On ZFC-formulae $\varphi(x)$ for which we know a non-negative integer n such that $\{x \in \mathbb{N}\colon \varphi(x)\} \subseteq \{x \in \mathbb{N}\colon x \leqslant n-1\}$ if the set $\{x \in \mathbb{N}\colon \varphi(x)\}$ 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 $g(3)=4$, and let $g(n+1)=g(n)!$ for every integer $n \geqslant 3$. For an integer $n \in \{3,\ldots,16\}$, let Ψ_n denote the following hypothetical statement: *if a system of equations* $\mathcal{S} \subseteq \Big\{x_i!=x_k:(i,k \in \{1,\ldots,n\}) \wedge (i \neq k)\Big\} \cup \Big\{x_i \cdot x_j = x_k: i,j,k \in \{1,\ldots,n\}\Big\}$ *has only finitely many solutions in positive integers* $x_1,\ldots,x_n$*, then each such solution* $(x_1,\ldots,x_n)$ *satisfies* $x_1,\ldots,x_n \leqslant g(n)$. We say that a non-negative integer m is a threshold number of a set $\mathcal{X} \subseteq \mathbb{N}$, if $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ contains an element greater than m. The following problem is open: *define a set* $\mathcal{X} \subseteq \mathbb{N}$ *that satisfies the following conditions:* `(1)` *a known algorithm for every* $n \in \mathbb{N}$ *decides whether or not* $n \in \mathcal{X}$*,* `(2)` *a known algorithm returns a threshold number of* $\mathcal{X}$*,* `(3)` *new elements of* $\mathcal{X}$ *are still discovered,* `(4)` *we do not know any algorithm deciding the inequality* $\mathrm{card}(\mathcal{X})<\infty$. The statement Ψ_9 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 Ψ_{16} implies that the set of twin primes solves the problem.

2010 Mathematics Subject Classification: 03D20, 11A41

Key words and phrases: arithmetical consistency of ZFC, composite Fermat numbers, finiteness of a set, incompleteness of ZFC, infiniteness of a set, oracle for the halting problem, prime numbers of the form n^2+1, prime numbers of the form $n!+1$, twin primes, Sophie Germain primes

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

$$\mathrm{card}(\{x \in \mathbb{N}\colon \varphi(x)\}) < \infty \Longrightarrow \{x \in \mathbb{N}\colon \varphi(x)\} \subseteq \{x \in \mathbb{N}\colon x \leqslant n-1\}$$

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, $\mathrm{card}(\{x \in \mathbb{N}\colon x \leqslant n-1\}) = n$.

Corollary 1 *The title altered to* "On ZFC-formulae $\varphi(x)$ for which we know a non-negative integer n such that $\mathrm{card}(\{x \in \mathbb{N}\colon \varphi(x)\}) \leqslant n$ if the set $\{x \in \mathbb{N}\colon \varphi(x)\}$ 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 $\mathcal{X} \subseteq \mathbb{N}$, if $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ contains an element greater than m, cf. [25] and [26]. If a set $\mathcal{X} \subseteq \mathbb{N}$ is empty or infinite, then any non-negative integer m is a threshold number of $\mathcal{X}$. If a set $\mathcal{X} \subseteq \mathbb{N}$ is non-empty and finite, then the all threshold numbers of $\mathcal{X}$ form the set $\{\max(\mathcal{X}), \max(\mathcal{X})+1, \max(\mathcal{X})+2, \ldots\}$.

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 [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 [15, 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 [23]. It is conjectured that the set of Sophie Germain primes is infinite, see [18, p. 330]. For each of these sets, we do not know any threshold number.

Open Problem 1 *Define a set* $\mathcal{X} \subseteq \mathbb{N}$ *that satisfies the following conditions:*
(1) *a known algorithm for every* $n \in \mathbb{N}$ *decides whether or not* $n \in \mathcal{X}$,

(2) *a known algorithm returns a threshold number of* $\mathcal{X}$*,*
(3) *new elements of* $\mathcal{X}$ *are still discovered,*
(4) *we do not know any algorithm deciding the inequality* $\mathrm{card}(\mathcal{X}) < \infty$*.*

The following statement: *for every non-negative integer* n *there exist*

$$\textit{prime numbers } p \textit{ and } q \textit{ such that } p+2=q \textit{ and } p \in \left[10^{n}, 10^{n+1}\right] \quad \texttt{(T)}$$

is a Π_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 Π_1 statements, see [1]. The statement (T) is equivalent to the non-halting of a Turing machine. If a set $\mathcal{X} \subseteq \mathbb{N}$ is computable and we know a threshold number of $\mathcal{X}$, then the infinity of $\mathcal{X}$ is equivalent to the halting of a Turing machine.

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 $\max(H(x_1),\ldots,H(x_n))$.

Observation 1 *The equation* $x^5-x=y^2-y$ *has only finitely many rational solutions, see [14, p. 212]. The known rational solutions are* $(x,y)=(-1,0)$, $(-1,1)$, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, $(2,-5)$, $(2,6)$, $(3,-15)$, $(3,16)$, $(30,-4929)$, $(30,4930)$, $\left(\frac{1}{4},\frac{15}{32}\right)$, $\left(\frac{1}{4},\frac{17}{32}\right)$, $\left(-\frac{15}{16},-\frac{185}{1024}\right)$, $\left(-\frac{15}{16},\frac{1209}{1024}\right)$*, and the existence of other solutions is an open question, see [19, pp. 223–224].*

Corollary 2 *The set* $\mathcal{T}=\{n\in\mathbb{N}:$ *the equation* $x^5-x=y^2-y$ *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* $\mathcal{T}$*.*

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

$$\begin{cases} x^2+y^2 &= s^2\\ x^2+z^2 &= t^2\\ y^2+z^2 &= u^2\\ x^2+y^2+z^2 &= v^2 \end{cases}$$

Let $\mathcal{F}=\Big\{n\in\mathbb{N}\setminus\{0\}:\Big(\text{the system } \mathcal{L} \text{ has no solutions in } \{1,\ldots,n\}^7\Big)\wedge\Big(\text{the system } \mathcal{L} \text{ has a solution in } \{1,\ldots,n+1\}^7\Big)\Big\}$. A perfect cuboid is a cuboid having integer side lengths, integer face diagonals, and an integer space diagonal.

Observation 2 *([22]) No perfect cuboids are known.*

Corollary 3 *We know an algorithm which for every* $n \in \mathbb{N}$ *decides whether or not* $n \in \mathcal{F}$*. ZFC proves that* $\mathrm{card}(\mathcal{F}) \in \{0,1\}$*. We do not know any algorithm which returns* $\mathrm{card}(\mathcal{F})$*. We do not know any algorithm which returns a threshold number of* $\mathcal{F}$*.*

Let

$$\mathcal{H} = \begin{cases} \mathbb{N}, \text{ if } \sin\left(9^{9^{9^{9^{9}}}}\right) < 0 \\ \mathbb{N} \cap \left[0, \ \sin\left(9^{9^{9^{9^{9}}}}\right) \cdot 9^{9^{9^{9^{9}}}}\right) \text{ otherwise} \end{cases}$$

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

Observation 3 *The number* $9^{9^{9^{9^{9}}}}$ *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

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

Theorem 1 *ZFC proves that* $\mathrm{card}(\mathcal{K}) = 1$*. 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 [7] and [10, 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 *([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*.*

Observation 4 *([9, p. 53]) The polynomial* $D(x_1, \ldots, x_m)$ *is not effectively known.*

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 2 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 2 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 $\mathcal{V} =$

$$\Big\{n \in \mathbb{N} : \Big(\text{the polynomial } D(x_1, \ldots, x_m) \text{ has no solutions in } \{0, \ldots, n\}^m\Big) \wedge$$

$$\Big(\text{the polynomial } D(x_1, \ldots, x_m) \text{ has a solution in } \{0, \ldots, n+1\}^m\Big)\Big\}.$$

Since the sets $\{0, \ldots, n\}^m$ and $\{0, \ldots, n+1\}^m$ are finite, there exists an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in \mathcal{V}$. According to Observation 4, at present we are not able to write a computer program that realizes such an algorithm. Theorem 2 implies the next theorem.

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

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

satisfies conditions (5)-(9).

4 Basic lemmas and hypothetical statements $\Psi_3, \ldots, \Psi_{16}$

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

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

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*

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

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, [8, p. 89]). For every positive integer* x, x *divides* $(x-1)!+1$ *if and only if* $x=1$ *or* x *is prime.*

For an integer $n \geqslant 3$, let $\mathcal{U}_n$ denote the following system of equations:

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

The diagram in Figure 1 illustrates the construction of the system $\mathcal{U}_n$.

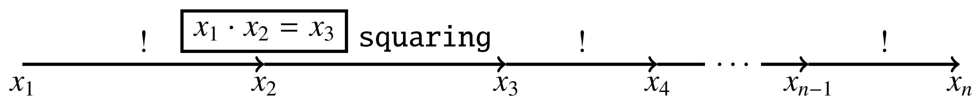

Fig. 1 Construction of the system $\mathcal{U}_n$

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

Lemma 6 *For every integer* $n \geqslant 3$*, the system* $\mathcal{U}_n$ *has exactly two solutions in positive integers, namely* $(1, \dots, 1)$ *and* $\Big(2, 2, g(3), \dots, g(n)\Big)$.

Let

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

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

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

Lemma 7 *Every statement* Ψ_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 8 *For every statement* Ψ_n*, the bound* $g(n)$ *cannot be decreased.*

Proof. It follows from Lemma 6 because $\mathcal{U}_n \subseteq B_n$. ■

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 $\mathcal{A}$.

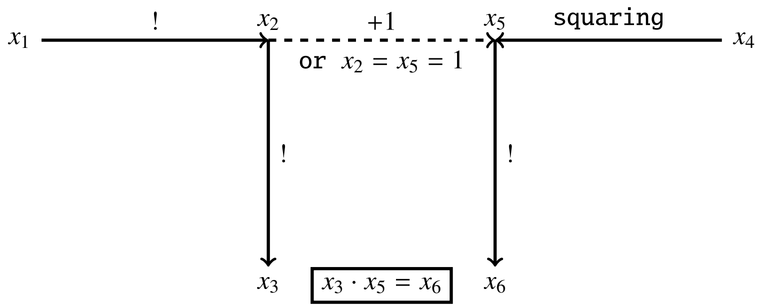

Fig. 2 Construction of the system $\mathcal{A}$

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. ■

It is conjectured that $x! + 1$ is a perfect square only for $x \in \{4, 5, 7\}$, see [21, 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* Ψ_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 Ψ_6 implies that $x_6 = (x_1! + 1)! \leqslant g(6) = g(5)!$. Hence, $x_1! + 1 \leqslant g(5) = g(4)!$. Consequently, $x_1 < g(4) = 24$. If $x_1 \in \{1, \dots, 23\}$, 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 $n^2 + 1$? Are there infinitely many prime numbers of the form $n! + 1$?

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:

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

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

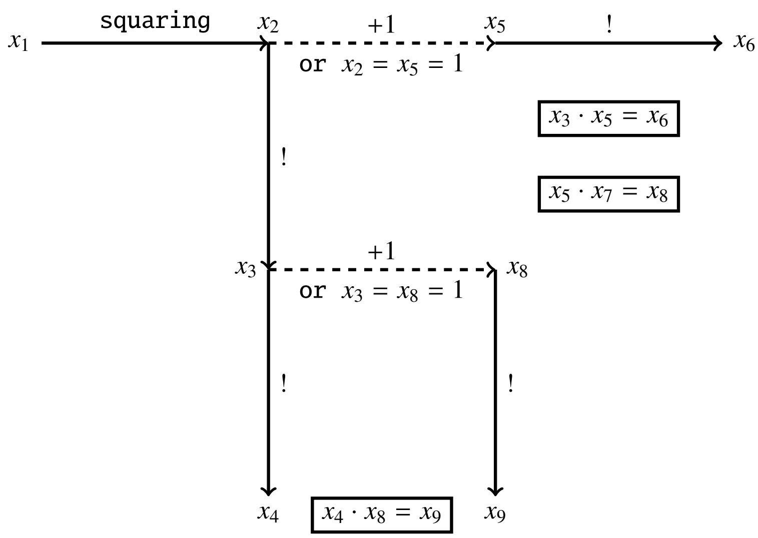

Fig. 3 Construction of the system $\mathcal{B}$

Lemma 10 *For every integer* $x_1 \geqslant 2$*, 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:*

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

Proof. By Lemma 2, for every integer $x_1 \geqslant 2$, 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. ■

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 $x_1, \ldots, x_9 \leqslant 2$. 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, $x_9 = x_8! \leqslant 2$. ■

Theorem 7 *The statement Ψ_9 proves the following implication: if there exists an integer $x_1 \geqslant 2$ 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 $x_1^2 \geqslant g(7)$. Hence, $(x_1^2)! \geqslant g(7)! = g(8)$. Consequently,

$$x_9 = ((x_1^2)! + 1)! \geqslant (g(8) + 1)! > g(8)! = g(9)$$

Since $\mathcal{B} \subseteq B_9$, the statement Ψ_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 $n^2 + 1$. ■

Corollary 4 *Let $\mathcal{X}_9$ denote the set of primes of the form $n^2 + 1$. The statement Ψ_9 implies that we know an algorithm such that it returns a threshold number of $\mathcal{X}_9$, and this number equals $\max(\mathcal{X}_9)$, if $\mathcal{X}_9$ is finite. Assuming the statement Ψ_9, a single query to an oracle for the halting problem decides the infinity of $\mathcal{X}_9$. Assuming the statement Ψ_9, the infinity of $\mathcal{X}_9$ is decidable in the limit.*

Proof. We consider an algorithm which computes $\max(\mathcal{X}_9 \cap [1, g(7)])$. ■

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 Ψ_9 proves the following implication: if there exists an integer $x_1 \geqslant g(6)$ 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. ■

7 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 $\mathcal{C}$ denote the following system of equations:

$$
\left\{
\begin{array}{rcl}
x_1! & = & x_2 \\
x_2! & = & x_3 \\
x_4! & = & x_5 \\
x_6! & = & x_7 \\
x_7! & = & x_8 \\
x_9! & = & x_{10} \\
x_{12}! & = & x_{13} \\
x_{15}! & = & x_{16}
\end{array}
\right.
\qquad\qquad
\begin{array}{rcl}
x_2 \cdot x_4 & = & x_5 \\
x_5 \cdot x_6 & = & x_7 \\
x_7 \cdot x_9 & = & x_{10} \\
x_4 \cdot x_{11} & = & x_{12} \\
x_3 \cdot x_{12} & = & x_{13} \\
x_9 \cdot x_{14} & = & x_{15} \\
x_8 \cdot x_{15} & = & x_{16}
\end{array}
$$

Lemma 2 and the diagram in Figure 4 explain the construction of the system $\mathcal{C}$.

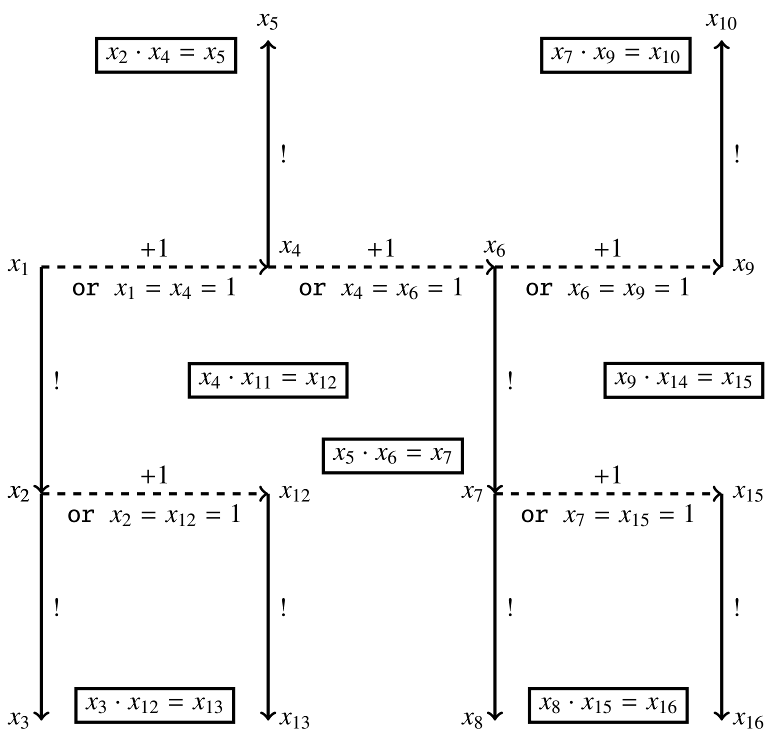

Fig. 4 Construction of the system $\mathcal{C}$

Lemma 12 *For every* $x_4, x_9 \in \mathbb{N} \setminus \{0, 1, 2\}$*, the system* $\mathcal{C}$ *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:*

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

Proof. By Lemma 2, for every $x_4, x_9 \in \mathbb{N} \setminus \{0,1,2\}$, the system $\mathcal{C}$ 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

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

Hence, the claim of Lemma 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* $\mathcal{C}$ *and satisfy* $(x_4 \in \{1,2\}) \vee (x_9 \in \{1,2\})$.

Proof. If a tuple $(x_1,\ldots,x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ solves the system $\mathcal{C}$ and $(x_4 \in \{1,2\}) \vee (x_9 \in \{1,2\})$, then $x_1,\ldots,x_{16} \leqslant 7!$. 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* Ψ_{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 $\mathcal{C}$. Since $x_9 > g(14)$, we obtain that $x_9-1 \geqslant g(14)$. Therefore, $(x_9-1)! \geqslant g(14)! = g(15)$. Hence, $(x_9-1)!+1 > g(15)$. Consequently,

$$x_{16} = ((x_9-1)!+1)! > g(15)! = g(16)$$

Since $\mathcal{C} \subseteq B_{16}$, the statement Ψ_{16} and the inequality $x_{16} > g(16)$ imply that the system $\mathcal{C}$ 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 5 *(cf. [6]). Let $\mathcal{X}_{16}$ denote the set of twin primes. The statement Ψ_{16} implies that we know an algorithm such that it returns a threshold number of $\mathcal{X}_{16}$, and this number equals* $\max(\mathcal{X}_{16})$*, if $\mathcal{X}_{16}$ is finite. Assuming the statement Ψ_{16}, a single query to an oracle for the halting problem decides the infinity of $\mathcal{X}_{16}$. Assuming the statement Ψ_{16}, the infinity of $\mathcal{X}_{16}$ is decidable in the limit.*

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

8 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 $n \geqslant 5$. For an integer $n \geqslant 5$, let $\mathcal{J}_n$ denote the following system of equations:

$$\begin{cases} \forall i \in \{1, \ldots, n-1\} \setminus \{3\} \; \Gamma(x_i) & = & x_{i+1} \\ x_1 \cdot x_1 & = & x_4 \\ x_2 \cdot x_3 & = & x_5 \end{cases}$$

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

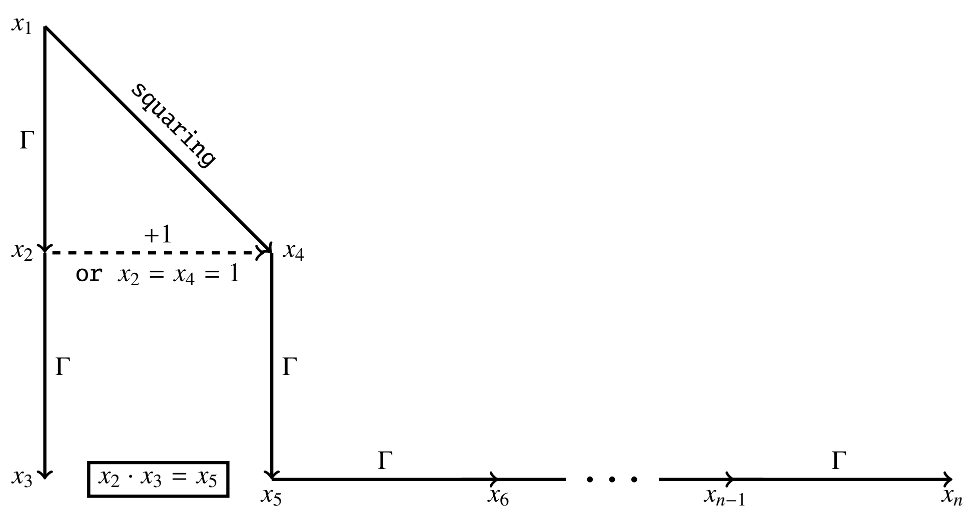

Fig. 5 Construction of the system $\mathcal{J}_n$

For every integer $n \geqslant 5$, 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 $n \geqslant 5$, let Δ_n denote the following statement: *if a system of equations* $\mathcal{S} \subseteq$

$\Big\{\Gamma(x_i) = x_k : i,k \in \{1,\dots,n\}\Big\} \cup \Big\{x_i \cdot x_j = x_k : i,j,k \in \{1,\dots,n\}\Big\}$ *has only finitely many solutions in positive integers* $x_1,\dots,x_n$*, then each such solution* $(x_1,\dots,x_n)$ *satisfies* $x_1,\dots,x_n \leqslant \lambda(n)$.

Hypothesis 2 *The statements* $\Delta_5,\dots,\Delta_{14}$ *are true.*

Lemmas 3 and 5 imply that the statements Δ_n have similar consequences as the statements Ψ_n.

Theorem 10 *The statement* Δ_6 *implies that any prime number* $p \geqslant 25$ *proves the infinitude of primes.*

Proof. It follows from Lemmas 3 and 5. We leave the details to the reader. ■

9 Hypothetical statements $\Sigma_3,\dots,\Sigma_{16}$ and their consequences

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

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

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

$$\begin{cases} \hfill x_1 \cdot x_1 &= x_1 \\ \hfill \Gamma_n(x_2) &= x_1 \\ \forall i \in \{2,\dots,n-1\}\ x_i \cdot x_i &= x_{i+1} \end{cases}$$

Lemma 14 *For every integer* $n \in \{3,\dots,16\}$*,* $P_n \subseteq Q_n$ *and the system* P_n *with* Γ *instead of* Γ_n *has exactly one solution in positive integers* $x_1,\dots,x_n$*, namely* $\Big(1, 2^{2^0},\ 2^{2^1}, 2^{2^2},\dots,2^{2^{n-2}}\Big)$.

For an integer $n \in \{3,\dots,16\}$, let Σ_n denote the following statement: if a system of equations $\mathcal{S} \subseteq Q_n$ with Γ instead of Γ_n has only finitely many solutions in positive integers $x_1,\dots,x_n$, then every tuple $(x_1,\dots,x_n) \in (\mathbb{N} \setminus \{0\})^n$ that solves the original system $\mathcal{S}$ satisfies $x_1,\dots,x_n \leqslant 2^{2^{n-2}}$.

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

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

Let $\mathcal{Z}_9 \subseteq Q_9$ be the system of equations in Figure 6.

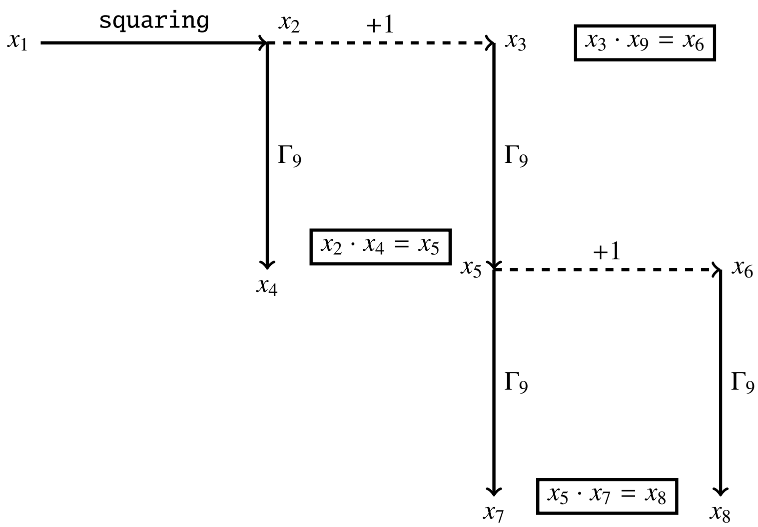

Fig. 6 Construction of the system $\mathcal{Z}_9$

Lemma 16 *For every positive integer* x_1*, the system* $\mathcal{Z}_9$ *is solvable in positive integers* $x_2, \dots, x_9$ *if and only if* $x_1 > 2^{2^{9-4}}$ *and* $x_1^2 + 1$ *is prime. In this case, positive integers* $x_2, \dots, x_9$ *are uniquely determined by* x_1*. For every positive integer* n*, at most finitely many tuples* $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ *begin with* n *and solve the system* $\mathcal{Z}_9$ *with* Γ *instead of* Γ_9*.*

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

Lemma 17 *([20]). The number* $(13!)^2 + 1 = 38775788043632640001$ *is prime.*

Lemma 18 $\Big((13!)^2 \geqslant 2^{2^{9-3}} + 1 = 18446744073709551617\Big) \wedge \big(\Gamma_9((13!)^2) > 2^{2^{9-2}}\big)$.

Theorem 11 *The statement* Σ_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* Σ_9 *implies that any prime of the form* $n! + 1$ *with* $n \geqslant 2^{2^{9-3}}$ *proves the infinitude of primes of the form* $n! + 1$*.*

Proof. We leave the proof to the reader. ■

Corollary 6 *Let $\mathcal{Y}_9$ denote the set of primes of the form $n!+1$. The statement Σ_9 implies that we know an algorithm such that it returns a threshold number of $\mathcal{Y}_9$, and this number equals* $\max(\mathcal{Y}_9)$*, if $\mathcal{Y}_9$ is finite. Assuming the statement Σ_9, a single query to an oracle for the halting problem decides the infinity of $\mathcal{Y}_9$. Assuming the statement Σ_9, the infinity of $\mathcal{Y}_9$ is decidable in the limit.*

Proof. We consider an algorithm which computes
$\max(\mathcal{Y}_9 \cap [1, (2^{2^{9-3}}-1)!+1])$. ■

Let $\mathcal{Z}_{14} \subseteq Q_{14}$ be the system of equations in Figure 7.

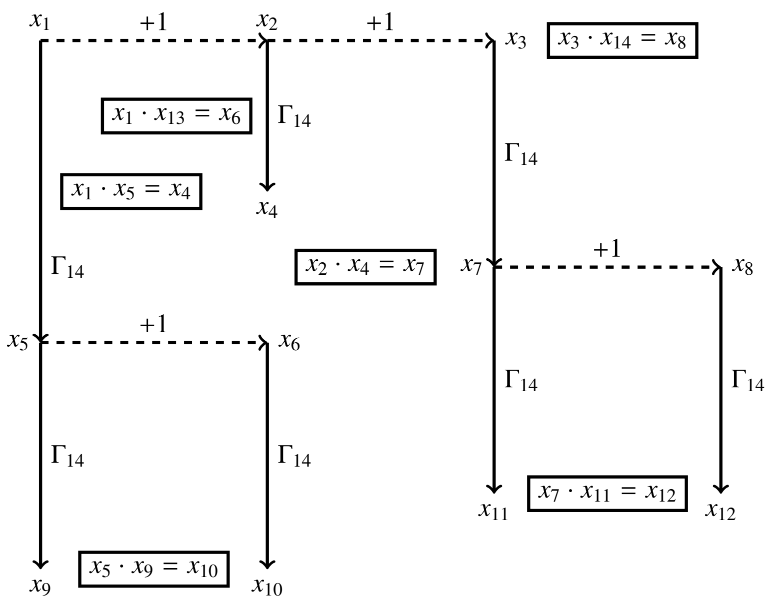

Fig. 7 Construction of the system $\mathcal{Z}_{14}$

Lemma 19 *For every positive integer x_1, the system $\mathcal{Z}_{14}$ is solvable in positive integers $x_2, \ldots, x_{14}$ if and only if x_1 and x_1+2 are prime and $x_1 \geqslant 2^{2^{14-3}}+1$. 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 $\mathcal{Z}_{14}$ with Γ instead of Γ_{14}.*

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

Lemma 20 *([24, 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 *The statement* Σ_{14} *implies the infinitude of twin primes.*

Proof. It follows from Lemmas 19–21. ■

A prime p is said to be a Sophie Germain prime if both p and $2p+1$ are prime, see [23]. It is conjectured that there are infinitely many Sophie Germain primes, see [18, p. 330]. Let $\mathcal{Z}_{16} \subseteq Q_{16}$ be the system of equations in Figure 8.

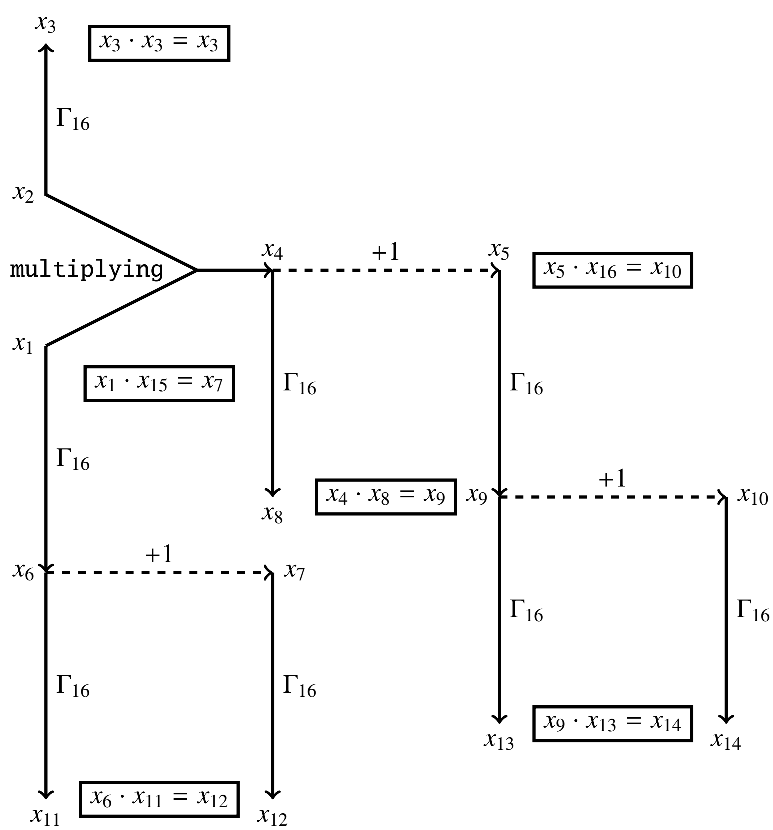

Fig. 8 Construction of the system $\mathcal{Z}_{16}$

Lemma 22 *For every positive integer* x_1*, the system* $\mathcal{Z}_{16}$ *is solvable in positive integers* $x_2, \dots, x_{16}$ *if and only if* x_1 *is a Sophie Germain prime and*

$x_1 \geqslant 2^{2^{16-3}} + 1$. *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* $\mathcal{Z}_{16}$ *with* Γ *instead of* Γ_{16}.

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

Lemma 23 *([18, p. 330]).* $8069496435 \cdot 10^{5072} - 1$ *is a Sophie Germain prime (Harvey Dubner).*

Lemma 24 $8069496435 \cdot 10^{5072} - 1 > 2^{2^{16-2}}$.

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

Proof. It follows from Lemmas 22–24. ■

Theorem 15 *The statement* Σ_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. ■

The question of solving the equation $x(x+1) = y!$ was posed by P. Erdös, 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 [13].

Theorem 16 *The statement* Σ_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. ■

10 Hypothetical statements $\Omega_3, \ldots, \Omega_{16}$ and their consequences

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

Lemma 25 *The number $(65!)^2+1$ is prime and $65! > 2^{2^{9-2}}$.*

Proof. The following `PARI/GP` ([17]) command

```
(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 ([24, 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 $\mathcal{Z}_9$ and $x_1 > 2^{2^{9-2}}$, then $x_1 = \min(x_1, \ldots, x_9)$.*

Theorem 17 *The statement Ω_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 $\mathcal{Z}_{14}$ and $x_1 > 2^{2^{14-2}}$, then $x_1 = \min(x_1, \ldots, x_{14})$.*

Theorem 18 *The statement Ω_{14} implies the infinitude of twin primes.*

Proof. It follows from Lemmas 19–21 and 27. ■

11 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 3 *([12, 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 [11, p. 23]. Let

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

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

Lemma 28 *The following subsystem of* H_n

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

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 ξ_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* $x_1,\ldots,x_n \leqslant h(n)$. The statement ξ_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* ξ_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. ■

Theorem 19 *The statement* ξ_{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

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

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

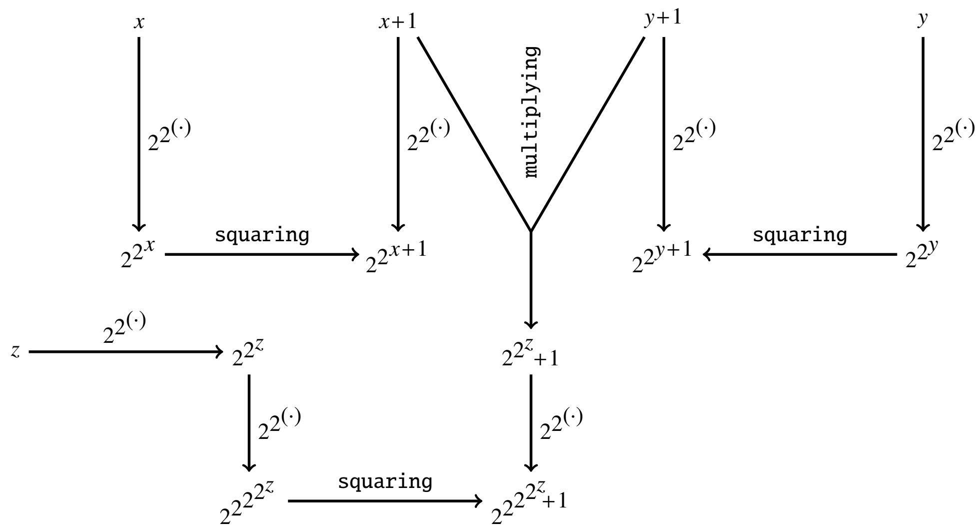

Fig. 9 Construction of the system $\mathcal{G}$

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

Corollary 7 *Let* $\mathcal{W}_{13}$ *denote the set of composite Fermat numbers. The statement* ξ_{13} *implies that we know an algorithm such that it returns a threshold number of* $\mathcal{W}_{13}$*, and this number equals* $\max(\mathcal{W}_{13})$*, if* $\mathcal{W}_{13}$ *is finite. Assuming the statement* ξ_{13}*, a single query to an oracle for the halting problem decides the infinity of* $\mathcal{W}_{13}$*. Assuming the statement* ξ_{13}*, the infinity of* $\mathcal{W}_{13}$ *is decidable in the limit.*

Proof. We consider an algorithm which computes $\max(\mathcal{W}_{13} \cap [1, h(12)])$. ∎

References

[1] C. H. Bennett, *Chaitin's Omega,* in: *Fractal music, hypercards, and more ...* (M. Gardner, ed.), W. H. Freeman, New York, 1992, 307–319.

[2] D. Berend and J. E. Harmse, *On polynomial-factorial Diophantine equations,* Trans. Amer. Math. Soc. 358 (2006), no. 4, 1741–1779.

[3] 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, `http://doi.org/10.1090/S0025-5718-01-01315-1`.

[4] C. S. Calude, H. Jürgensen, S. Legg, *Solving problems with finite test sets,* in: Finite versus Infinite: Contributions to an Eternal Dilemma (C. Calude and G. Păun, eds.), 39–52, Springer, London, 2000.

[5] N. C. A. da Costa and F. A. Doria, *On the foundations of science (LIVRO): essays, first series,* E-papers Serviços Editoriais Ltda, Rio de Janeiro, 2013.

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

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

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

[9] H. Friedman, *The incompleteness phenomena,* in: Proceedings of the AMS Centennial Symposium 1988, 49–84, Amer. Math. Soc., Providence, RI, 1992.

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

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

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

[13] F. Luca, *The Diophantine equation* $P(x) = n!$ *and a result of M. Overholt,* Glas. Mat. Ser. III 37 (57) (2002), no. 2, 269–273

[14] M. Mignotte and A. Pethő, *On the Diophantine equation* $x^p - x = y^q - y$, Publ. Mat. 43 (1999), no. 1, 207–216.

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

[16] M. Overholt, *The Diophantine equation* $n! + 1 = m^2$, Bull. London Math. Soc. 25 (1993), no. 2, 104.

[17] PARI/GP *online documentation,* http://pari.math.u-bordeaux.fr/dochtml/html/Arithmetic_functions.html.

[18] P. Ribenboim, *The new book of prime number records,* Springer, New York, 1996, http://doi.org/10.1007/978-1-4612-0759-7.

[19] S. Siksek, *Chabauty and the Mordell–Weil Sieve,* in: Advances on Superelliptic Curves and Their Applications (eds. L. Beshaj, T. Shaska, E. Zhupa), 194–224, IOS Press, Amsterdam, 2015, http://dx.doi.org/10.3233/978-1-61499-520-3-194.

[20] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, Smallest prime factor of* $\mathrm{A020549}(n) = (n!)^2 + 1$, http://oeis.org/A282706.

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

[22] Wolfram MathWorld, *Perfect Cuboid,* http://mathworld.wolfram.com/PerfectCuboid.html.

[23] Wolfram MathWorld, *Sophie Germain prime,* http://mathworld.wolfram.com/SophieGermainPrime.html.

[24] S. Y. Yan, *Number theory for computing,* 2nd ed., Springer, Berlin, 2002.

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

[26] A. A. Zenkin, *Superinduction: new logical method for mathematical proofs with a computer,* in: J. Cachro and K. Kijania-Placek (eds.), Volume of Abstracts, 11th International Congress of Logic, Methodology and Philosophy of Science, August 20–26, 1999, Cracow, Poland, p. 94, The Faculty of Philosophy, Jagiellonian University, Cracow, 1999.