

# On sets $\mathcal{W} \subseteq \mathbb{N}$ such that the infinity of $\mathcal{W}$ is equivalent to the existence in $\mathcal{W}$ of an element that is greater than a threshold number computed with using the definition of $\mathcal{W}$

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

**Abstract**—Let  $f(1) = 2$ ,  $f(2) = 4$ , and let  $f(n+1) = f(n)!$  for every integer  $n \geq 2$ . For a positive integer  $n$ , let  $\Theta_n$  denote the statement: if a system  $\mathcal{S} \subseteq \{x_i! = x_k : i, k \in \{1, \dots, n\}\} \cup \{x_i \cdot x_j = x_k : i, j, k \in \{1, \dots, n\}\}$  has only finitely many solutions in integers  $x_1, \dots, x_n$  greater than 1, then each such solution  $(x_1, \dots, x_n)$  satisfies  $\min(x_1, \dots, x_n) \leq f(n)$ . The statement  $\Theta_9$  proves that if there exists an integer  $x > f(9)$  such that  $x^2 + 1$  (alternatively,  $x! + 1$ ) is prime, then there are infinitely many primes of the form  $n^2 + 1$  (respectively,  $n! + 1$ ). The statement  $\Theta_{16}$  proves that if there exists a twin prime greater than  $f(16) + 3$ , then there are infinitely many twin primes. We formulate the statements  $\Phi_n$  and prove:  $\Phi_4$  equivalently expresses that there are infinitely many primes of the form  $n! + 1$ ,  $\Phi_6$  implies that for infinitely many primes  $p$  the number  $p! + 1$  is prime,  $\Phi_6$  implies that there are infinitely many primes of the form  $n! - 1$ ,  $\Phi_7$  implies that there are infinitely many twin primes.

**Index Terms**—composite Fermat numbers, prime numbers of the form  $n! + 1$ , prime numbers of the form  $n! - 1$ , prime numbers of the form  $n^2 + 1$ , prime numbers  $p$  such that  $p! + 1$  is prime, single query to an oracle for the halting problem, twin prime conjecture.

## I. SPECTRA OF SENTENCES AND THEIR THRESHOLD NUMBERS

**T**HE following observation concerns the theme described in the title of the article.

**Observation 1.** If  $\mathcal{W}$  is a subset of  $\{0, \dots, n\}$  where  $n$  is a non-negative integer, then we take any integer  $m \geq n$  as a threshold number for  $\mathcal{W}$ . If  $\mathcal{W}$  is an infinite subset of  $\mathbb{N}$ , then we take any non-negative integer  $m$  as a threshold number for  $\mathcal{W}$ .

We define the set  $\mathcal{U} \subseteq \mathbb{N}$  by declaring that a non-negative integer  $n$  belongs to  $\mathcal{U}$  if and only if  $\sin\left(10^{10^{10^{10}}}\right) > 0$ . This inequality is practically undecidable, see [4].

**Corollary 1.** The set  $\mathcal{U}$  equals  $\emptyset$  or  $\mathbb{N}$ . The statement “ $\mathcal{U} = \emptyset$ ” remains unproven and the statement “ $\mathcal{U} = \mathbb{N}$ ” remains unproven. Every non-negative integer  $m$  is a threshold number for  $\mathcal{U}$ . For every non-negative integer  $k$ , the sentence “ $k \in \mathcal{U}$ ” is only theoretically decidable.

The first-order language of graph theory contains two relation symbols of arity 2:  $\sim$  and  $=$ , respectively for adjacency and equality of vertices. The term first-order imposes the condition that the variables represent vertices and hence the quantifiers apply to vertices only. For a first-order sentence  $\Lambda$  about graphs, let  $\text{Spectrum}(\Lambda)$  denote the set of all positive integers  $n$  such that there is a graph on  $n$  vertices satisfying  $\Lambda$ .

**Theorem 1.** ([10, p. 171]). If a sentence  $\Lambda$  in the language of graph theory has the form  $\exists x_1 \dots x_k \forall y_1 \dots y_l \Upsilon(x_1, \dots, x_k, y_1, \dots, y_l)$ , where  $\Upsilon(x_1, \dots, x_k, y_1, \dots, y_l)$  is quantifier-free, then either  $\text{Spectrum}(\Lambda) \subseteq [1, (2^k \cdot 4^l) - 1]$  or  $\text{Spectrum}(\Lambda) \supseteq [k + l, \infty) \cap \mathbb{N}$ .

**Corollary 2.** The number  $(2^k \cdot 4^l) - 1$  is a threshold number for  $\text{Spectrum}(\Lambda)$ .

The classes of the infinite recursively enumerable sets and of the infinite recursive sets are not recursively enumerable, see [8, p. 234].

**Corollary 3.** If an algorithm  $\text{Alg}_1$  for every recursive set  $\mathcal{W} \subseteq \mathbb{N}$  finds a non-negative integer  $\text{Alg}_1(\mathcal{W})$ , then there exists a finite set  $\mathcal{M} \subseteq \mathbb{N}$  such that  $\mathcal{M} \cap [\text{Alg}_1(\mathcal{M}) + 1, \infty) \neq \emptyset$ .

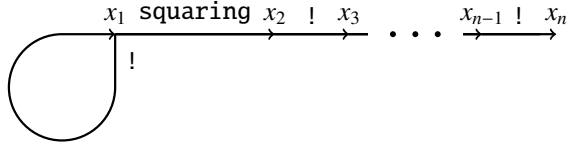
**Corollary 4.** If an algorithm  $\text{Alg}_2$  for every recursively enumerable set  $\mathcal{W} \subseteq \mathbb{N}$  finds a non-negative integer  $\text{Alg}_2(\mathcal{W})$ , then there exists a finite set  $\mathcal{M} \subseteq \mathbb{N}$  such that  $\mathcal{M} \cap [\text{Alg}_2(\mathcal{M}) + 1, \infty) \neq \emptyset$ .

## II. BASIC LEMMAS

Let  $f(1) = 2$ ,  $f(2) = 4$ , and let  $f(n+1) = f(n)!$  for every integer  $n \geq 2$ . Let  $\mathcal{V}_1$  denote the system of equations  $\{x_1! = x_1\}$ , and let  $\mathcal{V}_2$  denote the system of equations  $\{x_1! = x_1, x_1 \cdot x_1 = x_2\}$ . For an integer  $n \geq 3$ , let  $\mathcal{V}_n$  denote the following system of equations:

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

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



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

**Lemma 1.** For every positive integer  $n$ , the system  $\mathcal{V}_n$  has exactly one solution in integers greater than 1, namely  $(f(1), \dots, f(n))$ .

Let

$$H_n = \{x_i! = x_k : i, k \in \{1, \dots, n\}\} \cup$$

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

For a positive integer  $n$ , let  $\Theta_n$  denote the following statement: if a system  $\mathcal{S} \subseteq H_n$  has at most finitely many solutions in integers  $x_1, \dots, x_n$  greater than 1, then each such solution  $(x_1, \dots, x_n)$  satisfies  $\min(x_1, \dots, x_n) \leq f(n)$ . The assumption  $\min(x_1, \dots, x_n) \leq f(n)$  is weaker than the assumption  $\max(x_1, \dots, x_n) \leq f(n)$  suggested by Lemma 1.

**Lemma 2.** For every positive integer  $n$ , the system  $H_n$  has a finite number of subsystems.

**Theorem 2.** Every statement  $\Theta_n$  is true with an unknown integer bound that depends on  $n$ .

*Proof.* It follows from Lemma 2.  $\square$

**Lemma 3.** For every integers  $x$  and  $y$  greater than 1,  $x! \cdot y = y!$  if and only if  $x + 1 = y$ .

**Lemma 4.** If  $x \geq 4$ , then  $\frac{(x-1)! + 1}{x} > 1$ .

**Lemma 5.** (Wilson's theorem, [3, p. 89]). For every integer  $x \geq 2$ ,  $x$  is prime if and only if  $x$  divides  $(x-1)! + 1$ .

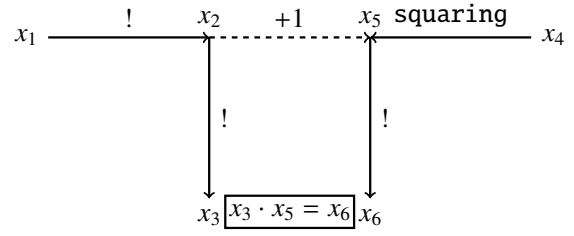
### III. BROCARD'S PROBLEM

A weak form of Szpiro's conjecture implies that there are only finitely many solutions to the Brocard-Ramanujan equation  $x! + 1 = y^2$ , see [9]. It is conjectured that  $x! + 1$  is a square only for  $x \in \{4, 5, 7\}$ , see [16, p. 297].

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



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

**Lemma 6.** For every integers  $x_1$  and  $x_4$  greater than 1, the system  $\mathcal{A}$  is solvable in integers  $x_2, x_3, x_5, x_6$  greater than 1 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:

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

and  $x_1 = \min(x_1, \dots, x_6)$ .

*Proof.* It follows from Lemma 3.  $\square$

**Theorem 3.** The statement  $\Theta_6$  proves the following implication: if the equation  $x_1! + 1 = x_4^2$  has only finitely many solutions in positive integers, then each such solution  $(x_1, x_4)$  satisfies  $x_1 \leq f(6)$ .

*Proof.* 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 6, there exists a unique tuple  $(x_2, x_3, x_5, x_6) \in (\mathbb{N} \setminus \{0, 1\})^4$  such that the tuple  $(x_1, \dots, x_6)$  solves the system  $\mathcal{A}$ . Lemma 6 guarantees that  $x_1 = \min(x_1, \dots, x_6)$ . By the antecedent and Lemma 6, the system  $\mathcal{A}$  has only finitely many solutions in integers  $x_1, \dots, x_6$  greater than 1. Therefore, the statement  $\Theta_6$  implies that  $x_1 = \min(x_1, \dots, x_6) \leq f(6)$ .  $\square$

**Hypothesis 1.** The implication in Theorem 3 is true.

**Corollary 5.** Assuming Hypothesis 1, a single query to an oracle for the halting problem decides the problem of the infinitude of the solutions of the equation  $x! + 1 = y^2$ .

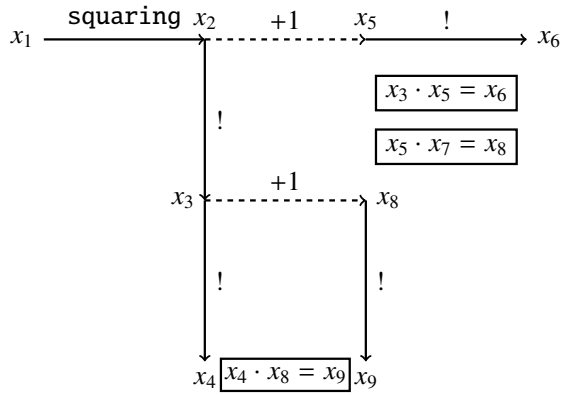
### IV. ARE THERE INFINITELY MANY PRIME NUMBERS OF THE FORM $n^2 + 1$ ?

Landau's conjecture states that there are infinitely many primes of the form  $n^2 + 1$ , see [7, pp. 37–38].

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

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

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



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

**Lemma 7.** For every integer  $x_1 \geq 2$ , the system  $\mathcal{B}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 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:

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

and  $\min(x_1, \dots, x_9) = x_1$ .

*Proof.* By Lemmas 3 and 4, for every integer  $x_1 \geq 2$ , the system  $\mathcal{B}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 if and only if  $x_1^2 + 1$  divides  $(x_1^2)! + 1$ . Hence, the claim of Lemma 7 follows from Lemma 5.  $\square$

**Theorem 4.** The statement  $\Theta_9$  proves the following implication: if there exists an integer  $x_1 > f(9)$  such that  $x_1^2 + 1$  is prime, then there are infinitely many primes of the form  $n^2 + 1$ .

*Proof.* Assume that an integer  $x_1$  is greater than  $f(9)$  and  $x_1^2 + 1$  is prime. By Lemma 7, there exists a unique tuple  $(x_2, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^8$  such that the tuple  $(x_1, x_2, \dots, x_9)$  solves the system  $\mathcal{B}$ . Lemma 7 guarantees that  $\min(x_1, \dots, x_9) = x_1$ . Since  $\mathcal{B} \subseteq H_9$ , the statement  $\Theta_9$  and the inequality  $\min(x_1, \dots, x_9) = x_1 > f(9)$  imply that the system  $\mathcal{B}$  has infinitely many solutions  $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9$ . According to Lemma 7, there are infinitely many primes of the form  $n^2 + 1$ .  $\square$

**Hypothesis 2.** The implication in Theorem 4 is true.

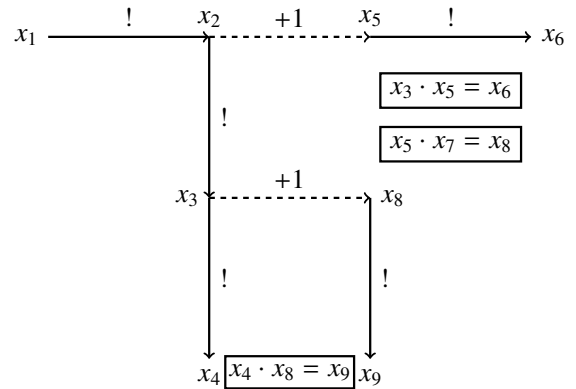
**Corollary 6.** Assuming Hypothesis 2, a single query to an oracle for the halting problem decides the problem of the infinitude of primes of the form  $n^2 + 1$ .

## V. 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 [1, p. 443] and [12]. Let  $\mathcal{G}$  denote the following system of equations:

$$\left\{ \begin{array}{l} x_1! = x_2 \\ x_2! = x_3 \\ x_3! = x_4 \\ x_5! = x_6 \\ x_8! = x_9 \\ x_3 \cdot x_5 = x_6 \\ x_4 \cdot x_8 = x_9 \\ x_5 \cdot x_7 = x_8 \end{array} \right.$$

Lemma 3 and the diagram in Figure 4 explain the construction of the system  $\mathcal{G}$ .



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

**Lemma 8.** For every integer  $x_1 \geq 2$ , the system  $\mathcal{G}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 if and only if  $x_1! + 1$  is prime. In this case, the integers  $x_2, \dots, x_9$  are uniquely determined by the following equalities:

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

and  $\min(x_1, \dots, x_9) = x_1$ .

*Proof.* By Lemmas 3 and 4, for every integer  $x_1 \geq 2$ , the system  $\mathcal{G}$  is solvable in integers  $x_2, \dots, x_9$  greater than 1 if and only if  $x_1! + 1$  divides  $(x_1!)! + 1$ . Hence, the claim of Lemma 8 follows from Lemma 5.  $\square$

**Theorem 5.** The statement  $\Theta_9$  proves the following implication: if there exists an integer  $x_1 > f(9)$  such that  $x_1! + 1$  is prime, then there are infinitely many primes of the form  $n! + 1$ .

*Proof.* Assume that an integer  $x_1$  is greater than  $f(9)$  and  $x_1! + 1$  is prime. By Lemma 8, there exists a

unique tuple  $(x_2, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^8$  such that the tuple  $(x_1, x_2, \dots, x_9)$  solves the system  $\mathcal{G}$ . Lemma 8 guarantees that  $\min(x_1, \dots, x_9) = x_1$ . Since  $\mathcal{G} \subseteq H_9$ , the statement  $\Theta_9$  and the inequality  $\min(x_1, \dots, x_9) = x_1 > f(9)$  imply that the system  $\mathcal{G}$  has infinitely many solutions  $(x_1, \dots, x_9) \in (\mathbb{N} \setminus \{0, 1\})^9$ . According to Lemma 8, there are infinitely many primes of the form  $n! + 1$ .  $\square$

**Hypothesis 3.** *The implication in Theorem 5 is true.*

**Corollary 7.** *Assuming Hypothesis 3, a single query to an oracle for the halting problem decides the problem of the infinitude of primes of the form  $n! + 1$ .*

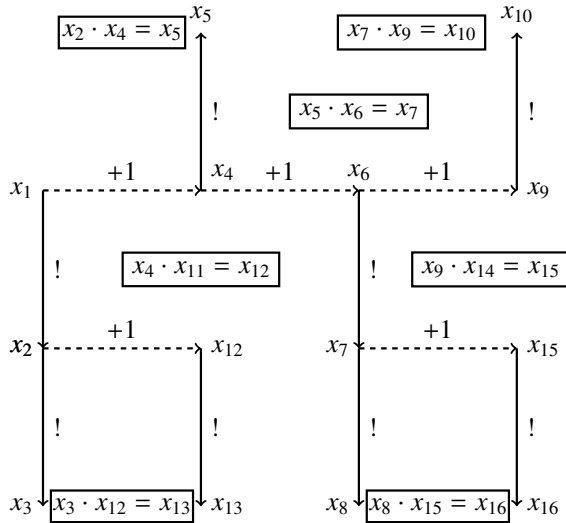
## VI. THE TWIN PRIME CONJECTURE

A twin prime is a prime number that is either 2 less or 2 more than another prime number. The twin prime conjecture states that there are infinitely many twin primes, see [7, p. 39].

Let  $C$  denote the following system of equations:

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

Lemma 3 and the diagram in Figure 5 explain the construction of the system  $C$ .



**Fig. 5** Construction of the system  $C$

**Lemma 9.** *If  $x_4 = 2$ , then the system  $C$  has no solutions in integers  $x_1, \dots, x_{16}$  greater than 1.*

*Proof.* The equality  $x_2 \cdot x_4 = x_5 = x_4!$  and the equality  $x_4 = 2$  imply that  $x_2 = 1$ .  $\square$

**Lemma 10.** *If  $x_4 = 3$ , then the system  $C$  has no solutions in integers  $x_1, \dots, x_{16}$  greater than 1.*

*Proof.* The equality  $x_4 \cdot x_{11} = x_{12} = (x_4 - 1)! + 1$  and the equality  $x_4 = 3$  imply that  $x_{11} = 1$ .  $\square$

**Lemma 11.** *For every  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$  and for every  $x_9 \in \mathbb{N} \setminus \{0, 1\}$ , the system  $C$  is solvable in integers  $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$  greater than 1 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:*

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

and  $\min(x_1, \dots, x_{16}) = x_1 = x_9 - 3$ .

*Proof.* By Lemmas 3 and 4, for every  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$  and for every  $x_9 \in \mathbb{N} \setminus \{0, 1\}$ , the system  $C$  is solvable in integers  $x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}$  greater than 1 if and only if

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

Hence, the claim of Lemma 11 follows from Lemma 5.  $\square$

**Theorem 6.** *The statement  $\Theta_{16}$  proves the following implication: if there exists a twin prime greater than  $f(16) + 3$ , then there are infinitely many twin primes.*

*Proof.* Assume the antecedent holds. Then, there exist prime numbers  $x_4$  and  $x_9$  such that  $x_9 = x_4 + 2 > f(16) + 3$ . Hence,  $x_4 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$ . By Lemma 11, there exists a unique tuple  $(x_1, x_2, x_3, x_5, x_6, x_7, x_8, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}) \in (\mathbb{N} \setminus \{0, 1\})^{14}$  such that the tuple  $(x_1, \dots, x_{16})$  solves the system  $C$ . Lemma 11 guarantees that  $\min(x_1, \dots, x_{16}) = x_1 = x_9 - 3 > f(16)$ . Since  $C \subseteq H_{16}$ , the statement  $\Theta_{16}$  and the inequality  $\min(x_1, \dots, x_{16}) > f(16)$  imply that the system  $C$  has infinitely many solutions in integers  $x_1, \dots, x_{16}$  greater than 1. According to Lemmas 9–11, there are infinitely many twin primes.  $\square$

**Hypothesis 4.** *The implication in Theorem 6 is true.*

**Corollary 8.** (cf. [2]). *Assuming Hypothesis 4, a single query to an oracle for the halting problem decides the twin prime problem.*

VII. ARE THERE INFINITELY MANY COMPOSITE 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  $n \geq 5$ , see [5, p. 23].

**Lemma 12.** ([6, p. 38]). *For every positive integer  $n$ , if a prime number  $p$  divides  $2^{2^n} + 1$ , then there exists a positive integer  $k$  such that  $p = k \cdot 2^{n+1} + 1$ .*

**Corollary 9.** *Since  $k \cdot 2^{n+1} + 1 \geq 2^{n+1} + 1 \geq n+3$ , for every positive integers  $x, y$ , and  $n$ , the equality  $(x+1)(y+1) = 2^{2^n} + 1$  implies that  $\min(n, x, x+1, y, y+1) = n$ .*

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

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

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

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

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

For a positive integer  $n$ , let  $\Psi_n$  denote the following statement: if a system  $S \subseteq G_n$  has at most finitely many solutions in positive integers  $x_1, \dots, x_n$ , then each such solution  $(x_1, \dots, x_n)$  satisfies  $\min(x_1, \dots, x_n) \leq g(n)$ . The assumption  $\min(x_1, \dots, x_n) \leq g(n)$  is weaker than the assumption  $\max(x_1, \dots, x_n) \leq g(n)$  suggested by Lemma 13.

**Lemma 14.** *For every positive integer  $n$ , the system  $G_n$  has a finite number of subsystems.*

**Theorem 7.** *Every statement  $\Psi_n$  is true with an unknown integer bound that depends on  $n$ .*

*Proof.* It follows from Lemma 14.  $\square$

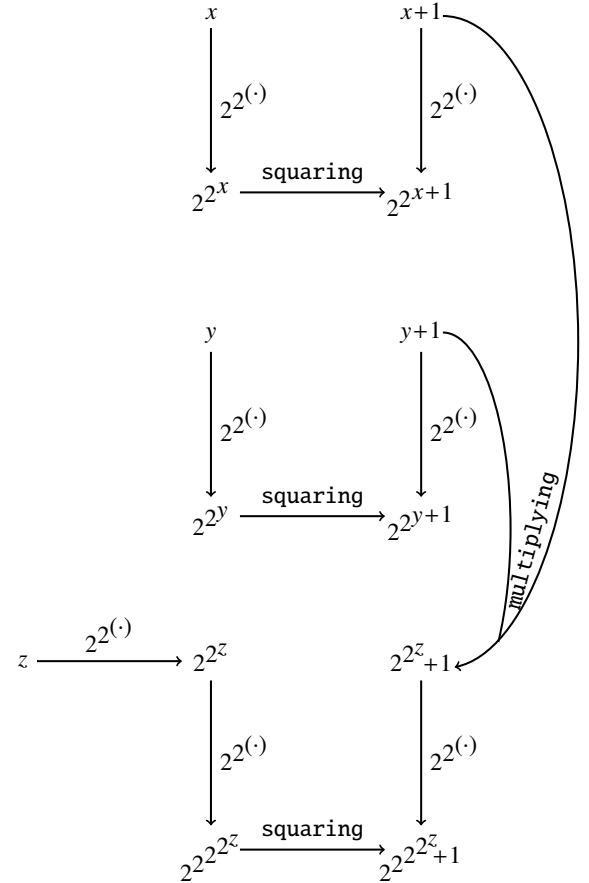
**Lemma 15.** *For every non-negative integers  $b$  and  $c$ ,  $b+1 = c$  if and only if  $2^{2^b} \cdot 2^{2^b} = 2^{2^c}$ .*

**Theorem 8.** *The statement  $\Psi_{13}$  proves the following implication: if  $2^{2^n} + 1$  is composite for some integer  $n > g(13)$ , then  $2^{2^n} + 1$  is composite for infinitely many positive integers  $n$ .*

*Proof.* Let us consider the equation

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

in positive integers. By Lemma 15, we can transform equation (1) into an equivalent system  $\mathcal{F}$  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 6.



**Fig. 6** Construction of the system  $\mathcal{F}$

Assume that  $2^{2^n} + 1$  is composite for some integer  $n > g(13)$ . By this and Corollary 9, equation (1) has a solution  $(x, y, z) \in (\mathbb{N} \setminus \{0\})^3$  such that  $z = n$  and  $z = \min(z, x, x+1, y, y+1)$ . Hence, the system  $\mathcal{F}$  has a solution in positive integers such that  $z = n$  and  $n$  is the smallest number in the solution sequence. Since  $n > g(13)$ , the statement  $\Psi_{13}$  implies that the system  $\mathcal{F}$  has infinitely many solutions in positive integers. Therefore, there are infinitely many positive integers  $n$  such that  $2^{2^n} + 1$  is composite.  $\square$

**Hypothesis 5.** *The implication in Theorem 8 is true.*

**Corollary 10.** *Assuming Hypothesis 5, a single query to an oracle for the halting problem decides whether or not the set of composite Fermat numbers is infinite.*

### VIII. COMPUTATIONS OF LENGTH $n$ AND THE STATEMENTS $\Phi_n$

For a positive integer  $x$ , let  $\Gamma(x)$  denote  $(x-1)!$ . Let  $\text{fact}^{-1}: \{1, 2, 6, 24, \dots\} \rightarrow \mathbb{N} \setminus \{0\}$  denote the inverse function to the factorial function. For positive integers  $x$  and  $y$ , let  $\text{rem}(x, y)$  denote the remainder from dividing  $x$  by  $y$ .

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

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

**Lemma 16.** ([11, pp. 214–215]). *For every positive integer  $x$ ,  $\text{rem}(\Gamma(x), x) \in \mathbb{N} \setminus \{0\}$  if and only if  $x \in \{4\} \cup \mathcal{P}$ .*

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

**Theorem 9.** *For every integer  $n \geq 4$  and for every positive integer  $x$ , the following computation  $\mathcal{H}_n$*

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

*returns positive integers  $x_1, \dots, x_n$  if and only if  $x = h(n)$ .*

*Proof.* We make three observations.

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

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

**Observation 4.** *If  $x_{n-3} = 1$ , then  $x_{n-2} = \Gamma(x_{n-3}) = 1$ . Hence,  $x_{n-1} = \Gamma(x_{n-2}) = 1$ . Therefore,  $x_n = \text{rem}(x_{n-1}, x_{n-2}) = 0 \notin \mathbb{N} \setminus \{0\}$ .*

Observations 2–4 cover the case when  $x_{n-3} \in \{1, 2, 3\}$ . If  $x_{n-3} \geq 4$ , then  $x_{n-2} = \Gamma(x_{n-3})$  is greater than 4 and composite. By Lemma 16,  $x_n = \text{rem}(x_{n-1}, x_{n-2}) = \text{rem}(\Gamma(x_{n-2}), x_{n-2}) = 0 \notin \mathbb{N} \setminus \{0\}$ .  $\square$

For an integer  $n \geq 4$ , let  $\Phi_n$  denote the following statement: if a computation of length  $n$  returns positive integers  $x_1, \dots, x_n$  for at most finitely many positive integers  $x$ , then every such  $x$  does not exceed  $h(n)$ .

**Theorem 10.** *For every integer  $n \geq 4$ , the bound  $h(n)$  in the statement  $\Phi_n$  cannot be decreased.*

*Proof.* It follows from Theorem 9.  $\square$

**Lemma 17.** *For every positive integer  $n$ , there are only finitely many computations of length  $n$ .*

**Theorem 11.** *For every integer  $n \geq 4$ , the statement  $\Phi_n$  is true with an unknown integer bound that depends on  $n$ .*

*Proof.* It follows from Lemma 17.  $\square$

### IX. CONSEQUENCES OF THE STATEMENTS $\Phi_4, \dots, \Phi_7$

**Lemma 18.** *If  $x \in \mathcal{P}$ , then  $\text{rem}(\Gamma(x), x) = x - 1$ .*

*Proof.* It follows from Lemma 5.  $\square$

**Lemma 19.** *For every positive integer  $x$ , the following computation  $\mathcal{T}$*

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

*returns positive integers  $x_1, \dots, x_4$  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  $T_i$  denote the set of positive integers  $x$  such that the first  $i$  instructions of the computation  $\mathcal{T}$  returns positive integers  $x_1, \dots, x_i$ . We show that

$$T_4 = \{4\} \cup (\{n! + 1 : n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P}) \quad (2)$$

For every positive integer  $x$ , the terms  $x_1$  and  $x_2$  belong to  $\mathbb{N} \setminus \{0\}$ . By Lemma 16, the term  $x_3$  (which equals  $\text{rem}(\Gamma(x), x)$ ) belongs to  $\mathbb{N} \setminus \{0\}$  if and only if  $x \in \{4\} \cup \mathcal{P}$ . Hence,  $T_3 = \{4\} \cup \mathcal{P}$ . If  $x = 4$ , then  $x_1, \dots, x_4 \in \mathbb{N} \setminus \{0\}$ . Hence,  $4 \in T_4$ . If  $x \in \mathcal{P}$ , then Lemma 18 implies that  $x_3 = \text{rem}(\Gamma(x), x) = x - 1 \in \mathbb{N} \setminus \{0\}$ . Therefore, for every  $x \in \mathcal{P}$ , the term  $x_4 = \text{fact}^{-1}(x_3)$  belongs to  $\mathbb{N} \setminus \{0\}$  if and only if  $x \in \{n! + 1 : n \in \mathbb{N} \setminus \{0\}\}$ . This proves equality (2).  $\square$

**Theorem 12.** *The statement  $\Phi_4$  implies that the set of primes of the form  $n! + 1$  is infinite.*

*Proof.* The number  $3! + 1 = 7$  is prime. By Lemma 19, for  $x = 7$  the computation  $\mathcal{T}$  returns positive integers  $x_1, \dots, x_4$ . Since  $x = 7 > 3 = h(4)$ , the statement  $\Phi_4$  guarantees that the computation  $\mathcal{T}$  returns positive integers  $x_1, \dots, x_4$  for infinitely many positive integers  $x$ . By Lemma 19, there are infinitely many primes of the form  $n! + 1$ .  $\square$

**Lemma 20.** *If  $x \in \mathbb{N} \setminus \{0, 1\}$ , then  $\text{fact}^{-1}(\Gamma(x)) = x - 1$ .*

**Theorem 13.** *If the set of primes of the form  $n! + 1$  is infinite, then the statement  $\Phi_4$  is true.*

*Proof.* There exist exactly 10 computations of length 4 that differ from  $\mathcal{H}_4$  and  $\mathcal{T}$ , see Table 1. For every such computation  $\mathcal{F}_i$ , we determine the set  $S_i$  of all positive integers  $x$  such that the computation  $\mathcal{F}_i$  outputs positive integers  $x_1, \dots, x_4$  on input  $x$ . We omit 10 easy proofs which use Lemmas 16 and 20. The sets  $S_i$  are infinite, see Table 1.

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

**Tab. 1** 12 computations of length 4,  $x \in \mathbb{N} \setminus \{0\}$

This completes the proof.  $\square$

**Hypothesis 6.** The statements  $\Phi_4, \dots, \Phi_7$  are true.

**Lemma 21.** For every positive integer  $x$ , the following computation  $\mathcal{Y}$

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

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

*Proof.* For an integer  $i \in \{1, \dots, 6\}$ , let  $Y_i$  denote the set of positive integers  $x$  such that the first  $i$  instructions of the computation  $\mathcal{Y}$  returns positive integers  $x_1, \dots, x_i$ . Since the computations  $\mathcal{T}$  and  $\mathcal{Y}$  have the same first four instructions, the equality  $Y_i = T_i$  holds for every  $i \in \{1, \dots, 4\}$ . In particular,

$$Y_4 = \{4\} \cup \{n! + 1 : n \in \mathbb{N} \setminus \{0\}\} \cap \mathcal{P}$$

We show that

$$Y_6 = \{4\} \cup (\{p! + 1 : p \in \mathcal{P}\} \cap \mathcal{P}) \quad (3)$$

If  $x = 4$ , then  $x_1, \dots, x_6 \in \mathbb{N} \setminus \{0\}$ . Hence,  $4 \in Y_6$ . Let  $x \in \mathcal{P}$ , and let  $x = n! + 1$ , where  $n \in \mathbb{N} \setminus \{0\}$ . Hence,  $n \neq 4$ . Lemma 18 implies that  $x_3 = \text{rem}(\Gamma(x), x) = x - 1 = n!$ . Hence,  $x_4 = \text{fact}^{-1}(x_3) = n$  and  $x_5 = \Gamma(x_4) = \Gamma(n) \in \mathbb{N} \setminus \{0\}$ . By Lemma 16, the term  $x_6$  (which equals  $\text{rem}(\Gamma(n), n)$ ) belongs to  $\mathbb{N} \setminus \{0\}$  if and only if  $n \in \{4\} \cup \mathcal{P}$ . This proves equality (3) as  $n \neq 4$ .  $\square$

**Theorem 14.** The statement  $\Phi_6$  implies that for infinitely many primes  $p$  the number  $p! + 1$  is prime.

*Proof.* The numbers 11 and  $11! + 1$  are prime, see [1, p. 441] and [14]. By Lemma 21, for  $x = 11! + 1$  the computation  $\mathcal{Y}$  returns positive integers  $x_1, \dots, x_6$ . Since  $x = 11! + 1 > 6! = h(6)$ , the statement  $\Phi_6$  guarantees that the computation  $\mathcal{Y}$  returns positive integers  $x_1, \dots, x_6$  for infinitely many positive integers  $x$ . By Lemma 21, for infinitely many primes  $p$  the number  $p! + 1$  is prime.  $\square$

**Lemma 22.** For every positive integer  $x$ , the following computation  $\mathcal{L}$

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

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

*Proof.* For an integer  $i \in \{1, \dots, 6\}$ , let  $L_i$  denote the set of positive integers  $x$  such that the first  $i$  instructions of the computation  $\mathcal{L}$  returns positive integers  $x_1, \dots, x_i$ . If  $x \in \{1, 2, 3\}$ , then  $x_6 = 0$ . Therefore,  $L_6 \subseteq \mathbb{N} \setminus \{0, 1, 2, 3\}$ . By Lemma 20, for every integer  $x \geq 4$ ,  $x_4 = (x - 1)! - 1$ ,  $x_5 = \Gamma((x - 1)! - 1)$ , and  $x_1, \dots, x_5 \in \mathbb{N} \setminus \{0\}$ . By Lemma 16, for every integer  $x \geq 4$ ,

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

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  $(x-1)! - 1 \geq 5$  for every integer  $x \geq 4$ . Hence,

$$L_6 = (\mathbb{N} \setminus \{0, 1, 2, 3\}) \cap \{x \in \mathbb{N} \setminus \{0, 1, 2, 3\} : (x-1)! - 1 \in \mathcal{P}\} = \{x \in \mathbb{N} \setminus \{0\} : (x-1)! - 1 \in \mathcal{P}\}$$

It is conjectured that there are infinitely many primes of the form  $n! - 1$ , see [1, p. 443] and [13].

**Theorem 15.** *The statement  $\Phi_6$  implies that there are infinitely many primes of the form  $x! - 1$ .*

*Proof.* The number  $(975-1)! - 1$  is prime, see [1, p. 441] and [13]. By Lemma 22, for  $x = 975$  the computation  $\mathcal{L}$  returns positive integers  $x_1, \dots, x_6$ . Since  $x = 975 > 720 = h(6)$ , the statement  $\Phi_6$  guarantees that the computation  $\mathcal{L}$  returns positive integers  $x_1, \dots, x_6$  for infinitely many positive integers  $x$ . By Lemma 22, the set  $\{x \in \mathbb{N} \setminus \{0\} : (x-1)! - 1 \in \mathcal{P}\}$  is infinite.  $\square$

**Lemma 23.** *For every positive integer  $x$ , the following computation  $\mathcal{D}$*

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

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

*Proof.* For an integer  $i \in \{1, \dots, 7\}$ , let  $D_i$  denote the set of positive integers  $x$  such that the first  $i$  instructions of the computation  $\mathcal{D}$  returns positive integers  $x_1, \dots, x_i$ . 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 16, for every integer  $x \geq 5$ , the term  $x_3$  (which equals  $\text{rem}(\Gamma(x), x)$ ) belongs to  $\mathbb{N} \setminus \{0\}$  if and only if  $x \in \mathcal{P} \setminus \{2, 3\}$ . By Lemma 18, for every  $x \in \mathcal{P} \setminus \{2, 3\}$ ,  $x_3 = x - 1 \in \mathbb{N} \setminus \{0, 1, 2, 3\}$ . By Lemma 20, 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 16, for every  $x \in \mathcal{P} \setminus \{2, 3\}$ , the term  $x_7$  (which equals  $\text{rem}(\Gamma(x_5), x_5)$ ) 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

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

$\square$

$\square$  **Theorem 16.** *The statement  $\Phi_7$  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 [15, p. 87]. By Lemma 23, for  $x = 459 \cdot 2^{8529} + 1$  the computation  $\mathcal{D}$  returns positive integers  $x_1, \dots, x_7$ . Since  $x > 720! = h(7)$ , the statement  $\Phi_7$  guarantees that the computation  $\mathcal{D}$  returns positive integers  $x_1, \dots, x_7$  for infinitely many positive integers  $x$ . By Lemma 23, there are infinitely many twin primes.  $\square$

## REFERENCES

- [1] C. K. Caldwell and Y. Gallot, *On the primality of  $n! \pm 1$  and  $2 \times 3 \times 5 \times \dots \times p \pm 1$* , Math. Comp. 71 (2002), no. 237, 441–448, <https://doi.org/10.1090/S0025-5718-01-01315-1>.
- [2] F. G. Dorais, *Can the twin prime problem be solved with a single use of a halting oracle?* July 23, 2011, <https://mathoverflow.net/questions/71050>.
- [3] M. Erickson, A. Vazzana, D. Garth, *Introduction to number theory*, 2nd ed., CRC Press, Boca Raton, FL, 2016.
- [4] J. van der Hoeven, *Undecidability versus undecidability*, Bull. Symbolic Logic 5 (1999), no. 1, 75, <https://dx.doi.org/10.2307/421141>.
- [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] W. Narkiewicz, *Rational number theory in the 20th century: From PNT to FLT*, Springer, London, 2012.
- [8] P. Odifreddi, *Classical recursion theory: the theory of functions and sets of natural numbers*, North-Holland, Amsterdam, 1989.
- [9] M. Overholt, *The Diophantine equation  $n! + 1 = m^2$* , Bull. London Math. Soc. 25 (1993), no. 2, 104, <https://doi.org/10.1112/blms/25.2.104>.
- [10] O. Pikhurko and O. Verbitsky, *Logical complexity of graphs: a survey; in: Model theoretic methods in finite combinatorics*, Contemp. Math. 558, 129–179, Amer. Math. Soc., Providence, RI, 2011, <https://dx.doi.org/10.1090/conm/558>.
- [11] W. Sierpiński, *Elementary theory of numbers*, 2nd ed. (ed. A. Schinzel), PWN – Polish Scientific Publishers and North-Holland, Warsaw-Amsterdam, 1987.
- [12] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002981, Numbers  $n$  such that  $n! + 1$  is prime*, <https://oeis.org/A002981>.
- [13] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A002982, Numbers  $n$  such that  $n! - 1$  is prime*, <https://oeis.org/A002982>.
- [14] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, A093804, Primes  $p$  such that  $p! + 1$  is also prime*, <https://oeis.org/A093804>.
- [15] S. Y. Yan, *Number theory for computing*, 2nd ed., Springer, Berlin, 2002.
- [16] E. W. Weisstein, *CRC Concise Encyclopedia of Mathematics*, 2nd ed., Chapman & Hall/CRC, Boca Raton, FL, 2002.