On ZFC-formulae $\varphi(x)$ for which we explicitly know an integer n such that $\max(\{x \in \mathbb{N}\colon \varphi(x)\}) \leqslant n$ if the set $\{x \in \mathbb{N}\colon \varphi(x)\}$ is finite

Apoloniusz Tyszka

Abstract

Let $\Gamma(k)$ denote $(k-1)!$, and let $\Gamma_n(k)$ denote $(k-1)!$, where $n \in \{3,\ldots,16\}$ and $k \in \{2\} \cup [2^{2^{n-3}}+1,\infty) \cap \mathbb{N}$. For an integer $n \in \{3,\ldots,16\}$, let Σ_n denote the following statement: if a system of equations $\mathcal{S} \subseteq \{\Gamma_n(x_i)=x_k:\ i,k \in \{1,\ldots,n\}\} \cup \{x_i \cdot x_j = x_k:\ i,j,k \in \{1,\ldots,n\}\}$ with Γ instead of Γ_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 $\mathcal{S}$ satisfies $x_1,\ldots,x_n \leqslant 2^{2^{n-2}}$. Our hypothesis claims that the statements $\Sigma_3,\ldots,\Sigma_{16}$ are true. 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 $\{(1,2),(2,3)\}$. 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 $\{(4,5),(5,11),(7,71)\}$. The statement Σ_9 implies the infinitude of primes of the form n^2+1. 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 $n!+1$. The statement Σ_{14} implies the infinitude of twin primes. The statement Σ_{16} implies the infinitude of Sophie Germain primes.

Key words and phrases: Brocard's problem, Brocard-Ramanujan equation $x!+1=y^2$, composite Fermat numbers, Erdös' equation $x(x+1)=y!$, prime numbers of the form n^2+1, prime numbers of the form $n!+1$, Sophie Germain primes, twin primes.

2010 Mathematics Subject Classification: 03B30, 11A41.

1 Definitions and basic lemmas

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

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

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

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. [17] and [18]. 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 $\{\max(\mathcal{X}), \max(\mathcal{X})+1, \max(\mathcal{X})+2, \ldots\}$.

Lemma 1. *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 2. *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 3. *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 4. *(Wilson's theorem, [4, p. 89]). For every positive integer x, x divides* $(x-1)! + 1$ *if and only if $x = 1$ or x is prime.*

2 A variant of chess provides an example which explains the title

Let us assume that there are no draws, castlings, and en passant captures. Let us assume that a player with no moves loses. As such, the game may continue forever. Let $\mathcal{H}$ denote the set of all positive integers n such that an appropriate strategy of `Black` guarantees that `White` cannot enforce a win in less than n moves.

Lemma 5. *([11, p. 128]). A player who is in a winning position is always able to enforce a win in a number of moves that is less than the number of positions in the game.*

Lemma 6. *The number of positions does not exceed* 13^{64}.

Proof. With castlings or en passant captures, a legality of a move depends not only on the positions of the pieces on the board. Without castlings and en passant captures, we observe that 13 corresponds to 12 distinct pieces and the empty square. 64 is the number of squares on the chessboard. □

Lemmas 5 and 6 imply the following corollary.

Corollary 1. *If* `White` *have a winning strategy, then* $\mathcal{H} \subseteq [1, 13^{64} - 1]$. *Otherwise,* $\mathcal{H} = \mathbb{N} \setminus \{0\}$. *The number* $13^{64} - 1$ *is a threshold number of $\mathcal{H}$, and we can decide the equality $\mathcal{H} = \mathbb{N} \setminus \{0\}$. If $\mathcal{H} \neq \mathbb{N} \setminus \{0\}$, then we can compute $\mathcal{H}$ and* $\max(\mathcal{H})$.

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 1. *([3, p. 35]). There exists a polynomial $D(x_1, \ldots, x_m)$ with integer coefficients such that if ZFC is arithmetically consistent, then the sentences* "The equation $D(x_1, \ldots, x_m) = 0$ is solvable in non-negative integers" *and* "The equation $D(x_1, \ldots, x_m) = 0$ is not solvable in non-negative integers" *are not provable in ZFC.*

Let $\mathcal{Y}$ 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, we know an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in \mathcal{Y}$. Let $\gamma \colon \mathbb{N}^{m+1} \to \mathbb{N}$ be a computable bijection, and let $\mathcal{E} \subseteq \mathbb{N}^{m+1}$ be the solution set of the equation $D(x_1, \ldots, x_m) + 0 \cdot x_{m+1} = 0$. Theorem 1 implies Theorems 2 and 3.

Theorem 2. *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.*

Theorem 3. *We know an algorithm which for every $n \in \mathbb{N}$ decides whether or not $n \in \gamma(\mathcal{E})$. The set $\gamma(\mathcal{E})$ is empty or infinite. In both cases, every non-negative integer n is a threshold number of $\gamma(\mathcal{E})$. If ZFC is arithmetically consistent, then the sentences* "$\gamma(\mathcal{E})$ is empty", "$\gamma(\mathcal{E})$ is not empty", "$\gamma(\mathcal{E})$ is finite", *and* "$\gamma(\mathcal{E})$ is infinite" *are not provable in ZFC.*

4 Hypothetical statements $\Psi_3, \ldots, \Psi_{16}$

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 $\mathcal{U}_n$.

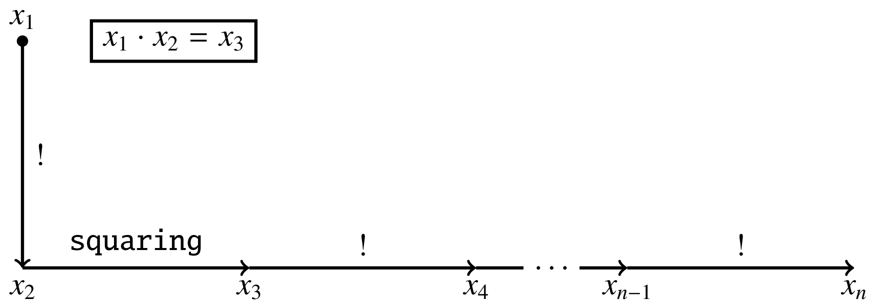

Fig. 1 Construction of the system $\mathcal{U}_n$

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

Lemma 7. *For every integer $n \geqslant 3$, the system $\mathcal{U}_n$ has exactly two solutions in positive integers, namely $(1,\ldots,1)$ and $\big(2,2,g(3),\ldots,g(n)\big)$.*

Let

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

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

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

Theorem 4. *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. □

Theorem 5. *For every statement Ψ_n, the bound $g(n)$ cannot be decreased.*

Proof. It follows from Lemma 7 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 1 and the diagram in Figure 2 explain the construction of the system $\mathcal{A}$.

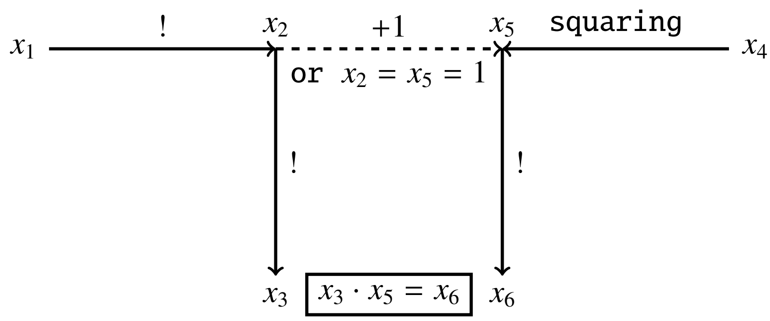

Fig. 2 Construction of the system $\mathcal{A}$

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:*

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

Proof. It follows from Lemma 1. □

It is conjectured that $x! + 1$ is a perfect square only for $x \in \{4, 5, 7\}$, see [14, 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 [9].

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 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 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 $x_1 \in \{1, \ldots, 23\}$, 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 $n^2 + 1$?

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

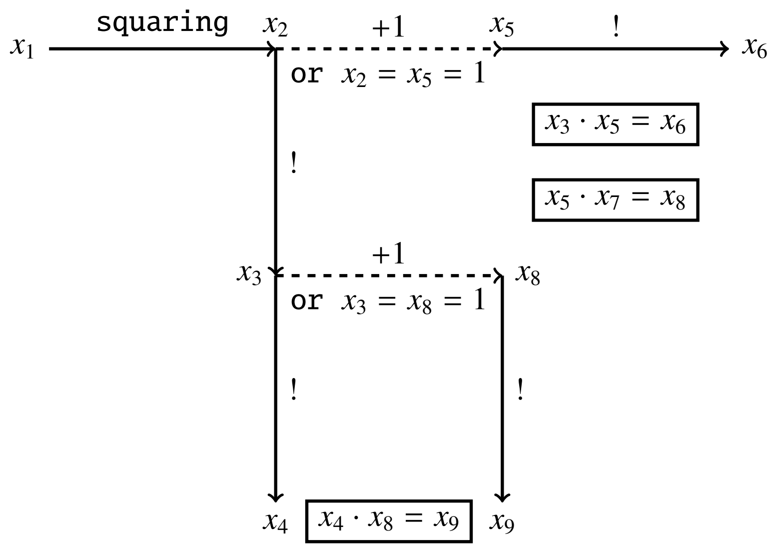

Fig. 3 Construction of the system $\mathcal{B}$

Lemma 9. *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:*

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

Proof. By Lemma 1, 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 9 follows from Lemma 4. □

Lemma 10. *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, $x_9 = x_8! \leqslant 2$. □

Edmund Landau's conjecture states that there are infinitely many primes of the form $n^2 + 1$, see [8, pp. 37–38].

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 9, 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 9 and 10, there are infinitely many primes of the form $n^2 + 1$. □

Corollary 2. *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.*

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

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] and [12].

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. □

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

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

Lemma 1 and the diagram in Figure 4 explain the construction of the system C.

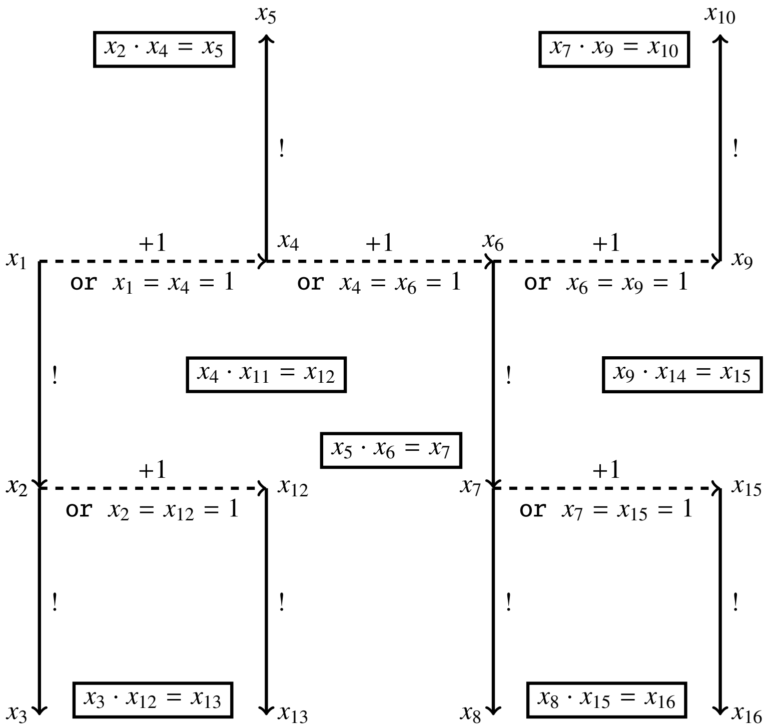

Fig. 4 Construction of the system C

Lemma 11. *For every $x_4, x_9 \in \mathbb{N} \setminus \{0,1,2\}$, the system C is solvable in positive integers $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$ 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:*

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

Proof. By Lemma 1, 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

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

Hence, the claim of Lemma 11 follows from Lemma 4. □

Lemma 12. *There are only finitely many tuples* $(x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ *which solve the system* C *and satisfy*

$$(x_4 \in \{1,2\}) \vee (x_9 \in \{1,2\})$$

Proof. If a tuple $(x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}$ solves the system 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 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 $x_9 - 1 \geqslant g(14)$. 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 $C \subseteq B_{16}$, the statement Ψ_{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. □

Corollary 3. *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.*

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

9 Hypothetical statements $\Delta_5, \ldots, \Delta_{14}$ about the Gamma function 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 2 and the diagram in Figure 5 explain the construction of the system $\mathcal{J}_n$.

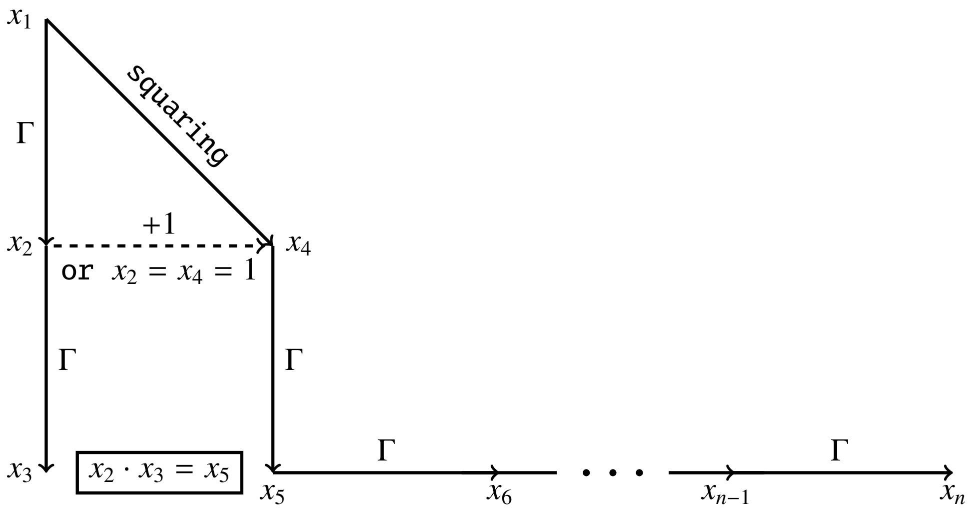

Fig. 5 Construction of the system $\mathcal{J}_n$

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

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

Lemmas 2 and 4 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 2 and 4. We leave the details to the reader. □

10 Hypothetical statements $\Sigma_3, \ldots, \Sigma_{16}$ about the Gamma function and their consequences

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

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

Lemma 13. *For every integer* $n \in \{3, \ldots, 16\}$*,* $P_n \subseteq Q_n$ *and the system* P_n *with* Γ *instead of* Γ_n *has exactly one solution in positive integers* $x_1, \ldots, x_n$*, namely* $\left(1, 2^{2^0},\ 2^{2^1}, 2^{2^2}, \ldots, 2^{2^{n-2}}\right)$*.*

For an integer $n \in \{3, \ldots, 16\}$, 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 $x_1, \ldots, x_n$, then every tuple $(x_1, \ldots, x_n) \in (\mathbb{N} \setminus \{0\})^n$ that solves the original system $\mathcal{S}$ satisfies $x_1, \ldots, x_n \leqslant 2^{2^{n-2}}$.

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

Lemma 14. *(cf. Lemma 2). 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* $(x + 1 = y) \wedge \left(x \geqslant 2^{2^{n-3}} + 1\right)$*.*

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

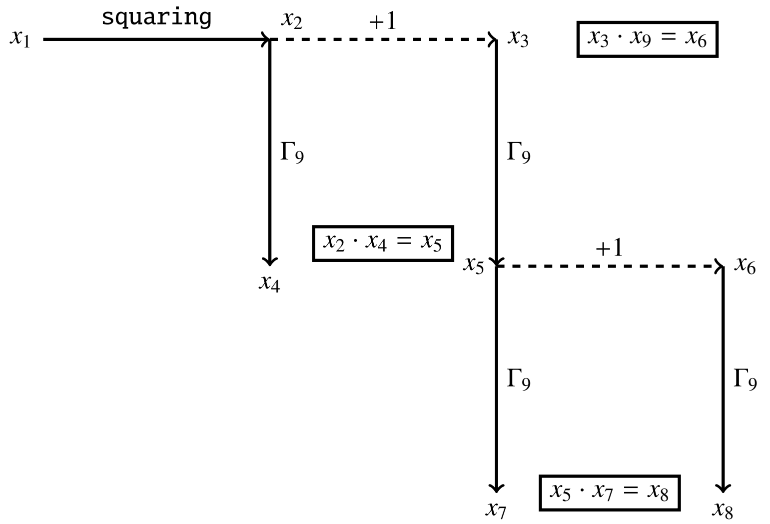

Fig. 6 Construction of the system $\mathcal{Z}_9$

Lemma 15. *For every positive integer x_1, the system $\mathcal{Z}_9$ 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 $\mathcal{Z}_9$ with Γ instead of Γ_9.*

Proof. It follows from Lemmas 2, 4, and 14. □

Lemma 16. *([13]). The number $(13!)^2 + 1 = 38775788043632640001$ is prime.*

Lemma 17. $\left((13!)^2 \geqslant 2^{2^{9-3}} + 1 = 18446744073709551617\right) \wedge \left(\Gamma_9((13!)^2) > 2^{2^{9-2}}\right)$.

Theorem 11. *The statement Σ_9 implies the infinitude of primes of the form $n^2 + 1$.*

Proof. It follows from Lemmas 15–17. □

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 4. *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.*

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.

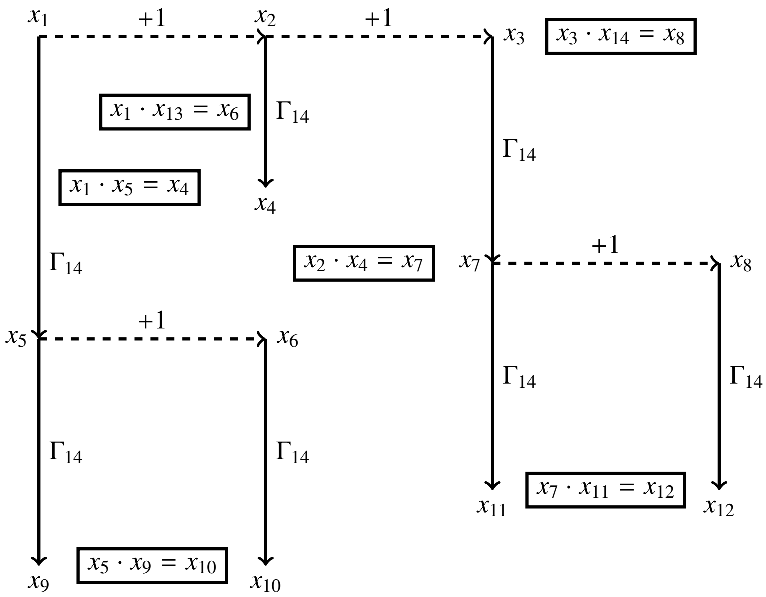

Fig. 7 Construction of the system $\mathcal{Z}_{14}$

Lemma 18. *For every positive integer x_1, the system $\mathcal{Z}_{14}$ is solvable in positive integers $x_2, \dots, x_{14}$ 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 $x_2, \dots, x_{14}$ are uniquely determined by x_1. For every positive integer n, at most finitely many tuples $(x_1, \dots, x_{14}) \in (\mathbb{N} \setminus \{0\})^{14}$ begin with n and solve the system $\mathcal{Z}_{14}$ with Γ instead of Γ_{14}.*

Proof. It follows from Lemmas 2, 4, and 14. □

Lemma 19. *([16, p. 87]). The numbers $459 \cdot 2^{8529} - 1$ and $459 \cdot 2^{8529} + 1$ are prime (Harvey Dubner).*

Lemma 20. $459 \cdot 2^{8529} - 1 > 2^{2^{14-2}} = 2^{4096}$.

Theorem 13. *The statement Σ_{14} implies the infinitude of twin primes.*

Proof. It follows from Lemmas 18–20. □

A prime p is said to be a Sophie Germain prime if both p and $2p+1$ are prime, see [15]. Let $\mathcal{Z}_{16} \subseteq Q_{16}$ be the system of equations in Figure 8.

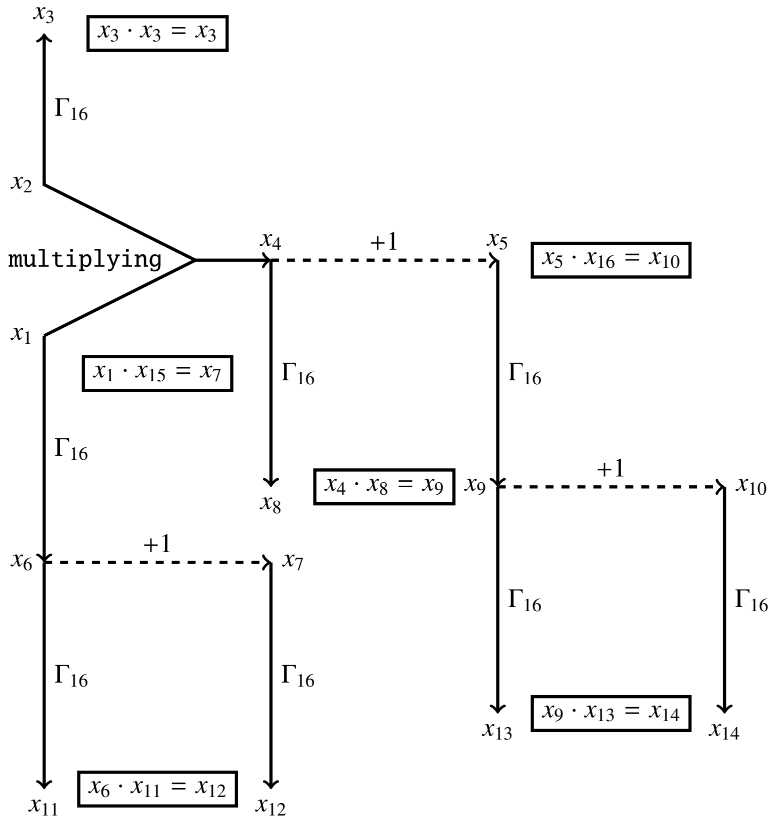

Fig. 8 Construction of the system $\mathcal{Z}_{16}$

Lemma 21. *For every positive integer x_1, the system $\mathcal{Z}_{16}$ is solvable in positive integers $x_2, \ldots, x_{16}$ if and only if x_1 is a Sophie Germain prime and $x_1 \geqslant 2^{2^{16-3}} + 1$. 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 2, 4, and 14. □

Lemma 22. *([10, p. 330]).* $8069496435 \cdot 10^{5072} - 1$ *is a Sophie Germain prime (Harvey Dubner).*

Lemma 23. $8069496435 \cdot 10^{5072} - 1 > 2^{2^{16-2}}$.

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

Proof. It follows from Lemmas 21–23. □

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 [1]. F. Luca proved that the *abc* conjecture implies that the equation $x(x+1) = y!$ has only finitely many solutions in positive integers, see [7].

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. □

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 [6, 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 [6, p. 1].

Open Problem. ([6, 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 [5, 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 24. *The following subsystem of* H_n

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

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* $S \subseteq H_n$ *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.*

Theorem 17. *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 18. *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

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

in positive integers. By Lemma 3, we can transform equation (1) into an equivalent system $\mathcal{G}$ 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.

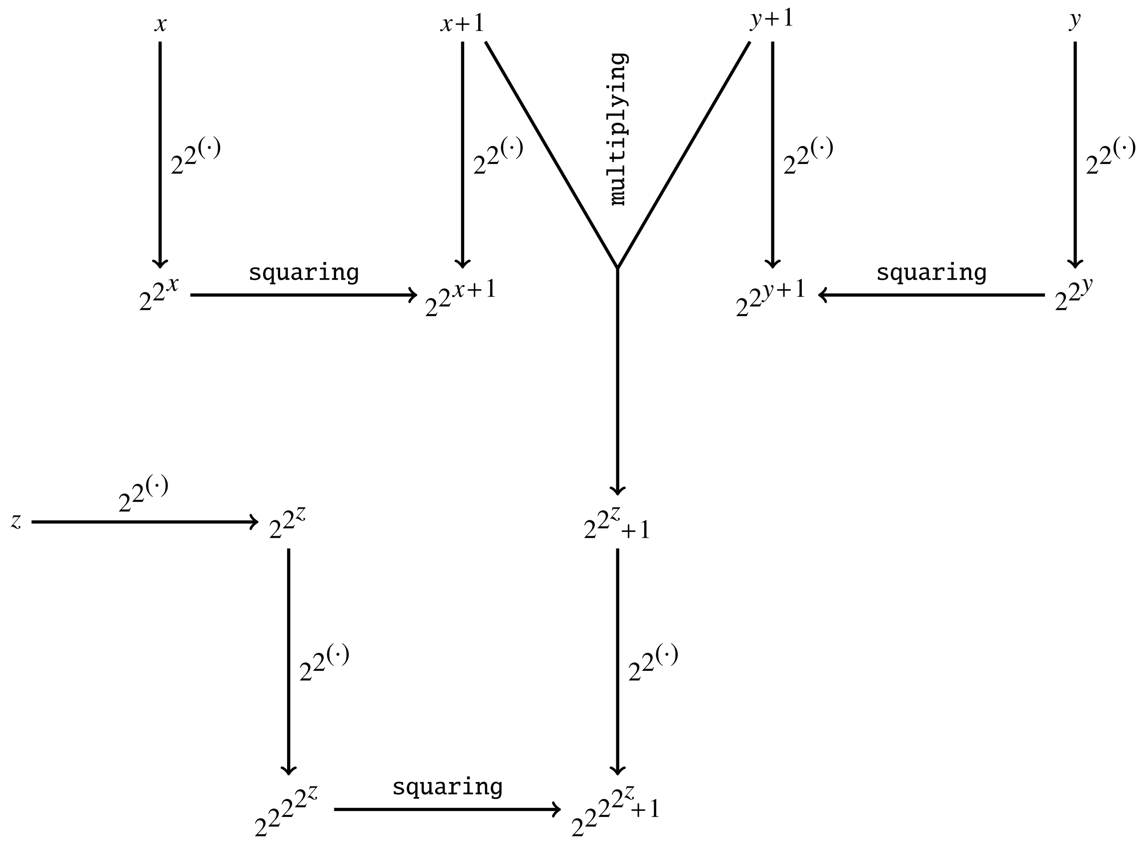

Fig. 9 Construction of the system $\mathcal{G}$

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 5. *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.*

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

References

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

[2] 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`.

[3] 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.

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

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

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

[7] 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

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

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

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

[11] U. Schwalbe and P. Waker, *Zermelo and the early history of game theory,* Games Econom. Behav. 34 (2001), no. 1, 123–137, `http://doi.org/10.1006/game.2000.0794`.

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

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

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

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

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

[17] 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`.

[18] 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.

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