ldots, n-1\} \setminus \{2\} & \quad x_i! = x_{i+1} \\
& \quad x_1 \cdot x_2 = x_3 \\
& \quad x_2 \cdot x_2 = x_3
\end{align*}$$

The diagram in Figure 1 illustrates the construction of the system $U_n$.

Let $g(3) = 4$, and let $g(n + 1) = g(n)!$ for every integer $n \geq 3$.

**Lemma 6.** For every integer $n \geq 3$, the system $U_n$ has exactly two solutions in positive integers, namely $(1, \ldots, 1)$ and $(2, 2, g(3), \ldots, g(n))$.

Let

$$B_n = \{x_i! = x_k : (i, k \in \{1, \ldots, n\}) \land (i \neq k)\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$$

For an integer $n \geq 3$, let $\Psi_n$ denote the following statement: if a system of equations $S \subseteq B_n$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leq g(n)$. The statement $\Psi_n$ says that for subsystems of $B_n$ the largest known solution is indeed the largest possible.

**Hypothesis 1.** The statements $\Psi_3, \ldots, \Psi_{16}$ are true.

**Remark 2.** By Lemma 2 and algebraic lemmas in [23, p. 110], the statement $\forall n \in \mathbb{N} \setminus \{0, 1, 2\} \Psi_n$ implies that there is an algorithm which takes as input a factorial Diophantine equation, and returns an integer such that this integer is greater than the solutions in positive integers, if these solutions form a finite set. This conclusion is a bit strange because a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [15, p. 300]. Therefore, the statement $\forall n \in \mathbb{N} \setminus \{0, 1, 2\} \Psi_n$ seems to be false.

**Lemma 7.** 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. \hfill \Box

**Lemma 8.** For every statement $\Psi_n$, the bound $g(n)$ cannot be decreased.

**Proof.** It follows from Lemma 6 because $U_n \subseteq B_n$. \hfill \Box
6  The Brocard-Ramanujan equation \( x! + 1 = y^2 \)

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

\[
\begin{aligned}
x_1! & = x_2 \\
x_2! & = x_3 \\
x_5! & = x_6 \\
x_4 \cdot x_4 & = x_5 \\
x_3 \cdot x_5 & = x_6
\end{aligned}
\]

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

**Lemma 9.** For every \( x_1, x_4 \in \mathbb{N} \setminus \{0, 1\} \), the system \( \mathcal{A} \) is solvable in positive integers \( x_2, x_3, x_5, x_6 \) 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:

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

**Proof.** It follows from Lemma 2. \( \square \)

It is conjectured that \( x! + 1 \) is a perfect square only for \( x \in \{4, 5, 7\} \), see [24, p. 297]. A weak form of Szpiro’s conjecture implies that there are only finitely many solutions to the equation \( x! + 1 = y^2 \), see [18].

**Theorem 6.** If the equation \( x! + 1 = x_4^2 \) has only finitely many solutions in positive integers, then the statement \( \Psi_6 \) guarantees that each such solution \( (x_1, x_4) \) belongs to the set \( \{(4, 5), (5, 11), (7, 71)\} \).

**Proof.** Suppose that the antecedent holds. 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 9 the system \( \mathcal{A} \) is solvable in positive integers \( x_2, x_3, x_5, x_6 \). Since \( \mathcal{A} \subseteq B_6 \), the statement \( \Psi_6 \) implies that \( x_6 = (x_1! + 1)! \leq g(6) = g(5)! \). Hence, \( x_1! + 1 \leq g(5) = g(4)! \). Consequently, \( x_1 < g(4) = 24 \). If \( x_1 \in \{1, \ldots, 23\} \), then \( x_1! + 1 \) is a perfect square only for \( x_1 \in \{4, 5, 7\} \). \( \square \)

7  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 [17, pp. 37–38]. Let \( \mathcal{B} \) denote the following system of equations:

\[
\begin{aligned}
x_2! & = x_3 \\
x_3! & = x_4 \\
x_5! & = x_6 \\
x_8! & = x_9
\end{aligned}
\]

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

Lemma 2 and the diagram in Figure 3 explain the construction of the system \( \mathcal{B} \).
Lemma 10. For every integer \( x_1 \geq 2 \), the system \( \mathcal{B} \) 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:

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

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

**Proof.** By Lemma 2, for every integer \( x_1 \geq 2 \), the system \( \mathcal{B} \) 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 10 follows from Lemma 5. \( \square \)

Lemma 11. There are only finitely many tuples \((x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9\) which solve the system \( \mathcal{B} \) and satisfy \( x_1 = 1 \).

**Proof.** If a tuple \((x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9\) solves the system \( \mathcal{B} \) and \( x_1 = 1 \), then \( x_1, \ldots, x_9 \leq 2 \). Indeed, \( x_1 = 1 \) implies that \( x_2 = x_1^2 = 1 \). Hence, for example, \( x_3 = x_2! = 1 \). Therefore, \( x_8 = x_3 + 1 = 2 \) or \( x_8 = 1 \). Consequently, \( x_9 = x_8! \leq 2 \). \( \square \)

Theorem 7. (cf. Theorem 11) The statement \( \Psi_9 \) proves the following implication: if there exists an integer \( x_1 \geq 2 \) such that \( x_1^2 + 1 \) is prime and greater than \( g(7) \), then there are infinitely many primes of the form \( n^2 + 1 \).

**Proof.** Suppose that the antecedent holds. By Lemma 10, 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 \( \mathcal{B} \). Since \( x_1^2 + 1 > g(7) \), we obtain that \( x_1^2 > g(7) \). Hence, \((x_1^2)! \geq g(7)! = g(8)\). Consequently,

\[
x_9 = ((x_1^2)! + 1)! \geq (g(8) + 1)! > g(8)! = g(9)
\]

Since \( \mathcal{B} \subseteq B_9 \), the statement \( \Psi_9 \) and the inequality \( x_9 > g(9) \) imply that the system \( \mathcal{B} \) has infinitely many solutions \((x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9\). According to Lemmas 10 and 11, there are infinitely many primes of the form \( n^2 + 1 \). \( \square \)

Corollary 5. Let \( X_9 \) denote the set of primes of the form \( n^2 + 1 \). The statement \( \Psi_9 \) implies that we know an algorithm such that it returns a threshold number of \( X_9 \), and this number equals \( \max(X_9) \), if \( X_9 \) is finite. Assuming the statement \( \Psi_9 \), a single query to an oracle for the halting problem decides the infinity of \( X_9 \). Assuming the statement \( \Psi_9 \), the infinity of \( X_9 \) is decidable in the limit.

**Proof.** We consider an algorithm which computes \( \max(X_9 \cap [1, g(7)]) \). \( \square \)
8 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 [3, p. 443].

**Theorem 8.** (cf. Theorem [12]) The statement $\Psi_9$ proves the following implication: if there exists an integer $x_4 \geq g(6)$ such that $x_4! + 1$ is prime, then there are infinitely many primes of the form $n! + 1$.

**Proof.** We leave the analogous proof to the reader. 

9 The twin prime conjecture

A twin prime is a prime number that differs from another prime number by 2. The twin prime conjecture states that there are infinitely many twin primes, see [17, p. 39]. Let $C$ denote the following system of equations:

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

Lemma [2] and the diagram in Figure 4 explain the construction of the system $C$.

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

**Lemma 12.** For every $x_4, x_9 \in \mathbb{N} \setminus \{0, 1, 2\}$, the system $C$ is solvable in positive integers $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$ 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:
Lemma 13. There are only finitely many tuples $(x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ which solve the system $C$ and satisfy $(x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})$.

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

\[
\left( x_4 + 2 = x_9 \right) \land \left( x_4(x_4 - 1) + 1 \right) \land \left( x_9(x_9 - 1) + 1 \right)
\]

Hence, the claim of Lemma [12] follows from Lemma [5].

Lemma 13. There are only finitely many tuples $(x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ which solve the system $C$ and satisfy $(x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})$.

Theorem 9. (cf. Theorem [13]) The statement $\Psi_{16}$ proves the following implication: if there exists a twin prime greater than $g(14)$, then there are infinitely many twin primes.

Proof. Suppose that the antecedent holds. Then, there exist prime numbers $x_4$ and $x_9$ such that $x_9 = x_4 + 2 > g(14)$. Hence, $x_4, x_9 \in \mathbb{N} \setminus \{0, 1, 2\}$. By Lemma [12] there exists a unique tuple

\[
(x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0\})^{14}
\]

such that the tuple $(x_1, \ldots, x_{16})$ solves the system $C$. Since $x_9 > g(14)$, we obtain that $x_9 - 1 \geq g(14)$. Therefore, $(x_9 - 1)! \geq g(14)! = g(15)$. Hence, $(x_9 - 1)! + 1 > g(15)!$. Consequently,

\[
x_{16} = ((x_9 - 1)! + 1)! > g(15)! = g(16)
\]

Since $C \subseteq B_{16}$, the statement $\Psi_{16}$ and the inequality $x_{16} > g(16)$ imply that the system $C$ has infinitely many solutions in positive integers $x_1, \ldots, x_{16}$. According to Lemmas [12] and [13] there are infinitely many twin primes.

Corollary 6. (cf. [17]) Let $X_{16}$ denote the set of twin primes. The statement $\Psi_{16}$ implies that we know an algorithm such that it returns a threshold number of $X_{16}$, and this number equals $\max(X_{16})$. If $X_{16}$ is finite. Assuming the statement $\Psi_{16}$, a single query to an oracle for the halting problem decides the infinity of $X_{16}$. Assuming the statement $\Psi_{16}$, the infinity of $X_{16}$ is decidable in the limit.

Proof. We consider an algorithm which computes $\max(X_{16} \cap [1, g(14)])$.

10 Hypothetical statements $\Delta_5, \ldots, \Delta_{14}$ and their consequences

Let $\lambda(5) = \Gamma(25)$, and let $\lambda(n + 1) = \Gamma(\lambda(n))$ for every integer $n \geq 5$. For an integer $n \geq 5$, let $\mathcal{J}_n$ denote the following system of equations:

\[
\left\{
\begin{array}{ll}
\forall i \in \{1, \ldots, n-1\} \setminus \{3\} \; \Gamma(x_i) &= x_{i+1} \\
x_1 \cdot x_1 &= x_4 \\
x_2 \cdot x_3 &= x_5
\end{array}
\right.
\]

Lemma [3] and the diagram in Figure 5 explain the construction of the system $\mathcal{J}_n$.  

9
For every integer \( n \geq 5 \), the system \( \mathcal{J}_n \) has exactly two solutions in positive integers, namely \((1, \ldots, 1)\) and \((5, 24, 23!, 25, \lambda(5), \ldots, \lambda(n))\). For an integer \( n \geq 5 \), let \( \Delta_n \) denote the following statement: if a system of equations \( S \subseteq \{ \Gamma(x_i) = x_k : i, k \in \{1, \ldots, n\} \} \cup \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \) has only finitely many solutions in positive integers \( x_1, \ldots, x_n \), then each such solution \((x_1, \ldots, x_n)\) satisfies \( x_1, \ldots, x_n \leq \lambda(n) \).

**Hypothesis 2.** The statements \( \Delta_5, \ldots, \Delta_{14} \) are true.

**Proposition 4.** Lemmas 3 and 5 imply that the statements \( \Delta_n \) have similar consequences as the statements \( \Psi_n \).

**Remark 3.** By Lemma 3 and algebraic lemmas in [23, p. 110], the statement \( \forall n \in \mathbb{N} \setminus \{0, 1, 2, 3, 4\} \Delta_n \) implies that there is an algorithm which takes as input a factorial Diophantine equation, and returns an integer such that this integer is greater than the solutions in positive integers, if these solutions form a finite set. This conclusion is a bit strange because a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [15, p. 300]. Therefore, the statement \( \forall n \in \mathbb{N} \setminus \{0, 1, 2, 3, 4\} \Delta_n \) seems to be false.

**Theorem 10.** The statement \( \Delta_6 \) implies that any prime number \( p \geq 25 \) proves the infinitude of primes.

**Proof.** It follows from Lemmas 3 and 5. We leave the details to the reader. \( \Box \)

### 11 Hypothetical statements \( \Sigma_3, \ldots, \Sigma_{16} \) and their consequences

Let \( \Gamma_n(k) \) denote \((k - 1)!, \) where \( n \in \{3, \ldots, 16\} \) and \( k \in \{2\} \cup \{2^{2n-3} + 1, \infty\} \cap \mathbb{N} \). For an integer \( n \in \{3, \ldots, 16\} \), let

\[
Q_n = \{ \Gamma_n(x_i) = x_k : i, k \in \{1, \ldots, n\} \} \cup \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \}
\]

For an integer \( n \in \{3, \ldots, 16\} \), let \( P_n \) denote the following system of equations:

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

**Lemma 14.** For every integer \( n \in \{3, \ldots, 16\} \), \( P_n \subseteq Q_n \) and the system \( P_n \) with \( \Gamma \) instead of \( \Gamma_n \) has exactly one solution in positive integers \( x_1, \ldots, x_n \), namely \( (1, 2^{20}, 2^{21}, 2^{22}, \ldots, 2^{2n-2}) \).
For an integer $n \in \{3, \ldots, 16\}$, let $\Sigma_n$ denote the following statement: if a system of equations $S \subseteq Q_n$ with $\Gamma$ instead of $\Gamma_n$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then every tuple $(x_1, \ldots, x_n) \in (\mathbb{N} \setminus \{0\})^n$ that solves the original system $S$ satisfies $x_1, \ldots, x_n \leq 2^{2^{n-2}}$.

**Hypothesis 3.** The statements $\Sigma_3, \ldots, \Sigma_{16}$ are true.

**Lemma 15.** (cf. Lemma 3) For every integer $n \in \{4, \ldots, 16\}$ and for every positive integers $x$ and $y$, $x \cdot \Gamma_n(x) = \Gamma_n(y)$ if and only if $(x+1 = y) \land \left( x \geq 2^{2^{n-3}} + 1 \right)$.

Let $Z_9 \subseteq Q_9$ be the system of equations in Figure 6.

![Image of system $Z_9$](image)

**Fig. 6** Construction of the system $Z_9$

**Lemma 16.** For every positive integer $x_1$, the system $Z_9$ is solvable in positive integers $x_2, \ldots, x_9$ if and only if $x_1 > 2^{2^{9-4}}$ and $x_1^2 + 1$ is prime. In this case, positive integers $x_2, \ldots, x_9$ are uniquely determined by $x_1$. For every positive integer $n$, at most finitely many tuples $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ begin with $n$ and solve the system $Z_9$ with $\Gamma$ instead of $\Gamma_9$.

**Proof.** It follows from Lemmas 3, 5, and 15. □

**Lemma 17.** (13!)² + 1 = 38775788043632640001 is prime.

**Lemma 18.** $(13!)^2 \geq 2^{2^{2^{9-3}}} + 1 = 18446744073709551617 \land \left( \Gamma_9((13!)^2) > 2^{2^{2^{9-2}}} \right)$.

**Theorem 11.** (cf. Theorem 7) The statement $\Sigma_9$ implies the infinitude of primes of the form $n^2 + 1$.

**Proof.** It follows from Lemmas 16–18. □

**Theorem 12.** (cf. Theorem 8) The statement $\Sigma_9$ implies that any prime of the form $n! + 1$ with $n \geq 2^{2^{9-3}}$ proves the infinitude of primes of the form $n! + 1$.

**Proof.** We leave the proof to the reader. □

**Corollary 7.** Let $Y_9$ denote the set of primes of the form $n! + 1$. The statement $\Sigma_9$ implies that we know an algorithm such that it returns a threshold number of $Y_9$, and this number equals $\max(Y_9)$. Assuming the statement $\Sigma_9$, a single query to an oracle for the halting problem decides the infinity of $Y_9$. Assuming the statement $\Sigma_9$, the infinity of $Y_9$ is decidable in the limit.
Proof. We consider an algorithm which computes \( \max(Y_9 \cap [1, (2^{29} - 1)! + 1]) \).

Let \( Z_{14} \subseteq Q_{14} \) be the system of equations in Figure 7.

![Fig. 7 Construction of the system \( Z_{14} \)](image)

**Lemma 19.** For every positive integer \( x_1 \), the system \( Z_{14} \) is solvable in positive integers \( x_2, \ldots, x_{14} \) if and only if \( x_1 \) and \( x_1 + 2 \) are prime and \( x_1 \geq 2^{14 - 3} + 1 \). In this case, positive integers \( x_2, \ldots, x_{14} \) are uniquely determined by \( x_1 \). For every positive integer \( n \), at most finitely many tuples \( (x_1, \ldots, x_{14}) \in (\mathbb{N} \setminus \{0\})^{14} \) begin with \( n \) and solve the system \( Z_{14} \) with \( \Gamma \) instead of \( \Gamma_{14} \).

**Proof.** It follows from Lemmas 3, 5, and 15.

**Lemma 20.** ([27], p. 87) The numbers \( 459 \cdot 2^{8529} - 1 \) and \( 459 \cdot 2^{8529} + 1 \) are prime (Harvey Dubner).

**Lemma 21.** \( 459 \cdot 2^{8529} - 1 > 2^{2^{14 - 2}} = 2^{4096} \).

**Theorem 13.** (cf. Theorem 9) The statement \( \Sigma_{14} \) implies the infinitude of twin primes.

**Proof.** It follows from Lemmas 19, 21.
**Fig. 8** Construction of the system $Z_{16}$

**Lemma 22.** For every positive integer $x_1$, the system $Z_{16}$ is solvable in positive integers $x_2, \ldots, x_{16}$ if and only if $x_1$ is a Sophie Germain prime and $x_1 \geq 2^{16-3} + 1$. In this case, positive integers $x_2, \ldots, x_{16}$ are uniquely determined by $x_1$. For every positive integer $n$, at most finitely many tuples $(x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ begin with $n$ and solve the system $Z_{16}$ with $\Gamma$ instead of $\Gamma_{16}$.

**Proof.** It follows from Lemmas 3, 5, and 15. $\square$

**Lemma 23.** $(\{20, p. 330\})$ 8069496435 · 10^{5072} − 1 is a Sophie Germain prime (Harvey Dubner).

**Lemma 24.** 8069496435 · 10^{5072} − 1 > 2^{16−2}.

**Theorem 14.** The statement $\Sigma_{16}$ implies the infinitude of Sophie Germain primes.

**Proof.** It follows from Lemmas 22, 24. $\square$

**Theorem 15.** The statement $\Sigma_6$ proves the following implication: if the equation $x(x + 1) = y!$ has only finitely many solutions in positive integers $x$ and $y$, then each such solution $(x, y)$ belongs to the set $\{(1, 2), (2, 3)\}$.

**Proof.** We leave the proof to the reader. $\square$

The question of solving the equation $x(x + 1) = y!$ was posed by P. Erdős, see [2]. F. Luca proved that the abc conjecture implies that the equation $x(x + 1) = y!$ has only finitely many solutions in positive integers, see [14].

**Theorem 16.** The statement $\Sigma_6$ proves the following implication: if the equation $x! + 1 = y^2$ has only finitely many solutions in positive integers $x$ and $y$, then each such solution $(x, y)$ belongs to the set $\{(4, 5), (5, 11), (7, 71)\}$.

**Proof.** We leave the proof to the reader. $\square$
12 Hypothetical statements $\Omega_3, \ldots, \Omega_{16}$ and their consequences

For an integer $n \in \{3, \ldots, 16\}$, let $\Omega_n$ denote the following statement: if a system of equations $S \subseteq \{ \Gamma(x_j) = x_k : i, k \in \{1, \ldots, n\} \} \cup \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \}$ has a solution in integers $x_1, \ldots, x_n$ greater than $2^{2n-2}$, then $S$ has infinitely many solutions in positive integers $x_1, \ldots, x_n$. For every $n \in \{3, \ldots, 16\}$, the statement $\Sigma_n$ implies the statement $\Omega_n$.

**Lemma 25.** The number $(65!)^2 + 1$ is prime and $65! > 2^{29-2}$.

**Proof.** The following PARI/GP ([19]) command

```
\text{(04:04) gp > isprime((65!)^2+1,\{flag=2\})}
\%1 = 1
```

is shown together with its output. This command performs the APRCL primality test, the best deterministic primality test algorithm ([27, p. 226]). It rigorously shows that the number $(65!)^2 + 1$ is prime. □

**Lemma 26.** If positive integers $x_1, \ldots, x_9$ solve the system $Z_9$ and $x_1 > 2^{29-2}$, then $x_1 = \min(x_1, \ldots, x_9)$.

**Theorem 17.** The statement $\Omega_9$ implies the infinitude of primes of the form $n^2 + 1$.

**Proof.** It follows from Lemmas [16 and 25–26] □

**Lemma 27.** If positive integers $x_1, \ldots, x_{14}$ solve the system $Z_{14}$ and $x_1 > 2^{214-2}$, then $x_1 = \min(x_1, \ldots, x_{14})$.

**Theorem 18.** The statement $\Omega_{14}$ implies the infinitude of twin primes.

**Proof.** It follows from Lemmas [19, 21 and 27] □

13 Are there infinitely many composite Fermat numbers?

Integers of the form $2^{2^n} + 1$ are called 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 [13, 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 [13, p. 1].

**Open Problem 3.** ([13, 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 $n \geq 5$, see [12, p. 23]. Let

$$H_n = \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \cup \{ 2^{2^i} = x_k : i, k \in \{1, \ldots, n\} \}$$

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

**Lemma 28.** The following subsystem of $H_n$

$$\left\{ \begin{array}{l}
    x_1 \cdot x_1 = x_1 \\
    \forall i \in \{1, \ldots, n-1\} \quad 2^{2^{x_i}} = x_{i+1}
\end{array} \right.$$  

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

14
For a positive integer \( n \), let \( \xi_n \) denote the following statement: if a system of equations \( S \subseteq H_n \) has only finitely many solutions in positive integers \( x_1, \ldots, x_n \), then each such solution \( (x_1, \ldots, x_n) \) satisfies \( x_1, \ldots, x_n \leq h(n) \). The statement \( \xi_n \) says that for subsystems of \( H_n \) the largest known solution is indeed the largest possible.

**Hypothesis 4.** The statements \( \xi_1, \ldots, \xi_{13} \) are true.

**Lemma 29.** Every statement \( \xi_n \) is true with an unknown integer bound that depends on \( n \).

**Proof.** For every positive integer \( n \), the system \( H_n \) has a finite number of subsystems. \( \square \)

**Theorem 19.** The statement \( \xi_{13} \) proves the following implication: if \( z \in \mathbb{N} \setminus \{0\} \) and \( 2^{2z} + 1 \) is composite and greater than \( h(12) \), then \( 2^{2z} + 1 \) is composite for infinitely many positive integers \( z \).

**Proof.** Let us consider the equation

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

in positive integers. By Lemma 4, we can transform the equation (E) into an equivalent system of equations \( G \) 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 9.

\[\text{Fig. 9} \quad \text{Construction of the system } G\]

Since \( 2^{2z} + 1 > h(12) \), we obtain that \( 2^{22^z} + 1 > h(13) \). By this, the statement \( \xi_{13} \) implies that the system \( G \) has infinitely many solutions in positive integers. It means that there are infinitely many composite Fermat numbers. \( \square \)

**Corollary 8.** Let \( W_{13} \) denote the set of composite Fermat numbers. The statement \( \xi_{13} \) implies that we know an algorithm such that it returns a threshold number of \( W_{13} \), and this number equals \( \max(W_{13}) \), if \( W_{13} \) is finite. Assuming the statement \( \xi_{13} \), a single query to an oracle for the halting problem decides the infinity of \( W_{13} \). Assuming the statement \( \xi_{13} \), the infinity of \( W_{13} \) is decidable in the limit.

**Proof.** We consider an algorithm which computes \( \max(W_{13} \cap [1, h(12)]) \). \( \square \)
References


16


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