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

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

Abstract

Let $\mathcal{P}$ denote the set of prime numbers, and let $\mathcal{M}$ denote the set of multiples of twin primes greater than $99999$. The set $\mathcal{X} = \left([2, 99999]\cap\mathcal{P}\right)\cup\mathcal{M}$ satisfies the following conditions: (1) a known and simple algorithm for every $n \in \mathbb{N}$ decides whether or not $n \in \mathcal{X}$, (2) a known and simple algorithm returns an integer $n$ such that $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ contains an element greater than $n$, (3) new elements of $\mathcal{X}$ are still discovered, (4) it is conjectured that $\mathcal{X}$ is infinite although we do not know any algorithm deciding the infiniteness of $\mathcal{X}$. The following problem is open: define a set $\mathcal{X} \subseteq \mathbb{N}$ such that $\mathcal{X}$ satisfies conditions (1)-(4) and

\[\text{the formula } n \in \mathcal{X} \text{ has the same intuitive meaning for every } n \in \mathbb{N}\] (5)

The problem remains open if condition (2) states that a known and simple algorithm returns an integer $n$ such that $\mathcal{X}$ is infinite if and only if $\text{card}(\mathcal{X}) > n$. 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 guess is that the statements $\Psi_3, \ldots, \Psi_{16}$ are true. The statement $\Psi_9$ implies that the set of primes of the form $n^2 + 1$ and the set of primes of the form $n! + 1$ satisfy conditions (1)-(5). The statement $\Psi_{16}$ implies that the set of twin primes satisfies conditions (1)-(5).

Key words and phrases: finiteness of a set, incompleteness of ZFC, infiniteness of a set, prime numbers of the form $n^2 + 1$, prime numbers of the form $n! + 1$, twin primes.

2010 Mathematics Subject Classification: 03D20, 11A41.

1 Introduction and basic lemmas

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

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

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 mathematical conjectures can be settled indirectly by proving stronger \( \Pi \) is a integer \( n \) (Wilson's theorem, [8, p. 89]). For every positive integer \( x \), \( x \) divides \( n \).

Lemma 4. (Wilson’s theorem, [8, p. 89]). For every positive integer \( x \), \( x \) divides \( (x - 1)! + 1 \) if and only if \( x = 1 \) or \( x \) is prime.

2 Subsets of \( \mathbb{N} \) and their threshold numbers

Definition 1. We say that an integer \( m \in \mathbb{N} \) 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. [22] and [23].

If a set \( X \subseteq \mathbb{N} \) is empty or finite, then any \( m \in \mathbb{N} \) is a threshold number of \( X \). If a set \( X \subseteq \mathbb{N} \) is non-empty and finite, then the all threshold numbers of \( X \) form the set \( \{ \max(X), \max(X) + 1, \max(X) + 2, \ldots \} \).

Definition 2. We say that a non-negative integer \( m \) is a weak threshold number of a set \( X \subseteq \mathbb{N} \), if \( X \) is infinite if and only if \( \text{card}(X) > m \).

Proposition 1. For every \( X \subseteq \mathbb{N} \), if an integer \( m \in \mathbb{N} \) is a threshold number of \( X \), then \( m + 1 \) is a weak threshold number of \( X \).

Proof. For every \( X \subseteq \mathbb{N} \), if \( m \in \mathbb{N} \) and \( \text{card}(X) > m + 1 \), then \( X \cap [m + 1, \infty) \neq \emptyset \). □

It is conjectured that the set of prime numbers of the form \( n^2 + 1 \) is infinite, see [15] pp. 37–38. It is conjectured that the set of prime numbers of the form \( n! + 1 \) is infinite, see [2] 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 [13] p. 39. It is conjectured that the set of composite numbers of the form \( 2^{2^n} + 1 \) is infinite, see [11] p. 23 and [12] pp. 158–159. A prime \( p \) is said to be a Sophie Germain prime if both \( p \) and \( 2p + 1 \) are prime, see [21]. It is conjectured that the set of Sophie Germain primes is infinite, see [17] p. 330. For each of these sets, we do not know any weak threshold number.

Open Problem 1. Define a set \( X \subseteq \mathbb{N} \) that satisfies the following conditions:
(a1) a known and simple algorithm for every \( n \in \mathbb{N} \) decides whether or not \( n \in X \),
(b1) a known and simple algorithm returns an integer \( n \) such that \( X \) is infinite if and only if \( \text{card}(X) > n \),
(c1) new elements of \( X \) are still discovered,
(d1) it is conjectured that \( X \) is infinite although we do not know any algorithm deciding the infiniteness of \( X \),
(e1) the formula \( n \in X \) has the same intuitive meaning for every \( n \in \mathbb{N} \).

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 \( \Pi \) statement which strengthens the twin prime conjecture, see [3] p. 43. C. H. Bennett claims that most mathematical conjectures can be settled indirectly by proving stronger \( \Pi \) statements, see [1]. The
The height of a rational number \( \frac{p}{q} \) is denoted by \( H \left( \frac{p}{q} \right) \) 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 2.** The equation \( x^5 - x = y^2 - y \) has only finitely many rational solutions, see [14] p. 212. The known rational solutions are \((x, y) = (-1, 0), (1, 0), (0, 0), (0, 1), (1, 1), (2, -5), (2, 6), (3, -15), (3, 16), (30, -4929), (30, 4930), \left( \frac{1}{2}, \frac{15}{16} \right), \left( \frac{1}{2}, \frac{17}{16} \right), \left( -\frac{15}{16}, -\frac{185}{1624} \right), \left( -\frac{15}{16}, \frac{1209}{1624} \right), \) and the existence of other solutions is an open question, see [18] pp. 223–224.

**Proposition 3.** The set \( \mathcal{T} = \{ n \in \mathbb{N} : \text{the equation } x^5 - x = y^2 - y \text{ has a rational solution of height } n \} \) is finite. We know an algorithm which for every \( n \in \mathbb{N} \) decides whether or not \( n \in \mathcal{T} \). We do not know any algorithm which returns a threshold number of \( \mathcal{T} \).

**Open Problem 2.** Define a set \( \mathcal{X} \subseteq \mathbb{N} \) that satisfies the following conditions:
\( (a2) \) a known and simple algorithm for every \( n \in \mathbb{N} \) decides whether or not \( n \in \mathcal{X} \),
\( (b2) \) a known and simple algorithm returns an integer \( n \) such that \( \mathcal{X} \) is infinite if and only if \( \mathcal{X} \) contains an element greater than \( n \),
\( (c2) \) new elements of \( \mathcal{X} \) are still discovered,
\( (d2) \) it is conjectured that \( \mathcal{X} \) is infinite although we do not know any algorithm deciding the infiniteness of \( \mathcal{X} \),
\( (e2) \) the formula \( n \in \mathcal{X} \) has the same intuitive meaning for every \( n \in \mathbb{N} \).

Let \( \mathcal{P} \) denote the set of prime numbers, and let \( \mathcal{M} \) denote the set of multiples of twin primes greater than \( 999999 \).

**Proposition 4.** The set \( \left( \mathcal{P} \setminus 2,999999 \right) \cap \mathcal{M} \) satisfies conditions (a2)–(d2).

Let
\[
\mathcal{H} = \begin{cases} 
\mathbb{N}, \text{ if } \sin \left( \frac{999999}{2} \right) < 0 \\
\mathbb{N} \cap \left[ 0, \sin \left( \frac{999999}{2} \right) \cdot 999999 \right), \text{ otherwise}
\end{cases}
\]

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

**Proposition 5.** The number \( 999999 \) 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
\[
\mathcal{K} = \begin{cases} 
\{ n \}, \text{ if } (n \in \mathbb{N}) \land \left( 2^{n_0} = \mathcal{S}_{n+1} \right) \\
\{ 0 \}, \text{ if } 2^{n_0} \geq \mathcal{S}_{\omega}
\end{cases}
\]

**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 \( 2^{n_0} \) can attain every value from the set \( \{ \mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3, \ldots \} \), see [7] and [10] p. 232. \( \square \)
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.** ([5] 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.** ([4], [9] p. 53). The polynomial $D(x_1, \ldots, x_m)$ is very complicated.

Let $Y$ 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 $n \in Y$. Theorem 2 implies the next theorem.

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

Let $E$ 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 $n \in E$. Theorem 2 implies the next theorem.

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

Let $V$ denote the set

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

Since the sets $\{0, \ldots, k\}^m$ and $\{0, \ldots, k+1\}^m$ are finite, there exists an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in V$. According to Remark 1 at present we do not know a simple computer program that realizes such an algorithm. Theorem 2 implies the next theorem.

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

**Open Problem 3.** Define a simple algorithm $A$ such that $A$ returns 0 or 1 on every input $k \in \mathbb{N}$ and the set

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

satisfies conditions (6)–(10).
4 Hypothetical statements $\Psi_3, \ldots, \Psi_{16}$

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

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

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

![Diagram](image)

**Fig. 1** Construction of the system $U_n$

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

**Lemma 5.** 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.

**Lemma 6.** 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. □

**Lemma 7.** For every statement $\Psi_n$, the bound $g(n)$ cannot be decreased.

**Proof.** It follows from Lemma 5 because $U_n \subseteq B_n$. □

**Remark 2.** By Lemma 2 and algebraic lemmas in [19, 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 unbelievable because a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [13, p. 300]. Therefore, the statement $\forall n \in \mathbb{N} \setminus \{0, 1, 2\} \Psi_n$ seems to be false.
5 The Brocard-Ramanujan equation $x! + 1 = y^2$

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

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

**Lemma 8.** 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:

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

**Proof.** It follows from Lemma 2. □

It is conjectured that $x! + 1$ is a perfect square only for $x \in \{4, 5, 7\}$, see [20, 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 [16].

**Theorem 6.** If the equation $x_1! + 1 = x_4^2$ 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 $x_1, x_4$ satisfy $x_1! + 1 = x_4^2$. Then, $x_1, x_4 \in \mathbb{N} \setminus \{0, 1\}$. By Lemma 8, 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 $x_1 \in \{4, 5, 7\}$. □

6 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 [15] 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 2 and the diagram in Figure 3 explain the construction of the system $\mathcal{B}$.
Lemma 9. For every integer $x_1 \geq 2$, the system $B$ 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:

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

Proof. By Lemma 4 for every integer $x_1 \geq 2$, the system $B$ 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 9 follows from Lemma 4. \qed

Lemma 10. There are only finitely many tuples $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ which solve the system $B$ and satisfy $x_1 = 1$.

Proof. If a tuple $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ solves the system $B$ 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, $x_9 = x_8! \leq 2$. \qed

Theorem 7. 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 9 there exists a unique tuple $(x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ such that the tuple $(x_1, x_2, \ldots, x_9)$ solves the system $B$. Since $x_1^2 + 1 > g(7)$, we obtain that $x_1^2 \geq g(7)$. 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 $B \subseteq B_9$, the statement $\Psi_9$ and the inequality $x_9 > g(9)$ imply that the system $B$ has infinitely many solutions $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$. According to Lemmas 9 and 10 there are infinitely many primes of the form $n^2 + 1$. \qed

Corollary 2. 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 infiniteness of $X_9$. Assuming the statement $\Psi_9$, the infiniteness of $X_9$ is decidable in the limit.

Proof. We consider an algorithm which computes $\max(X_9 \cap [1, g(7)])$. \qed
7 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 [2, p. 443].

**Theorem 8.** The statement \( \Psi_9 \) proves the following implication: if there exists an integer \( x_1 \geq g(6) \) such that \( x_1! + 1 \) is prime, then there are infinitely many primes of the form \( n! + 1 \).

**Proof.** We leave the analogous proof to the reader. \( \square \)

8 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 [15, p. 39]. Let \( C \) denote the following system of equations:

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

Theorem 8. The statement \( \Psi_9 \) proves the following implication: if there exists an integer \( x_1 \geq g(6) \) such that \( x_1! + 1 \) is prime, then there are infinitely many primes of the form \( n! + 1 \).

**Proof.** We leave the analogous proof to the reader. \( \square \)

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

| \( x_1! \) | \( x_2 \) | \( x_3! \) | \( x_4 \) | \( x_5 \) | \( x_6! \) | \( x_7 \) | \( x_8 \) | \( x_9! \) | \( x_{10} \) | \( x_{11} \) | \( x_{12}! \) | \( x_{13} \) | \( x_{14} \) | \( x_{15}! \) | \( x_{16} \) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| \( x_2 \cdot x_4 = x_5 \) | \( x_4 \cdot x_{11} = x_{12} \) | \( x_5 \cdot x_6 = x_7 \) | \( x_7 \cdot x_{14} = x_{15} \) | \( x_8 \cdot x_{15} = x_{16} \) |
Lemma 12. There are only finitely many tuples \((x_1, \ldots, x_{16})\) such that the tuple \((x_1, \ldots, x_{16})\) solves the system \(C\). Hence, the claim of Lemma 11 follows from Lemma 4.

Proof. By Lemma 3 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
\[
\left( x_4 + 2 = x_9 \right) \land \left( x_4 ((x_4 - 1)! + 1) \land (x_9 ((x_9 - 1)! + 1) \right)
\]
Hence, the claim of Lemma 11 follows from Lemma 4. \(\square\)

**Lemma 12.** There are only finitely many tuples \((x_1, \ldots, x_{16})\) such that the tuple \((x_1, \ldots, x_{16})\) solves the system \(C\) and satisfy \((x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})\).

Proof. If a tuple \((x_1, \ldots, x_{16})\) solves the system \(C\) and \((x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})\), then \(x_1, \ldots, x_{16} \leq 7\!). Indeed, for example, if \(x_4 = 2\) then \(x_6 = x_4 + 1 = 3\). Hence, \(x_7 = x_6! = 6\). Therefore, \(x_{15} = x_7 + 1 = 7\). Consequently, \(x_{16} = x_{15}! = 7\!)!.

**Theorem 9.** 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 \(x_9 = x_4 + 2 \geq g(14)\). Hence, \(x_4, x_9 \in \mathbb{N} \setminus \{0, 1, 2\}\). By Lemma 11 there exists a unique tuple
\[
(x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0\})^{14}
\]
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 11 and 12 there are infinitely many twin primes. \(\square\)

**Corollary 3.** (cf. [12]). 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 infiniteness of \(X_{16}\). Assuming the statement \(\Psi_{16}\), the infiniteness of \(X_{16}\) is decidable in the limit.

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

9  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 [12] 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 [12] p. 1.

**Open Problem 4.** ([12] p. 159). Are there infinitely many composite numbers of the form \(2^{2^n} + 1\)?
Most mathematicians believe that $2^{2n} + 1$ is composite for every integer $n \geq 5$, see [11, p. 23]. Let

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

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

**Lemma 13.** The following subsystem of $H_n$

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

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

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 2.** The statements $\xi_1, \ldots, \xi_{13}$ are true.

**Lemma 14.** 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. \qed

**Theorem 10.** The statement $\xi_{13}$ proves the following implication: if $z \in \mathbb{N} \setminus \{0\}$ and $2^{2^z} + 1$ is composite and greater than $h(12)$, then $2^{2^z} + 1$ is composite for infinitely many positive integers $z$.

**Proof.** Let us consider the equation

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

in positive integers. By Lemma 3 we can transform the equation (E) into an equivalent system of equations $G$ 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 5.
Since $2^{2z} + 1 > h(12)$, we obtain that $2^{2^{2z} + 1} > h(13)$. 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. □

**Corollary 4.** 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 infiniteness of $W_{13}$. Assuming the statement $\xi_{13}$, the infiniteness of $W_{13}$ is decidable in the limit.

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

**References**


