On sets $\mathcal{X} \subseteq \mathbb{N}$ for which we know an algorithm that computes a threshold number $t(\mathcal{X}) \in \mathbb{N}$ such that $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ contains an element greater than $t(\mathcal{X})$

Apoloniusz Tyszka

Abstract

Let $\Gamma_{\boxed{n}}(k)$ denote $(k-1)!$, where $n \in \{3,\ldots,16\}$ and $k \in \{2\} \cup \left\{2^{2^{n-3}}+1, 2^{2^{n-3}}+2, 2^{2^{n-3}}+3, \ldots\right\}$. For an integer $n \in \{3,\ldots,16\}$, let Σ_n denote the following statement: if a system of equations $\mathcal{S} \subseteq \{\Gamma_{\boxed{n}}(x_i) = x_k :\ i,k \in \{1,\ldots,n\}\} \cup \{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\ldots,n\}\}$ has only finitely many solutions in positive integers $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $x_1,\ldots,x_n \leqslant 2^{2^{n-2}}$. 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. A modified statement Σ_7 implies the infinitude of Wilson 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 $n!+1$, Richert's lemma, Sophie Germain primes, Wilson primes, twin prime conjecture.

2010 Mathematics Subject Classification: 03B30, 11A41, 68Q05.

1 Introduction

We consider sets $\mathcal{X} \subseteq \mathbb{N}$ for which we know an algorithm that computes a threshold number $t(\mathcal{X}) \in \mathbb{N}$ such that $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ contains an element greater than $t(\mathcal{X})$. We assume here that the sets $\mathcal{X} \subseteq \mathbb{N}$ are defined by formulae in the language of ZF whereas the algorithm that computes $t(\mathcal{X})$ is written specifically for $\mathcal{X}$. 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 $\{\max(\mathcal{X}), \max(\mathcal{X})+1, \max(\mathcal{X})+2, \ldots\}$.

2 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. *([4, 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.*

In Figure 1, $D(x_1,\ldots,x_m)$ stands for the polynomial described in Theorem 1. Let $\mathcal{K}$ denote the set of all positive integers k such that the algorithm in Figure 1 halts for k on the input. If *ZFC* is consistent, then $\mathcal{K} = \emptyset$. Otherwise, $\mathrm{card}(\mathcal{K}) = 1$.

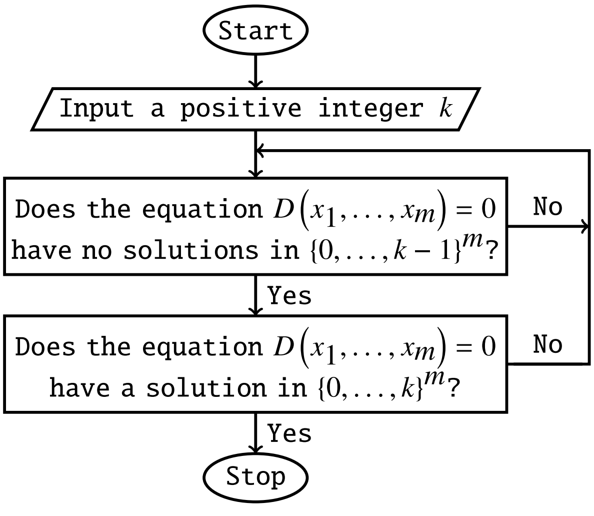
Start
Input a positive integer k
Does the equation $D(x_1,\ldots,x_m) = 0$ have no solutions in $\{0,\ldots,k-1\}^m$?
No
Yes
Does the equation $D(x_1,\ldots,x_m) = 0$ have a solution in $\{0,\ldots,k\}^m$?
No
Yes
Stop

Fig. 1 The algorithm which may halt only when *ZFC* is inconsistent

Theorem 4. *If ZFC is consistent, then for every positive integer n, the inclusion $\mathcal{K} \subseteq \{1,\ldots,n\}$ is not provable in ZFC.*

Proof. It follows from Gödel's second incompleteness theorem because the inclusion $\mathcal{K} \subseteq \{1,\ldots,n\}$ implies $\mathcal{K} = \emptyset$ and the consistency of *ZFC*. □

Theorem 5. *(cf. Theorem 29). If ZFC is consistent and a computer program halts for at most finitely many positive integers k on the input, then not always we can write the decimal expansion of a positive integer n which is not smaller than every such number k.*

Proof. We write a computer program which implements the algorithm in Figure 1. This program halts exactly for elements of $\mathcal{K}$ on the input. The set $\mathcal{K}$ is finite as $\mathrm{card}(\mathcal{K}) \leqslant 1$. By Theorem 4, if *ZFC* is consistent, then for every positive integer n, the inclusion $\mathcal{K} \subseteq \{1,\ldots,n\}$ is not provable in *ZFC*. □

3 Hypothetical statements $\Psi_3,\ldots,\Psi_{16}$ and number-theoretic lemmas

For a positive integer n, let $\Gamma(n)$ denote $(n-1)!$. Let $f(1) = 2$, $f(2) = 4$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 2$. Let $h(1) = 1$, and let $h(n+1) = 2^{2^{h(n)}}$ for every positive integer n. Let $g(3) = 4$, and let $g(n+1) = g(n)!$ for every integer $n \geqslant 3$. For an integer $n \geqslant 3$, let $\mathcal{U}_n$ denote the following system of equations:

$$\left\{\begin{array}{rcl} \forall i \in \{1,\ldots,n-1\} \setminus \{2\}\ x_i! & = & x_{i+1} \\ x_1 \cdot x_2 & = & x_3 \\ x_2 \cdot x_2 & = & x_3 \end{array}\right.$$

The diagram in Figure 2 illustrates the construction of the system $\mathcal{U}_n$.

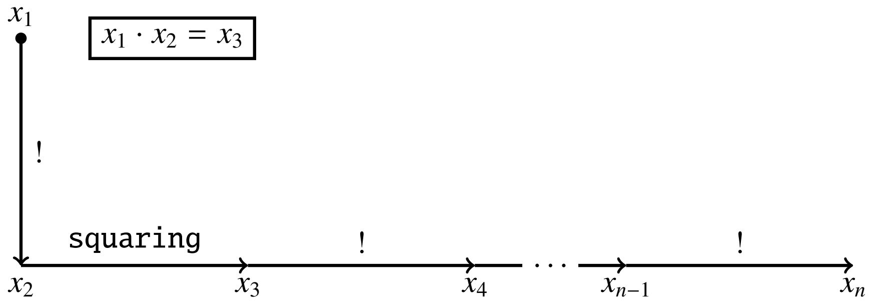

Fig. 2 Construction of the system $\mathcal{U}_n$

Lemma 1. *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 $\mathcal{S} \subseteq B_n$ 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.*

Theorem 6. *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 7. *For every statement Ψ_n, the bound $g(n)$ cannot be decreased.*

Proof. It follows from Lemma 1 because $\mathcal{U}_n \subseteq B_n$. □

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

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

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 positive integers x and y, $x + 1 = y$ if and only if*

$$(1 \neq y) \wedge (x! \cdot y = y!)$$

Lemma 5. *For every non-negative integers b and c, $b + 1 = c$ if and only if $2^{2^b} \cdot 2^{2^b} = 2^{2^c}$.*

Let $\mathcal{P}$ denote the set of prime numbers.

Lemma 6. *(Wilson's theorem, [7, p. 89]). For every positive integer x, x divides $(x - 1)! + 1$ if and only if $x \in \{1\} \cup \mathcal{P}$.*

4 Heuristic arguments against the statement $\forall n \in \mathbb{N} \setminus \{0,1,2\}\ \Psi_n$

Let

$$G_n = \{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\dots,n\}\} \cup \{x_i + 1 = x_k :\ i,k \in \{1,\dots,n\}\}$$

Hypothesis 2. *([30, p. 109]. If a system $\mathcal{S} \subseteq G_n$ has only finitely many solutions in non-negative integers $x_1,\dots,x_n$, then each such solution $(x_1,\dots,x_n)$ satisfies $x_1,\dots,x_n \leqslant h(2n)$.*

Hypothesis 3. *If a system $\mathcal{S} \subseteq G_n$ has only finitely many solutions in positive integers $x_1,\dots,x_n$, then each such solution $(x_1,\dots,x_n)$ satisfies $x_1,\dots,x_n \leqslant f(2n)$.*

Observations 1 and 2 heuristically justify Hypothesis 3.

Observation 1. *(cf. [30, p. 110, Observation 1]). For every system $\mathcal{S} \subseteq G_n$ which involves all the variables $x_1,\dots,x_n$, the following new system*

$$\left(\bigcup_{x_i \cdot x_j = x_k \in \mathcal{S}} \{x_i \cdot x_j = x_k\}\right) \cup \{x_k! = y_k :\ k \in \{1,\dots,n\}\} \cup \left(\bigcup_{x_i + 1 = x_k \in \mathcal{S}} \{1 \neq x_k,\ y_i \cdot x_k = y_k\}\right)$$

is equivalent to $\mathcal{S}$. If the system $\mathcal{S}$ has only finitely many solutions in positive integers $x_1,\dots,x_n$, then the new system has only finitely many solutions in positive integers $x_1,\dots,x_n,y_1,\dots,y_n$.

Proof. It follows from Lemma 4. □

Observation 2. *The equation $x_1! = x_1$ has exactly two solutions in positive integers, namely $x_1 = 1$ and $x_1 = f(1)$. The system $\begin{cases} x_1! = x_1 \\ x_1 \cdot x_1 = x_2 \end{cases}$ has exactly two solutions in positive integers, namely $(1,1)$ and $(f(1), f(2))$. For every integer $n \geqslant 3$, the following system*

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

has exactly two solutions in positive integers, namely $(1,\dots,1)$ and $(f(1),\dots,f(n))$.

For a positive integer n, let Φ_n denote the following statement: *if a system*

$$\mathcal{S} \subseteq \{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\dots,n\}\} \cup \{x_i! = x_k :\ i,k \in \{1,\dots,n\}\} \cup \{1 \neq x_k :\ k \in \{1,\dots,n\}\}$$

has only finitely many solutions in positive integers $x_1,\dots,x_n$, then each such solution $(x_1,\dots,x_n)$ satisfies $x_1,\dots,x_n \leqslant f(n)$.

Theorem 8. *The statement $\forall n \in \mathbb{N} \setminus \{0\}\ \Phi_n$ implies Hypothesis 3.*

Proof. It follows from Lemma 4. □

Let $\mathcal{R}ng$ denote the class of all rings $\boldsymbol{K}$ that extend $\mathbb{Z}$, and let

$$E_n = \{1 = x_k :\ k \in \{1,\dots,n\}\} \cup \{x_i + x_j = x_k :\ i,j,k \in \{1,\dots,n\}\} \cup \{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\dots,n\}\}$$

Th. Skolem proved that every Diophantine equation can be algorithmically transformed into an equivalent system of Diophantine equations of degree at most 2, see [22, pp. 2–3] and [13, pp. 3–4]. The following result strengthens Skolem's theorem.

Lemma 7. *([28, p. 720]). Let* $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$. *Assume that* $\deg(D, x_i) \geqslant 1$ *for each* $i \in \{1, \ldots, p\}$. *We can compute a positive integer* $n > p$ *and a system* $T \subseteq E_n$ *which satisfies the following two conditions:*

`Condition 1.` *If* $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$, *then*

$$\forall \tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K} \left(D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \Longleftrightarrow \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \boldsymbol{K}\ (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \textit{ solves } T\right)$$

`Condition 2.` *If* $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$, *then for each* $\tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K}$ *with* $D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0$, *there exists a unique tuple* $(\tilde{x}_{p+1}, \ldots, \tilde{x}_n) \in \boldsymbol{K}^{n-p}$ *such that the tuple* $(\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n)$ *solves* T.

Conditions 1 and 2 imply that for each $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$, *the equation* $D(x_1, \ldots, x_p) = 0$ *and the system* T *have the same number of solutions in* $\boldsymbol{K}$.

Let α, β, and γ denote variables.

Lemma 8. *([20, p. 100]) For each positive integers* x, y, z, $x + y = z$ *if and only if*

$$(zx + 1)(zy + 1) = z^2(xy + 1) + 1$$

Corollary 1. *We can express the equation* $x + y = z$ *as an equivalent system* $\mathcal{F}$, *where* $\mathcal{F}$ *involves* x, y, z *and* 9 *new variables, and where* $\mathcal{F}$ *consists of equations of the forms* $\alpha + 1 = \gamma$ *and* $\alpha \cdot \beta = \gamma$.

Proof. The new 9 variables express the following polynomials:

$$zx, \quad zx + 1, \quad zy, \quad zy + 1, \quad z^2, \quad xy, \quad xy + 1, \quad z^2(xy + 1), \quad z^2(xy + 1) + 1$$

□

Lemma 9. *(cf. [30, p. 110, Lemma 4]). Let* $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$. *Assume that* $\deg(D, x_i) \geqslant 1$ *for each* $i \in \{1, \ldots, p\}$. *We can compute a positive integer* $n > p$ *and a system* $T \subseteq G_n$ *which satisfies the following two conditions:*

`Condition 3.` *For every positive integers* $\tilde{x}_1, \ldots, \tilde{x}_p$,

$$D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \Longleftrightarrow \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \mathbb{N} \setminus \{0\}\ (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \textit{ solves } T$$

`Condition 4.` *If positive integers* $\tilde{x}_1, \ldots, \tilde{x}_p$ *satisfy* $D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0$, *then there exists a unique tuple* $(\tilde{x}_{p+1}, \ldots, \tilde{x}_n) \in (\mathbb{N} \setminus \{0\})^{n-p}$ *such that the tuple* $(\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n)$ *solves* T.

Conditions 3 and 4 imply that the equation $D(x_1, \ldots, x_p) = 0$ *and the system* T *have the same number of solutions in positive integers.*

Proof. Let the system T be given by Lemma 7. We replace in T each equation of the form $1 = x_k$ by the equation $x_k \cdot x_k = x_k$. Next, we apply Corollary 1 and replace in T each equation of the form $x_i + x_j = x_k$ by an equivalent system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. □

Theorem 9. *Hypothesis 3 implies that there is an algorithm which takes as input a 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.*

Proof. It follows from Lemma 9. □

Open Problem 1. *Is there an algorithm which takes as input a Diophantine equation, and returns an integer such that this integer is greater than the moduli of integer (non-negative integer, positive integer) solutions, if the solution set is finite?*

Matiyasevich's conjecture on finite-fold Diophantine representations ([15]) implies a negative answer to Open Problem 1, see [14, p. 42].

The statement $\forall n \in \mathbb{N} \setminus \{0\}\ \Phi_n$ implies that there is an algorithm which takes as input a factorial Diophantine equation, and returns an integer such that this integer is greater than the solutions in positive integers, if these solutions form a finite set. This conclusion is a bit strange because a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [12, p. 300].

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 3 explain the construction of the system $\mathcal{A}$.

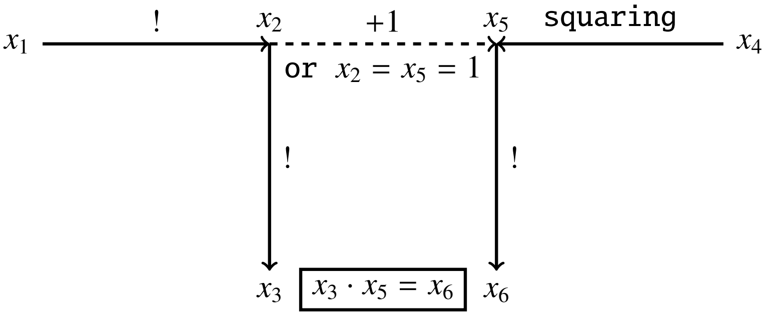

Fig. 3 Construction of the system $\mathcal{A}$

Lemma 10. *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 [31, 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 [17].

Theorem 10. *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 10, 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 $n^2 + 1$?

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 4 explain the construction of the system $\mathcal{B}$.

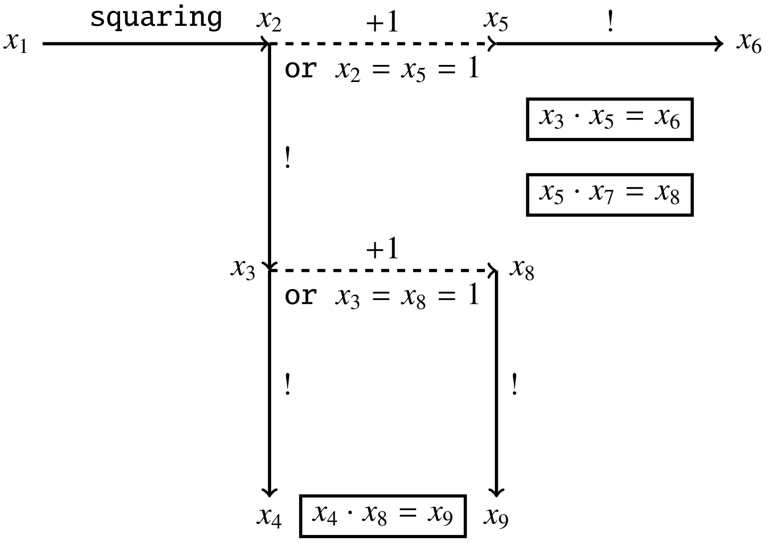

Fig. 4 Construction of the system $\mathcal{B}$

Lemma 11. *For every integer $x_1 \geqslant 2$, the system $\mathcal{B}$ is solvable in positive integers $x_2, \dots, x_9$ if and only if $x_1^2 + 1$ is prime. In this case, the integers $x_2, \dots, x_9$ 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 2, for every integer $x_1 \geqslant 2$, the system $\mathcal{B}$ is solvable in positive integers $x_2, \dots, x_9$ if and only if $x_1^2 + 1$ divides $(x_1^2)! + 1$. Hence, the claim of Lemma 11 follows from Lemma 6. □

Lemma 12. *There are only finitely many tuples $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ which solve the system $\mathcal{B}$ and satisfy $x_1 = 1$.*

Proof. If a tuple $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ solves the system $\mathcal{B}$ and $x_1 = 1$, then $x_1, \dots, x_9 \leqslant 2$. 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 [16, pp. 37–38].

Theorem 11. *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 11, there exists a unique tuple $(x_2, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^8$ such that the tuple $(x_1, x_2, \dots, x_9)$ 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 $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0\})^9$. According to Lemmas 11 and 12, there are infinitely many primes of the form $n^2 + 1$. □

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 [3, p. 443] and [23].

Theorem 12. *(cf. Theorem 17). 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 [16, p. 39]. Let C denote the following system of equations:

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

Lemma 2 and the diagram in Figure 5 explain the construction of the system C.

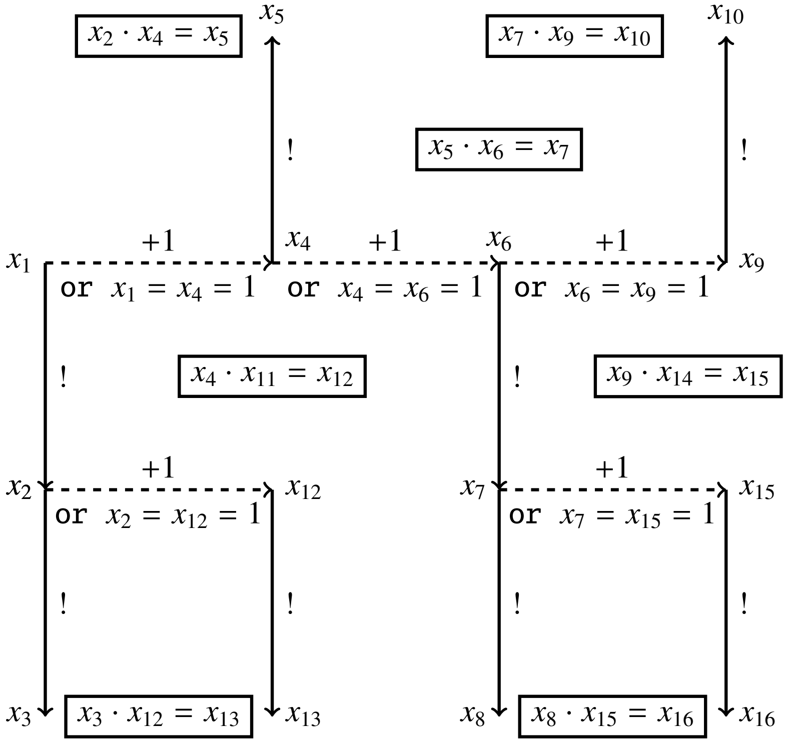

Fig. 5 Construction of the system C

Lemma 13. *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:*

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

Proof. By Lemma 2, for every $x_4, x_9 \in \mathbb{N} \setminus \{0,1,2\}$, the system 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 13 follows from Lemma 6. □

Lemma 14. *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 13. *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 13, 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 13 and 14, there are infinitely many twin primes. □

Let $\mathbb{P}(x)$ denote the predicate "*x is a prime number*". Dickson's conjecture ([16, p. 36], [33, p. 109]) implies that the existential theory of $(\mathbb{N}, =, +, \mathbb{P})$ is decidable, see [33, Theorem 2, p. 109]. For a positive integer n, let Θ_n denote the following statement: *for every system $\mathcal{S} \subseteq \{x_i + 1 = x_k : \ i,k \in \{1, \ldots, n\}\} \cup \{\mathbb{P}(x_i) : \ i \in \{1, \ldots, n\}\}$ the solvability of $\mathcal{S}$ in non-negative integers is decidable.*

Lemma 15. *If the existential theory of* $(\mathbb{N}, =, +, \mathbb{P})$ *is decidable, then the statements* Θ_n *are true.*

Proof. For every non-negative integers x and y, $x + 1 = y$ if and only if

$$\exists u, v \in \mathbb{N} \ \ ((u + u = v) \wedge \mathbb{P}(v) \wedge (x + u = y))$$

□

Theorem 14. *The conjunction of the implication (∗) and the statement* $\Theta_{g(14)+2}$ *implies that the twin prime conjecture is decidable.*

Proof. By the statement $\Theta_{g(14)+2}$, we can decide the truth of the sentence

$$\exists x_1 \ldots \exists x_{g(14)+2} \left((\forall i \in \{1, \ldots, g(14) + 1\} \ x_i + 1 = x_{i+1}) \wedge \mathbb{P}(x_{g(14)}) \wedge \mathbb{P}(x_{g(14)+2}) \right) \tag{1}$$

If sentence (1) is false, then the twin prime conjecture is false. If sentence (1) is true, then there exists a twin prime greater than $g(14)$. In this case, the twin prime conjecture follows from Theorem 13. □

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 3 and the diagram in Figure 6 explain the construction of the system $\mathcal{J}_n$.

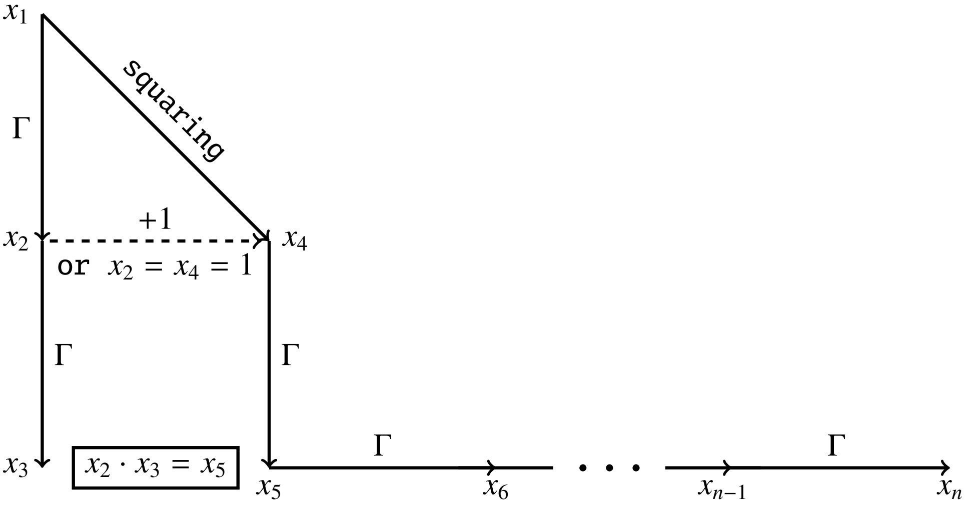

Fig. 6 Construction of the system $\mathcal{J}_n$

Observation 3. *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 4. *The statements* $\Delta_5, \ldots, \Delta_{14}$ *are true.*

Lemmas 3 and 6 imply that the statements Δ_n have similar consequences as the statements Ψ_n.

Theorem 15. *The statement* Δ_6 *implies that any prime number* $p \geqslant 25$ *proves the infinitude of primes.*

Proof. It follows from Lemmas 3 and 6. We leave the details to the reader. □

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

Let $\Gamma_{\boxed{n}}(k)$ denote $(k-1)!$, where $n \in \{3,\ldots,16\}$ and $k \in \{2\} \cup \left\{2^{2^{n-3}}+1,\ 2^{2^{n-3}}+2,\ 2^{2^{n-3}}+3,\ \ldots\right\}$. For an integer $n \in \{3,\ldots,16\}$, let

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

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

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

Lemma 16. *For every integer $n \in \{3,\ldots,16\}$, $P_n \subseteq Q_n$ and the system P_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 $\mathcal{S} \subseteq Q_n$ has only finitely many solutions in positive integers $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $x_1,\ldots,x_n \leqslant 2^{2^{n-2}}$.

Hypothesis 5. *The statements $\Sigma_3,\ldots,\Sigma_{16}$ are true.*

Lemma 17. *(cf. Lemma 3). For every integer $n \in \{4,\ldots,16\}$ and for every positive integers x and y, $x \cdot \Gamma_{\boxed{n}}(x) = \Gamma_{\boxed{n}}(y)$ 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 7.

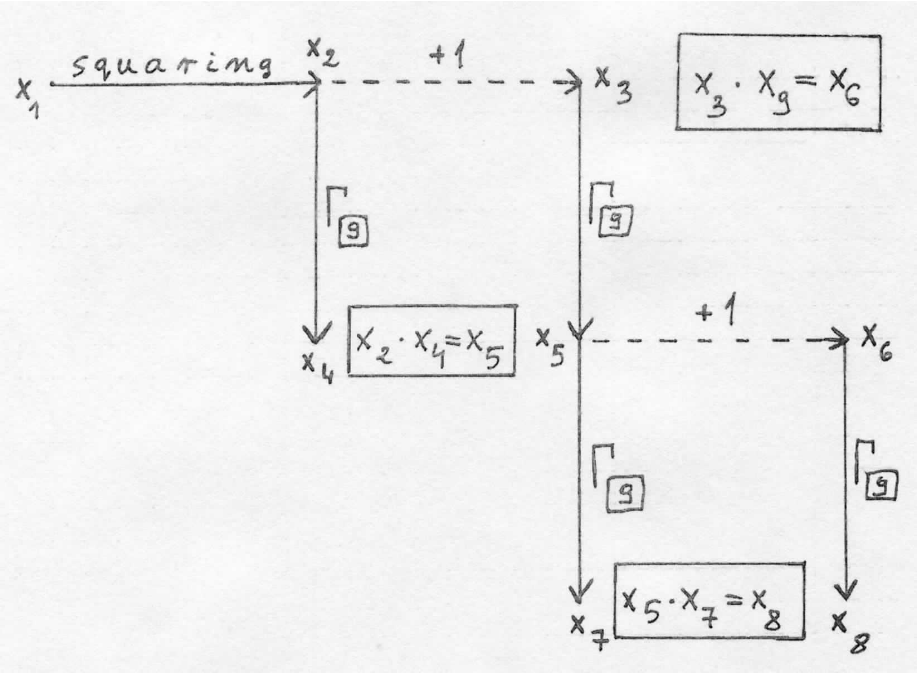

Fig. 7 Construction of the system $\mathcal{Z}_9$

Lemma 18. *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.*

Proof. It follows from Lemmas 6 and 17. □

Lemma 19. *([26]). The number* $(13!)^2 + 1 = 38775788043632640001$ *is prime.*

Lemma 20. $\left((13!)^2 \geqslant 2^{2^{9-3}} + 1 = 18446744073709551617\right) \wedge \left(\Gamma_{\boxed{9}}((13!)^2) > 2^{2^{9-2}}\right)$.

Theorem 16. *The statement* Σ_9 *implies the infinitude of primes of the form* $n^2 + 1$.

Proof. It follows from Lemmas 18–20. □

Theorem 17. *(cf. Theorem 12). 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. □

Let $\mathcal{Z}_{14} \subseteq Q_{14}$ be the system of equations in Figure 8.

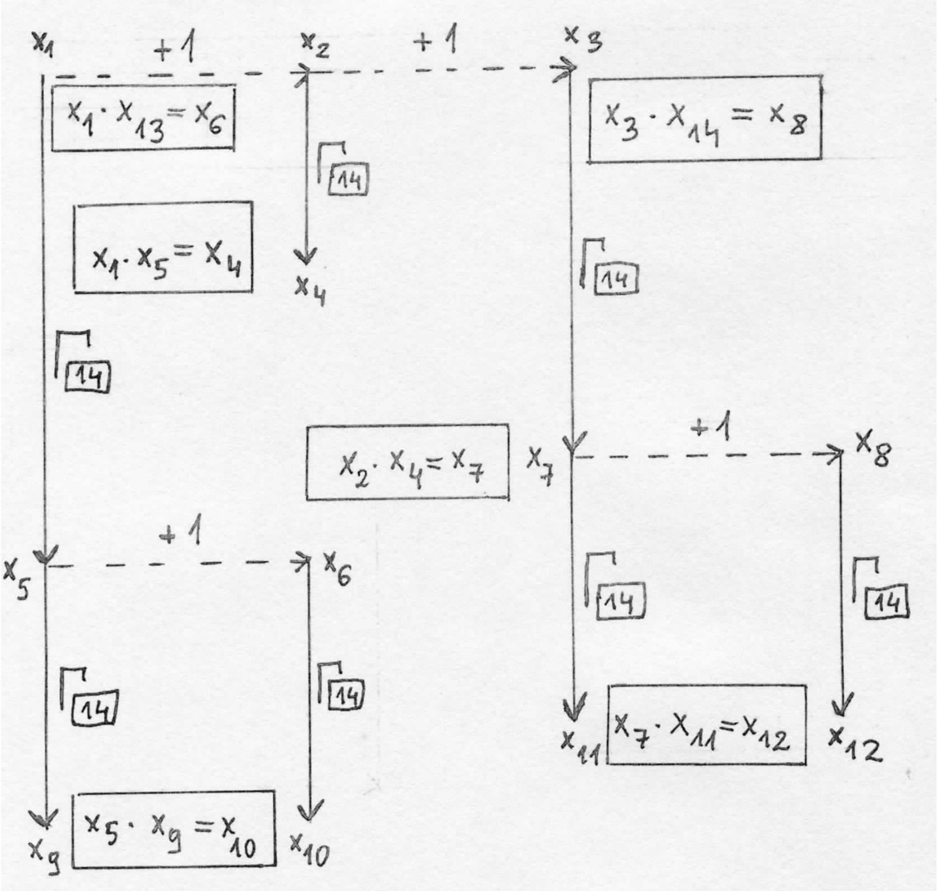

Fig. 8 Construction of the system $\mathcal{Z}_{14}$

Lemma 21. *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.

Proof. It follows from Lemmas 6 and 17. □

Lemma 22. *([34, p. 87]). The numbers* $459 \cdot 2^{8529} - 1$ *and* $459 \cdot 2^{8529} + 1$ *are prime (Harvey Dubner).*

Lemma 23. $459 \cdot 2^{8529} - 1 > 2^{2^{14-2}} = 2^{4096}$.

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

Proof. It follows from Lemmas 21–23. □

A prime p is said to be a Sophie Germain prime if both p and $2p + 1$ are prime, see [32]. Let $\mathcal{Z}_{16} \subseteq Q_{16}$ be the system of equations in Figure 9.

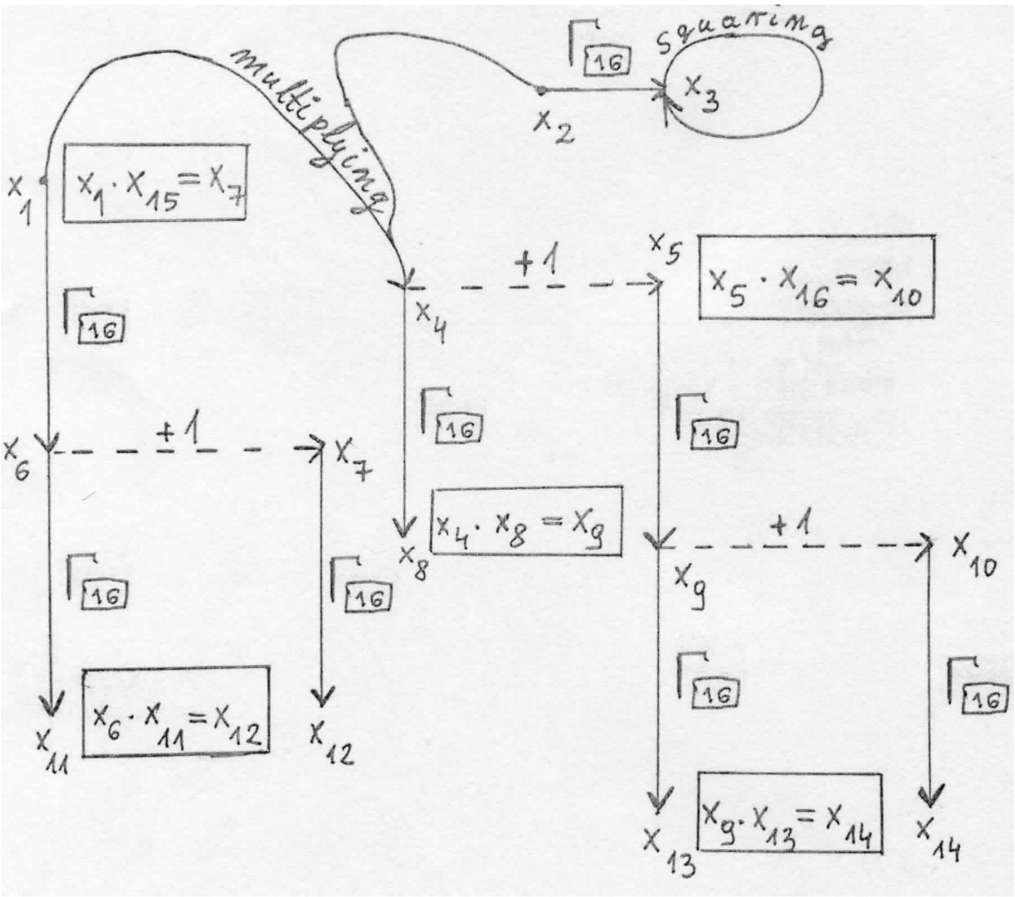

Fig. 9 Construction of the system $\mathcal{Z}_{16}$

Lemma 24. *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.*

Proof. It follows from Lemmas 6 and 17. □

Lemma 25. *([18, p. 330]).* $8069496435 \cdot 10^{5072} - 1$ *is a Sophie Germain prime (Harvey Dubner).*

Lemma 26. $8069496435 \cdot 10^{5072} - 1 > 2^{2^{16-2}}$.

Theorem 19. *The statement Σ_{16} implies the infinitude of Sophie Germain primes.*

Proof. It follows from Lemmas 24–26. □

Theorem 20. *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 [11].

Theorem 21. *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 A hypothesis which implies the infinitude of Wilson primes

Let

$$\mathcal{V}_7 = \{\Gamma_{\boxed{5}}(x_i) = x_k :\ i,k \in \{1,\ldots,7\}\} \cup \{x_i \cdot x_j = x_k :\ i,j,k \in \{1,\ldots,7\}\}$$

Let $\mathcal{I}_7$ denote the following system of equations:

$$\begin{cases} x_1 \cdot x_1 &=& x_1 \\ \Gamma_{\boxed{5}}(x_2) &=& x_1 \\ x_2 \cdot x_2 &=& x_3 \\ x_3 \cdot x_3 &=& x_4 \\ x_4 \cdot x_4 &=& x_5 \\ \Gamma_{\boxed{5}}(x_5) &=& x_6 \\ \Gamma_{\boxed{5}}(x_6) &=& x_7 \end{cases}$$

Lemma 27. *$\mathcal{I}_7 \subseteq \mathcal{V}_7$ and the system $\mathcal{I}_7$ has exactly one solution in positive integers $x_1,\ldots,x_7$, namely* $(1,2,4,16,256,255!,(255!-1)!)$.

Let Ξ_7 denote the following statement: if a system of equations $\mathcal{S} \subseteq \mathcal{V}_7$ has only finitely many solutions in positive integers $x_1,\ldots,x_7$, then each such solution $(x_1,\ldots,x_7)$ satisfies $x_1,\ldots,x_7 \leqslant (255!-1)!$.

Hypothesis 6. *The statement Ξ_7 is true.*

Lemma 28. *(cf. Lemma 3). For every positive integers x and y, $x \cdot \Gamma_{\boxed{5}}(x) = \Gamma_{\boxed{5}}(y)$ if and only if* $(x+1=y) \wedge (x \geqslant 17)$.

A Wilson prime is a prime number p such that p^2 divides $(p-1)!+1$, see [2], [18, p. 346], and [27]. It is conjectured that the set of Wilson primes is infinite, see [2]. Let $\mathcal{Z}_7 \subseteq \mathcal{V}_7$ be the system of equations in Figure 10.

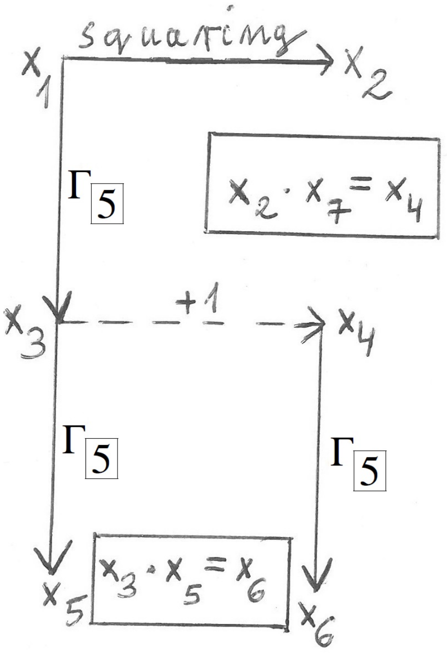

Fig. 10 Construction of the system $\mathcal{Z}_7$

Lemma 29. *For every positive integer x_1, the system $\mathcal{Z}_7$ is solvable in positive integers $x_2,\ldots,x_7$ if and only if x_1 is a Wilson prime prime and $x_1 \geqslant 17$. In this case, positive integers $x_2,\ldots,x_7$ are uniquely determined by x_1.*

Proof. It follows from Lemmas 6 and 28. □

Lemma 30. *([2], [18, p. 346], [27]).* 563 *is a Wilson prime.*

Lemma 31. $\Gamma_{\boxed{5}}(\Gamma_{\boxed{5}}(563) + 1) > (255! - 1)!$.

Theorem 22. *The statement Ξ_7 implies the infinitude of Wilson primes.*

Proof. It follows from Lemmas 29–31. □

Let $\widehat{\Xi_7}$ denote the following statement: if a system of equations

$$\mathcal{S} \subseteq \{\Gamma_{\boxed{6}}(x_i) = x_k : \ i,k \in \{1,\ldots,7\}\} \cup \{x_i \cdot x_j = x_k : \ i,j,k \in \{1,\ldots,7\}\}$$

has only finitely many solutions in positive integers $x_1,\ldots,x_7$, then each such solution $(x_1,\ldots,x_7)$ satisfies $x_1,\ldots,x_7 \leqslant (256^2 - 1)!$.

Theorem 23. *The statement $\widehat{\Xi_7}$ implies the infinitude of Wilson primes.*

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

12 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 [10, 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 [10, p. 1].

Open Problem 2. *([10, 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 [9, p. 23].

Theorem 24. *([29]). An unproven inequality stated in [29] implies that $2^{2^n} + 1$ is composite for every integer $n \geqslant 5$.*

Let

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

Lemma 32. *The following subsystem of H_n*

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

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 Γ_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 Γ_n says that for subsystems of H_n the largest known solution is indeed the largest possible.

Hypothesis 7. *The statements $\Gamma_1,\ldots,\Gamma_{13}$ are true.*

The truth of the statement $\forall n \in \mathbb{N} \setminus \{0\}\ \Gamma_n$ is doubtful because a computable upper bound on non-negative integer solutions does not exist for exponential Diophantine equations with a finite number of solutions, see [12, p. 300].

Theorem 25. *Every statement Γ_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 26. *The statement Γ_{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

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

in positive integers. By Lemma 5, we can transform equation (2) 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 11.

$$\begin{tikzcd}
x \arrow[d, "2^{2^{(\cdot)}}"] & x+1 \arrow[d, "2^{2^{(\cdot)}}"] \arrow[ddr, no head, "\texttt{multiplying}"] & & y+1 \arrow[d, "2^{2^{(\cdot)}}"] \arrow[ddl, no head] & y \arrow[d, "2^{2^{(\cdot)}}"] \\
2^{2^x} \arrow[r, "\texttt{squaring}"] & 2^{2^{x+1}} & & 2^{2^{y+1}} & 2^{2^y} \arrow[l, "\texttt{squaring}"'] \\
z \arrow[r, "2^{2^{(\cdot)}}"] & 2^{2^z} \arrow[d, "2^{2^{(\cdot)}}"] & 2^{2^z}+1 \arrow[d, "2^{2^{(\cdot)}}"] & & \\
 & 2^{2^{2^z}} \arrow[r, "\texttt{squaring}"] & 2^{2^{2^z}+1} & &
\end{tikzcd}$$

Fig. 11 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 Γ_{13} implies that the system $\mathcal{G}$ has infinitely many solutions in positive integers. It means that there are infinitely many composite Fermat numbers. □

13 Subsets of $\mathbb{N}$ whose infinitude is unconditionally equivalent to the halting of a Turing machine

The following lemma is known as Richert's lemma.

Lemma 33. *([6], [19], [21, p. 152]). Let $\{m_i\}_{i=1}^{\infty}$ be an increasing sequence of positive integers such that for some positive integer k the inequality $m_{i+1} \leqslant 2m_i$ holds for all $i > k$. Suppose there exists a non-negative integer b such that the numbers $b+1$, $b+2$, $b+3$, $\ldots$, $b+m_{k+1}$ are all expressible as sums of one or more distinct elements of the set $\{m_1, \ldots, m_k\}$. Then every integer greater than b is expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$.*

Let $\mathcal{T}$ denote the set of all positive integers i such that every integer $j \geqslant i$ is expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$. Obviously, $\mathcal{T} = \emptyset$ or $\mathcal{T} = [d, \infty) \cap \mathbb{N}$ for some positive integer d.

Corollary 2. *If the sequence $\{m_i\}_{i=1}^{\infty}$ is computable and the algorithm in Figure 12 terminates, then almost all positive integers are expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$. In particular, if the sequence $\{m_i\}_{i=1}^{\infty}$ is computable and the algorithm in Figure 12 terminates, then the set $\mathcal{T}$ is infinite. In this case, the algorithm is Figure 12 prints all positive integers which are not expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$.*

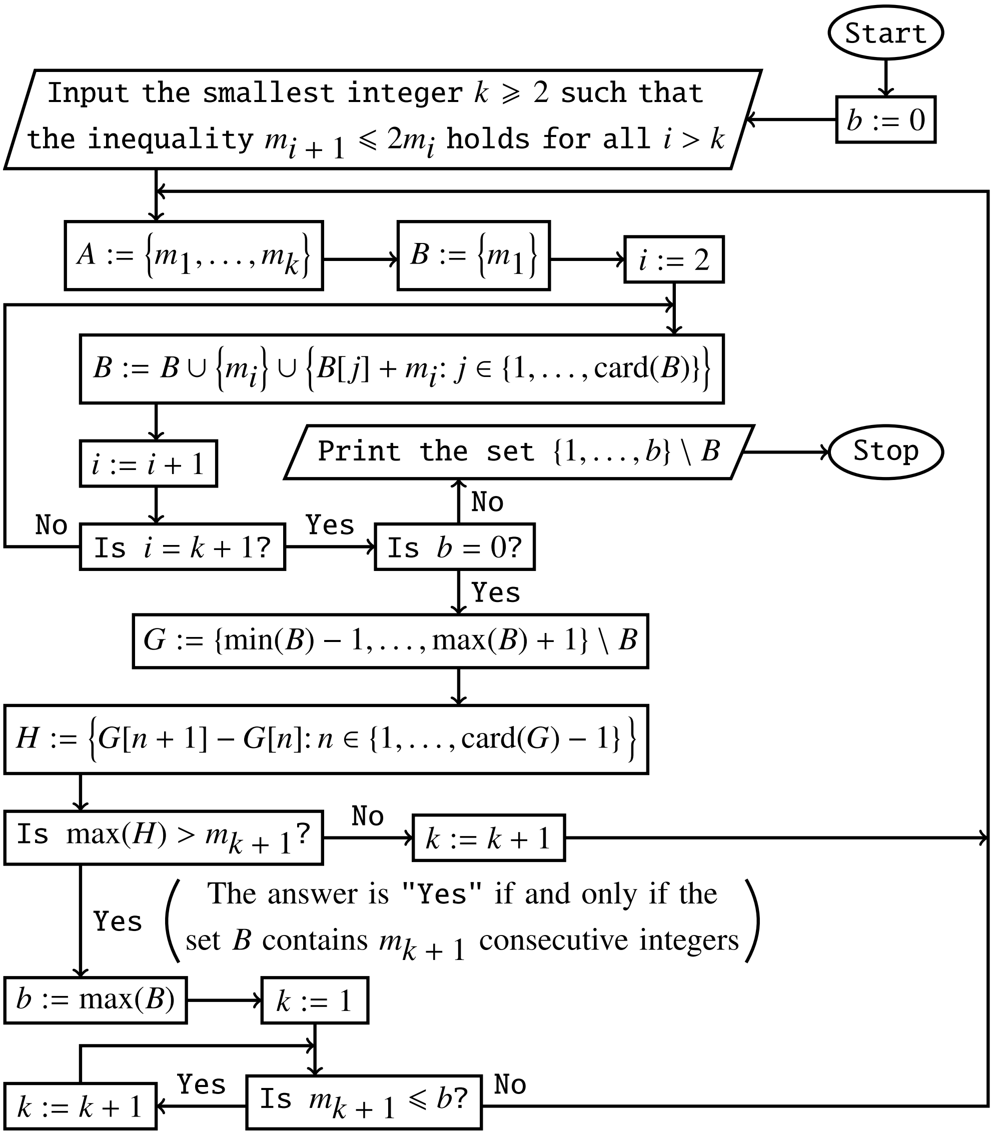
Start
$b := 0$
Input the smallest integer $k \geqslant 2$ such that the inequality $m_{i+1} \leqslant 2m_i$ holds for all $i > k$
$A := \{m_1, \ldots, m_k\}$
$B := \{m_1\}$
$i := 2$
$B := B \cup \{m_i\} \cup \{B[j] + m_i \colon j \in \{1, \ldots, \text{card}(B)\}\}$
$i := i + 1$
Print the set $\{1, \ldots, b\} \setminus B$
Stop
No
Is $i = k + 1$?
Yes
Is $b = 0$?
No
Yes
$G := \{\min(B) - 1, \ldots, \max(B) + 1\} \setminus B$
$H := \{G[n+1] - G[n] \colon n \in \{1, \ldots, \text{card}(G) - 1\}\}$
Is $\max(H) > m_{k+1}$?
No
$k := k + 1$
Yes
The answer is "Yes" if and only if the set B contains m_{k+1} consecutive integers
$b := \max(B)$
$k := 1$
$k := k + 1$
Yes
Is $m_{k+1} \leqslant b$?
No

Fig. 12 The algorithm which uses Richert's lemma

Theorem 27. *([8, Theorem 2.3]). If there exists $\varepsilon > 0$ such that the inequality $m_{i+1} \leqslant (2 - \varepsilon) \cdot m_i$ holds for every sufficiently large i, then the algorithm in Figure 12 terminates if and only if almost all positive integers are expressible as a sum of one or more distinct elements of the set $\{m_1, m_2, m_3, \ldots\}$.*

Corollary 3. *If there exists $\varepsilon > 0$ such that the inequality $m_{i+1} \leqslant (2 - \varepsilon) \cdot m_i$ holds for every sufficiently large i, then the algorithm in Figure 12 terminates if and only if the set $\mathcal{T}$ is infinite.*

We show how the algorithm in Figure 12 works for a concrete sequence $\{m_i\}_{i=1}^{\infty}$. Let $[\cdot]$ denote the integer part function. For a positive integer i, let $t_i = \dfrac{(i+19)^{i+19}}{(i+19)! \cdot 2^{i+19}}$, and let $m_i = [t_i]$.

Lemma 34. *The inequality $m_{i+1} \leqslant 2m_i$ holds for every positive integer i.*

Proof. For every positive integer i,

$$\frac{m_i}{m_{i+1}} = \frac{[t_i]}{[t_{i+1}]} > \frac{t_i - 1}{t_{i+1}} = \frac{t_i}{t_{i+1}} - \frac{1}{t_{i+1}} \geqslant \frac{t_i}{t_{i+1}} - \frac{1}{t_2} =$$

$$2 \cdot \frac{i+20}{i+19} \cdot \left(1 - \frac{1}{i+20}\right)^{i+20} - \frac{21! \cdot 2^{21}}{21^{21}} > 2 \cdot \left(1 - \frac{1}{21}\right)^{21} - \frac{21! \cdot 2^{21}}{21^{21}} = \frac{408715852844271520448512000 0}{5842587018385982521381124421}$$

The last fraction was computed by *MuPAD* and is greater than $\frac{1}{2}$. □

Theorem 28. *The algorithm in Figure 12 terminates for the sequence $\{m_i\}_{i=1}^{\infty}$.*

Proof. By Lemma 34, we take $k = 2$ as the initial value of k. The following *MuPAD* code

```
k:=2:
repeat
A:={floor((i+19)^(i+19)/((i+19)!*2^(i+19))) $i=1..k+1}:
B:={A[1]}:
for i from 2 to nops(A)-1 do
B:=B union {A[i]} union {B[j]+A[i] $j=1..nops(B)}:
end_for:
G:={y $y=B[1]-1..B[nops(B)]+1} minus B:
H:={G[n+1]-G[n] $n=1..nops(G)-1}:
k:=k+1:
until H[nops(H)]>A[nops(A)] end_repeat:
b:=B[nops(B)]:
k:=1:
while floor((k+20)^(k+20)/((k+20)!*2^(k+20)))<=b do
k:=k+1:
end_while:
A:={floor((i+19)^(i+19)/((i+19)!*2^(i+19))) $i=1..k}:
B:={A[1]}:
for i from 2 to nops(A)-1 do
B:=B union {A[i]} union {B[j]+A[i] $j=1..nops(B)}:
end_for:
print({n $n=1..b} minus B):
```

implements the algorithm in Figure 12 because *MuPAD* automatically orders every finite set of integers and the inequality `H[nops(H)]>A[nops(A)]` holds true if and only if the set B contains m_{k+1} consecutive integers. The code returns the following output:

```
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,

   21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38,

   39, 40, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 55, 56, 57, 58,

   59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 73, 74, 75, 76, 77,

   78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 97,

   98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111,

   112, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 127,
129, 130, 131, 132, 133, 134, 135, 136, 138, 139, 140, 141, 142, 143,
144, 145, 146, 147, 148, 149, 151, 152, 153, 154, 155, 156, 157, 158,
159, 160, 161, 162, 163, 164, 165, 166, 171, 172, 173, 174, 175, 176,
177, 178, 179, 180, 181, 183, 184, 185, 186, 187, 188, 189, 190, 192,
193, 194, 195, 196, 197, 198, 199, 201, 202, 203, 204, 205, 206, 207,
208, 210, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 225, 226,
228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 243,
244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 255, 256, 257, 258,
259, 260, 261, 262, 264, 267, 269, 270, 271, 272, 273, 274, 275, 276,
277, 279, 280, 282, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293,
294, 297, 300, 301, 302, 304, 305, 306, 308, 309, 310, 311, 312, 313,
314, 315, 316, 317, 318, 321, 324, 325, 326, 327, 328, 329, 330, 331,
332, 333, 334, 335, 336, 341, 342, 343, 345, 346, 347, 348, 349, 351,
354, 356, 358, 359, 360, 362, 363, 365, 366, 367, 368, 369, 371, 372,
373, 374, 376, 378, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389,
390, 400, 401, 402, 403, 405, 406, 407, 408, 410, 412, 413, 414, 415,
417, 419, 420, 421, 422, 423, 425, 426, 428, 430, 432, 434, 437, 439,
441, 442, 443, 444, 446, 447, 452, 454, 455, 456, 457, 459, 460, 461,
462, 463, 464, 467, 474, 475, 477, 478, 479, 480, 482, 483, 484, 486,
487, 488, 491, 495, 496, 497, 498, 501, 502, 504, 506, 508, 509, 511,
513, 515, 516, 518, 519, 521, 524, 528, 529, 531, 533, 535, 536, 537,
538, 539, 542, 543, 548, 549, 550, 551, 552, 553, 555, 556, 558, 559,
560, 562, 563, 567, 570, 575, 576, 578, 580, 582, 583, 585, 587, 589,
590, 591, 592, 593, 596, 600, 603, 605, 607, 608, 609, 611, 614, 616,
617, 624, 629, 630, 632, 633, 634, 637, 639, 644, 647, 648, 649, 650,
652, 654, 657, 659, 661, 663, 665, 671, 674, 676, 678, 679, 681, 683,
684, 686, 688, 689, 691, 701, 704, 705, 706, 713, 715, 717, 718, 719,

720, 725, 728, 729, 732, 733, 735, 737, 745, 746, 750, 755, 758, 760,

766, 770, 773, 775, 777, 778, 780, 785, 786, 787, 789, 790, 791, 804,

807, 809, 811, 812, 814, 816, 819, 824, 827, 829, 830, 832, 834, 841,

845, 846, 851, 856, 858, 861, 865, 866, 871, 881, 883, 886, 887, 888,

899, 902, 903, 905, 906, 908, 912, 920, 925, 928, 940, 942, 943, 947,

952, 953, 955, 957, 959, 960, 962, 974, 977, 979, 982, 984, 986, 994,

997, 999, 1004, 1015, 1028, 1031, 1035, 1036, 1048, 1049, 1051, 1053,

1056, 1058, 1069, 1073, 1076, 1078, 1080, 1082, 1088, 1089, 1090, 1093,

1095, 1107, 1110, 1122, 1123, 1127, 1129, 1130, 1132, 1147, 1152, 1154,

1164, 1169, 1174, 1179, 1184, 1201, 1205, 1206, 1218, 1219, 1223, 1224,

1226, 1228, 1246, 1250, 1255, 1257, 1258, 1259, 1260, 1275, 1277, 1280,

1298, 1300, 1302, 1307, 1315, 1322, 1329, 1331, 1346, 1351, 1352, 1354,

1356, 1372, 1374, 1376, 1381, 1383, 1385, 1387, 1396, 1398, 1403, 1405,

1426, 1427, 1428, 1450, 1457, 1468, 1472, 1477, 1482, 1497, 1499, 1526,

1529, 1533, 1549, 1551, 1573, 1580, 1583, 1603, 1605, 1610, 1625, 1627,

1647, 1667, 1679, 1681, 1699, 1701, 1721, 1753, 1773, 1775, 1780, 1795,

1817, 1832, 1849, 1852, 1869, 1871, 1886, 1923, 1925, 1943, 1945, 1950,

1997, 2022, 2039, 2073, 2120, 2174, 2221, 2246, 2297, 2369, 2416, 2591,

2761}
```

□

Corollary 4. $\mathcal{T} = [2762, \infty) \cap \mathbb{N}$.

MuPAD is a general-purpose computer algebra system. *MuPAD* is no longer available as a stand-alone computer program, but only as the *Symbolic Math Toolbox* of *MATLAB*. Fortunately, the presented code can be executed by *MuPAD Light*, which was offered for free for research and education until autumn 2005.

14 A hypothetical infinitude of various classes of primes via computer programs which halt for at most finitely many positive integers on the input

Let $\mathrm{fact}^{-1}\colon \{1,2,6,24,\ldots\} \to \mathbb{N} \setminus \{0\}$ denote the inverse function to the factorial function. For positive integers x and y, let $\mathrm{rem}(x,y)$ denote the remainder from dividing x by y.

Definition. *For a positive integer n, by a program of length n we understand any sequence of terms $x_1,\ldots,x_n$ such that x_1 is defined as the variable x, and for every integer $i \in \{2,\ldots,n\}$, x_i is defined as $\Gamma(x_{i-1})$, or* $\mathrm{fact}^{-1}(x_{i-1})$, *or* $\mathrm{rem}(x_{i-1},x_{i-2})$ *– but only if $i \geqslant 3$ and x_{i-1} is defined as* $\Gamma(x_{i-2})$.

Let $\delta(4)=3$, and let $\delta(n+1)=\delta(n)!$ for every integer $n \geqslant 4$. For an integer $n \geqslant 4$, let Ω_n denote the following statement: if a program of length n returns positive integers $x_1,\ldots,x_n$ for at most finitely many positive integers x, then every such x does not exceed $\delta(n)$.

Theorem 29. *(cf. Theorem 5). For every integer $n \geqslant 4$, the statement Ω_n is true with an unknown integer bound that depends on n.*

Proof. For every positive integer n, there are only finitely many programs of length n. □

Lemma 35. *([21, pp. 214–215]) . For every positive integer x,* $\mathrm{rem}(\Gamma(x),x) \in \mathbb{N} \setminus \{0\}$ *if and only if $x \in \{4\} \cup \mathcal{P}$.*

Theorem 30. *For every integer $n \geqslant 4$ and for every positive integer x, the following program $\mathcal{H}_n$*

$$\left\{\begin{array}{rcl} x_1 & := & x \\ \forall i \in \{2,\ldots,n-3\}\; x_i & := & \mathrm{fact}^{-1}(x_{i-1}) \\ x_{n-2} & := & \Gamma(x_{n-3}) \\ x_{n-1} & := & \Gamma(x_{n-2}) \\ x_n & := & \mathrm{rem}(x_{n-1},x_{n-2}) \end{array}\right.$$

returns positive integers $x_1,\ldots,x_n$ if and only if $x=\delta(n)$.

Proof. We make three observations.

Observation 4. *If $x_{n-3}=3$, then $x_1,\ldots,x_{n-3} \in \mathbb{N} \setminus \{0\}$ and $x=x_1=\delta(n)$.*
If $x=\delta(n)$, then $x_1,\ldots,x_{n-3} \in \mathbb{N} \setminus \{0\}$ and $x_{n-3}=3$.
Hence, $x_{n-2}=\Gamma(x_{n-3})=2$ and $x_{n-1}=\Gamma(x_{n-2})=1$. Therefore, $x_n=$ $\mathrm{rem}(x_{n-1},x_{n-2})=1$.

Observation 5. *If $x_{n-3}=2$, then $x=x_1=\ldots=x_{n-3}=2$.*
If $x=2$, then $x_1=\ldots=x_{n-3}=2$. Hence, $x_{n-2}=\Gamma(x_{n-3})=1$ and $x_{n-1}=\Gamma(x_{n-2})=1$.
Therefore, $x_n=$ $\mathrm{rem}(x_{n-1},x_{n-2})=0 \notin \mathbb{N} \setminus \{0\}$.

Observation 6. *If $x_{n-3}=1$, then $x_{n-2}=\Gamma(x_{n-3})=1$. Hence, $x_{n-1}=\Gamma(x_{n-2})=1$.*
Therefore, $x_n=$ $\mathrm{rem}(x_{n-1},x_{n-2})=0 \notin \mathbb{N} \setminus \{0\}$.

Observations 4–6 cover the case when $x_{n-3} \in \{1,2,3\}$. If $x_{n-3} \geqslant 4$, then $x_{n-2}=\Gamma(x_{n-3})$ is greater than 4 and composite. By Lemma 35, $x_n=\mathrm{rem}(x_{n-1},x_{n-2})=\mathrm{rem}(\Gamma(x_{n-2}),x_{n-2})=0 \notin \mathbb{N} \setminus \{0\}$. □

Corollary 5. *For every integer $n \geqslant 4$, the bound $\delta(n)$ in the statement Ω_n cannot be decreased.*

Lemma 36. *If $x \in \mathcal{P}$, then* $\mathrm{rem}(\Gamma(x),x)=x-1$.

Proof. It follows from Lemma 6. □

Lemma 37. *For every positive integer x, the following program $\mathcal{A}$*

$$\left\{\begin{array}{rcl} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \mathrm{rem}(x_2,x_1) \\ x_4 & := & \mathrm{fact}^{-1}(x_3) \end{array}\right.$$

returns positive integers $x_1,\ldots,x_4$ if and only if $x=4$ or x is a prime number of the form $n!+1$.

Proof. For an integer $i \in \{1, \dots, 4\}$, let A_i denote the set of positive integers x such that the first i instructions of the program $\mathcal{A}$ returns positive integers $x_1, \dots, x_i$. We show that

$$A_4 = \{4\} \cup \{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P} \tag{4}$$

For every positive integer x, the terms x_1 and x_2 belong to $\mathbb{N} \setminus \{0\}$. By Lemma 35, the term x_3 (which equals $\mathrm{rem}(\Gamma(x), x)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \{4\} \cup \mathcal{P}$. Hence, $A_3 = \{4\} \cup \mathcal{P}$. If $x = 4$, then $x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\}$. Hence, $4 \in A_4$. If $x \in \mathcal{P}$, then Lemma 36 implies that $x_3 = \mathrm{rem}(\Gamma(x), x) = x - 1 \in \mathbb{N} \setminus \{0\}$. Therefore, for every $x \in \mathcal{P}$, the term $x_4 = \mathrm{fact}^{-1}(x_3)$ belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\}$. This proves equality (4). □

Theorem 31. *The statement Ω_4 implies that the set of primes of the form $n! + 1$ is infinite.*

Proof. The number $3! + 1 = 7$ is prime. By Lemma 37, for $x = 7$ the program $\mathcal{A}$ returns positive integers $x_1, \dots, x_4$. Since $x = 7 > 3 = \delta(4)$, the statement Ω_4 guarantees that the program $\mathcal{A}$ returns positive integers $x_1, \dots, x_4$ for infinitely many positive integers x. By Lemma 37, there are infinitely many primes of the form $n! + 1$. □

Lemma 38. *If $x \in \mathbb{N} \setminus \{0, 1\}$, then* $\mathrm{fact}^{-1}(\Gamma(x)) = x - 1$.

Theorem 32. *If the set of primes of the form $n! + 1$ is infinite, then the statement Ω_4 is true.*

Proof. There exist exactly 10 programs of length 4 that differ from $\mathcal{H}_4$ and $\mathcal{A}$, see Figure 13. For every such program $\mathcal{F}_i$, we determine the set S_i of all positive integers x such that the program $\mathcal{F}_i$ outputs positive integers $x_1, \dots, x_4$ on input x. We omit 10 easy proofs which use Lemmas 35 and 38. The sets S_i are infinite, see Figure 13.

$\mathcal{F}_1$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \Gamma(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \mathbb{N} \setminus \{0\} = S_1$
$\mathcal{F}_2$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \mathrm{fact}^{-1}(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \mathbb{N} \setminus \{0\} = S_2$
$\mathcal{H}_4$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \mathrm{rem}(x_3, x_2)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x = 3$
$\mathcal{F}_3$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \mathrm{fact}^{-1}(x_2)$	$x_4 := \Gamma(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \mathbb{N} \setminus \{0\} = S_3$
$\mathcal{F}_4$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \mathrm{fact}^{-1}(x_2)$	$x_4 := \mathrm{fact}^{-1}(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{1\} \cup \{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\} = S_4$
$\mathcal{F}_5$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \mathrm{rem}(x_2, x_1)$	$x_4 := \Gamma(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{4\} \cup \mathcal{P} = S_5$
$\mathcal{A}$	$x_1 := x$	$x_2 := \Gamma(x_1)$	$x_3 := \mathrm{rem}(x_2, x_1)$	$x_4 := \mathrm{fact}^{-1}(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{4\} \cup \{n! + 1 :\ n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P}$
$\mathcal{F}_6$	$x_1 := x$	$x_2 := \mathrm{fact}^{-1}(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \Gamma(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{n! : n \in \mathbb{N} \setminus \{0\}\} = S_6$
$\mathcal{F}_7$	$x_1 := x$	$x_2 := \mathrm{fact}^{-1}(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \mathrm{fact}^{-1}(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{n! : n \in \mathbb{N} \setminus \{0\}\} = S_7$
$\mathcal{F}_8$	$x_1 := x$	$x_2 := \mathrm{fact}^{-1}(x_1)$	$x_3 := \Gamma(x_2)$	$x_4 := \mathrm{rem}(x_3, x_2)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{4!\} \cup \{p! :\ p \in \mathcal{P}\} = S_8$
$\mathcal{F}_9$	$x_1 := x$	$x_2 := \mathrm{fact}^{-1}(x_1)$	$x_3 := \mathrm{fact}^{-1}(x_2)$	$x_4 := \Gamma(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{(n!)! :\ n \in \mathbb{N} \setminus \{0\}\} = S_9$
$\mathcal{F}_{10}$	$x_1 := x$	$x_2 := \mathrm{fact}^{-1}(x_1)$	$x_3 := \mathrm{fact}^{-1}(x_2)$	$x_4 := \mathrm{fact}^{-1}(x_3)$	$x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\} \Longleftrightarrow$ $x \in \{((n!)!)! :\ n \in \mathbb{N} \setminus \{0\}\} = S_{10}$

Fig. 13 12 programs of length 4, $x \in \mathbb{N} \setminus \{0\}$

This completes the proof. □

Hypothesis 8. *The statements $\Omega_4, \dots, \Omega_7$ are true.*

Lemma 39. *For every positive integer x, the following program $\mathcal{B}$*

$$\left\{\begin{array}{lcl} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \mathrm{rem}(x_2, x_1) \\ x_4 & := & \mathrm{fact}^{-1}(x_3) \\ x_5 & := & \Gamma(x_4) \\ x_6 & := & \mathrm{rem}(x_5, x_4) \end{array}\right.$$

returns positive integers $x_1, \ldots, x_6$ if and only if $x \in \{4\} \cup \{p! + 1 : \ p \in \mathcal{P}\} \cap \mathcal{P}$

Proof. For an integer $i \in \{1, \ldots, 6\}$, let B_i denote the set of positive integers x such that the first i instructions of the program $\mathcal{B}$ returns positive integers $x_1, \ldots, x_i$. Since the programs $\mathcal{A}$ and $\mathcal{B}$ have the same first four instructions, the equality $B_i = A_i$ holds for every $i \in \{1, \ldots, 4\}$. In particular,

$$B_4 = \{4\} \cup \{n! + 1 : \ n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P}$$

We show that

$$B_6 = \{4\} \cup \{p! + 1 : \ p \in \mathcal{P}\} \cap \mathcal{P} \tag{5}$$

If $x = 4$, then $x_1, \ldots, x_6 \in \mathbb{N} \setminus \{0\}$. Hence, $4 \in B_6$. Let $x \in \mathcal{P}$, and let $x = n! + 1$, where $n \in \mathbb{N} \setminus \{0\}$. Hence, $n \neq 4$. Lemma 36 implies that $x_3 = \mathrm{rem}(\Gamma(x), x) = x - 1 = n!$. Hence, $x_4 = \mathrm{fact}^{-1}(x_3) = n$ and $x_5 = \Gamma(x_4) = \Gamma(n) \in \mathbb{N} \setminus \{0\}$. By Lemma 35, the term x_6 (which equals $\mathrm{rem}(\Gamma(n), n)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $n \in \{4\} \cup \mathcal{P}$. This proves equality (5) as $n \neq 4$. □

Theorem 33. *The statement Ω_6 implies that for infinitely many primes p the number $p! + 1$ is prime.*

Proof. The numbers 11 and $11! + 1$ are prime, see [3, p. 441] and [25]. By Lemma 39, for $x = 11! + 1$ the program $\mathcal{B}$ returns positive integers $x_1, \ldots, x_6$. Since $x = 11! + 1 > 6! = \delta(6)$, the statement Ω_6 guarantees that the program $\mathcal{B}$ returns positive integers $x_1, \ldots, x_6$ for infinitely many positive integers x. By Lemma 39, for infinitely many primes p the number $p! + 1$ is prime. □

Lemma 40. *For every positive integer x, the following program C*

$$\left\{\begin{array}{lcl} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \Gamma(x_2) \\ x_4 & := & \mathrm{fact}^{-1}(x_3) \\ x_5 & := & \Gamma(x_4) \\ x_6 & := & \mathrm{rem}(x_5, x_4) \end{array}\right.$$

returns positive integers $x_1, \ldots, x_6$ if and only if $(x - 1)! - 1$ is prime.

Proof. For an integer $i \in \{1, \ldots, 6\}$, let C_i denote the set of positive integers x such that the first i instructions of the program C returns positive integers $x_1, \ldots, x_i$. If $x \in \{1, 2, 3\}$, then $x_6 = 0$. Therefore, $C_6 \subseteq \mathbb{N} \setminus \{0, 1, 2, 3\}$. By Lemma 38, for every integer $x \geqslant 4$, $x_4 = (x - 1)! - 1$, $x_5 = \Gamma((x - 1)! - 1)$, and $x_1, \ldots, x_5 \in \mathbb{N} \setminus \{0\}$. By Lemma 35, for every integer $x \geqslant 4$,

$$x_6 = \mathrm{rem}(\Gamma((x - 1)! - 1), (x - 1)! - 1)$$

belongs to $\mathbb{N} \setminus \{0\}$ if and only if $(x - 1)! - 1 \in \{4\} \cup \mathcal{P}$. The last condition equivalently expresses that $(x - 1)! - 1$ is prime as $(x - 1)! - 1 \geqslant 5$ for every integer $x \geqslant 4$. Hence,

$$C_6 = (\mathbb{N} \setminus \{0, 1, 2, 3\}) \cap \{x \in \mathbb{N} \setminus \{0, 1, 2, 3\} : \ (x - 1)! - 1 \in \mathcal{P}\} = \{x \in \mathbb{N} \setminus \{0\} : \ (x - 1)! - 1 \in \mathcal{P}\}$$

□

It is conjectured that there are infinitely many primes of the form $n! - 1$, see [3, p. 443] and [24].

Theorem 34. *The statement Ω_6 implies that there are infinitely many primes of the form $x! - 1$.*

Proof. The number $(975 - 1)! - 1$ is prime, see [3, p. 441] and [24]. By Lemma 40, for $x = 975$ the program C returns positive integers $x_1, \ldots, x_6$. Since $x = 975 > 720 = \delta(6)$, the statement Ω_6 guarantees that the program C returns positive integers $x_1, \ldots, x_6$ for infinitely many positive integers x. By Lemma 40, the set $\{x \in \mathbb{N} \setminus \{0\} : (x-1)! - 1 \in \mathcal{P}\}$ is infinite. □

Lemma 41. *For every positive integer x, the following program $\mathcal{D}$*

$$\begin{cases} x_1 & := & x \\ x_2 & := & \Gamma(x_1) \\ x_3 & := & \mathrm{rem}(x_2, x_1) \\ x_4 & := & \Gamma(x_3) \\ x_5 & := & \mathrm{fact}^{-1}(x_4) \\ x_6 & := & \Gamma(x_5) \\ x_7 & := & \mathrm{rem}(x_6, x_5) \end{cases}$$

returns positive integers $x_1, \ldots, x_7$ if and only if both x and $x - 2$ are prime.

Proof. For an integer $i \in \{1, \ldots, 7\}$, let D_i denote the set of positive integers x such that the first i instructions of the program $\mathcal{D}$ returns positive integers $x_1, \ldots, x_i$. If $x = 1$, then $x_3 = 0$. Hence, $D_7 \subseteq D_3 \subseteq \mathbb{N} \setminus \{0, 1\}$. If $x \in \{2, 3, 4\}$, then $x_7 = 0$. Therefore,

$$D_7 \subseteq (\mathbb{N} \setminus \{0, 1\}) \cap (\mathbb{N} \setminus \{0, 2, 3, 4\}) = \mathbb{N} \setminus \{0, 1, 2, 3, 4\}$$

By Lemma 35, for every integer $x \geqslant 5$, the term x_3 (which equals $\mathrm{rem}(\Gamma(x), x)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x \in \mathcal{P} \setminus \{2, 3\}$. By Lemma 36, for every $x \in \mathcal{P} \setminus \{2, 3\}$, $x_3 = x - 1 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$. By Lemma 38, for every $x \in \mathcal{P} \setminus \{2, 3\}$, the terms x_4 and x_5 belong to $\mathbb{N} \setminus \{0\}$ and $x_5 = x_3 - 1 = x - 2$. By Lemma 35, for every $x \in \mathcal{P} \setminus \{2, 3\}$, the term x_7 (which equals $\mathrm{rem}(\Gamma(x_5), x_5)$) belongs to $\mathbb{N} \setminus \{0\}$ if and only if $x_5 = x - 2 \in \{4\} \cup \mathcal{P}$. From these facts, we obtain that

$$D_7 = (\mathbb{N} \setminus \{0, 1, 2, 3, 4\}) \cap (\mathcal{P} \setminus \{2, 3\}) \cap (\{6\} \cup \{p + 2 : p \in \mathcal{P}\}) = \{p \in \mathcal{P} : p - 2 \in \mathcal{P}\}$$

□

Theorem 35. *The statement Ω_7 implies that there are infinitely many twin primes.*

Proof. Harvey Dubner proved that the numbers $459 \cdot 2^{8529} - 1$ and $459 \cdot 2^{8529} + 1$ are prime, see [34, p. 87]. By Lemma 41, for $x = 459 \cdot 2^{8529} + 1$ the program $\mathcal{D}$ returns positive integers $x_1, \ldots, x_7$. Since $x > 720! = \delta(7)$, the statement Ω_7 guarantees that the program $\mathcal{D}$ returns positive integers $x_1, \ldots, x_7$ for infinitely many positive integers x. By Lemma 41, there are infinitely many twin primes. □

We can transform every program of length n into a computer program with n instructions which for every $x \in \mathbb{N} \setminus \{0\}$ does the same if $(x_1, \ldots, x_n) \in (\mathbb{N} \setminus \{0\})^n$, and never halts if $(x_1, \ldots, x_n) \notin (\mathbb{N} \setminus \{0\})^n$ or the tuple $(x_1, \ldots, x_n)$ is undefined. To do so, we perform the following steps:

a) We replace the instruction $x_1 := x$ by the following instruction:

$$x_1 := x \;\&\; \mathtt{PRINT}(x_1)$$

b) We replace every instruction of the form $x_i = \Gamma(x_{i-1})$ by the following instruction:

$$x_i := \Gamma(x_{i-1}) \;\&\; \mathtt{PRINT}(x_i)$$

c) We replace every instruction of the form $x_i := \mathrm{fact}^{-1}(x_{i-1})$ by the following instruction:

$$\mathtt{IF}\ \mathrm{fact}^{-1}(x_{i-1}) \in \mathbb{N} \setminus \{0\}\ \mathtt{THEN}\ x_i := \mathrm{fact}^{-1}(x_{i-1}) \;\&\; \mathtt{PRINT}(x_i)\ \mathtt{ELSE\ GOTO\ Instruction\ 1}$$

d) We replace every instruction of the form $x_i := \mathrm{rem}(x_{i-1}, x_{i-2})$ by the following instruction:

$$\mathtt{IF}\ \mathrm{rem}(x_{i-1}, x_{i-2}) \in \mathbb{N} \setminus \{0\}\ \mathtt{THEN}\ x_i := \mathrm{rem}(x_{i-1}, x_{i-2}) \;\&\; \mathtt{PRINT}(x_i)\ \mathtt{ELSE\ GOTO\ Instruction\ 1}$$

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, *The Prime Glossary: Wilson prime,* `http://primes.utm.edu/glossary/xpage/WilsonPrime.html`.

[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] 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.

[5] M. Davis, Yu. Matiyasevich, J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution;* in: Mathematical developments arising from Hilbert problems (ed. F. E. Browder), Proc. Sympos. Pure Math., vol. 28, Part 2, Amer. Math. Soc., Providence, RI, 1976, 323–378, `http://dx.doi.org/10.1090/pspum/028.2`; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., Providence, RI, 1996, 269–324.

[6] R. E. Dressler, A. Mąkowski, T. Parker,, *Sums of distinct primes from congruence classes modulo* 12, Math. Comp. 28 (1974), 651–652.

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

[8] T. Kløve, *Sums of distinct elements from a fixed set,* Math. Comp. 29 (1975), 1144–1149.

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

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

[11] 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

[12] Yu. Matiyasevich, *Existence of noneffectivizable estimates in the theory of exponential Diophantine equations,* J. Sov. Math. vol. 8, no. 3, 1977, 299–311, `http://dx.doi.org/10.1007/bf01091549`.

[13] Yu. Matiyasevich, *Hilbert's tenth problem,* MIT Press, Cambridge, MA, 1993.

[14] Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done;* in: Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 1–47, Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000, `http://dx.doi.org/10.1090/conm/270`.

[15] Yu. Matiyasevich, *Towards finite-fold Diophantine representations,* J. Math. Sci. (N. Y.) vol. 171, no. 6, 2010, 745–752, `http://dx.doi.org/10.1007%2Fs10958-010-0179-4`.

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

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

[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] H.-E. Richert, *Über Zerlegungen in paarweise verschiedene Zahlen,* Norsk Mat. Tidsskr. 31 (1949), 120–122.

[20] J. Robinson, *Definability and decision problems in arithmetic,* J. Symbolic Logic 14 (1949), no. 2, 98–114, `http://dx.doi.org/10.2307/2266510`; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., Providence, RI, 1996, 7–23

[21] W. Sierpiński, *Elementary theory of numbers,* 2nd ed. (ed. A. Schinzel), PWN – Polish Scientific Publishers and North-Holland, Warsaw-Amsterdam, 1987.

[22] Th. Skolem, *Diophantische Gleichungen*, Julius Springer, Berlin, 1938.

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

[24] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002982, Numbers n such that* $n! - 1$ *is prime,* `http://oeis.org/A002982`.

[25] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A093804, Primes p such that* $p! + 1$ *is also prime,* `http://oeis.org/A093804`.

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

[27] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A007540, Wilson primes: primes p such that* $(p-1)! \equiv -1 \pmod{p^2}$, `http://oeis.org/A007540`.

[28] A. Tyszka, *Conjecturally computable functions which unconditionally do not have any finite-fold Diophantine representation,* Inform. Process. Lett. 113 (2013), no. 19–21, 719–722, `http://dx.doi.org/10.1016/j.ipl.2013.07.004`.

[29] A. Tyszka, *Is there a computable upper bound for the height of a solution of a Diophantine equation with a unique solution in positive integers?,* Open Comput. Sci. 7 (2017), no. 1, 17–23, `http://doi.org/10.1515/comp-2017-0003`.

[30] A. Tyszka, *A hypothetical upper bound on the heights of the solutions of a Diophantine equation with a finite number of solutions,* Open Comput. Sci. 8 (2018), no. 1, 109–114, `http://dx.doi.org/10.1515/comp-2018-0012`.

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

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

[33] A. R. Woods, *Some problems in logic and number theory, and their connections,* Ph.D. thesis, University of Manchester, Manchester, 1981, `http://staffhome.ecm.uwa.edu.au/~00017049/thesis/WoodsPhDThesis.pdf`; reprinted in: *New studies in weak arithmetics* (eds. P. Cégielski, C. Cornaros, C. Dimitracopoulos), CSLI Lecture Notes, vol. 211, 271–388, CSLI Publ., Stanford, CA, 2013.

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

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 116B, 30-149 Kraków, Poland
E-mail: `rttyszka@cyf-kr.edu.pl`