On sets $\mathcal{W} \subseteq \mathbb{N} \setminus \{0\}$ for which we can compute $t(\mathcal{W}) \in \mathbb{N}$ such that any element of $\mathcal{W}$ which is greater than $t(\mathcal{W})$ proves that $\mathcal{W}$ is infinite

Apoloniusz Tyszka

Abstract

Let $f(1) = 2$, $f(2) = 4$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 2$. For a positive integer n, let Γ_n denote the statement: if a system $\mathcal{S} \subseteq \left\{x_i! = x_k:\ i,k \in \{1,\ldots,n\}\right\} \cup \left\{x_i \cdot x_j = x_k:\ i,j,k \in \{1,\ldots,n\}\right\}$ has at most finitely many solutions in integers $x_1,\ldots,x_n$ greater than 1, then each such solution $(x_1,\ldots,x_n)$ satisfies $\min(x_1,\ldots,x_n) \leqslant f(n)$. We conjecture that the statements $\Gamma_1,\ldots,\Gamma_{16}$ are true. The statement Γ_9 proves the implication: if there exists an integer $x > f(9)$ such that x^2+1 is prime, then there are infinitely many primes of the form n^2+1. The statement Γ_{16} proves the implication: if there exists a twin prime greater than $f(16)+3$, then there are infinitely many twin primes. Let $g(1) = 1$, and let $g(n+1) = 2^{2^{g(n)}}$ for every positive integer n. We formulate a conjecture which proves the 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.

Key words and phrases: composite Fermat numbers, prime numbers of the form n^2+1, proving the infinitude of a subset of positive integers, single query to an oracle for the halting problem, twin prime conjecture.

2010 Mathematics Subject Classification: 11U05.

1. Introduction and basic lemmas

In sections 1–4, we study a conjecture which provides a common approach to Brocard's problem, the problem of the infinitude of primes of the form n^2+1, and the twin prime problem. Let $f(1) = 2$, $f(2) = 4$, and let $f(n+1) = f(n)!$ for every integer $n \geqslant 2$. 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 $n \geqslant 3$, let $\mathcal{V}_n$ denote the following system of equations:

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

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

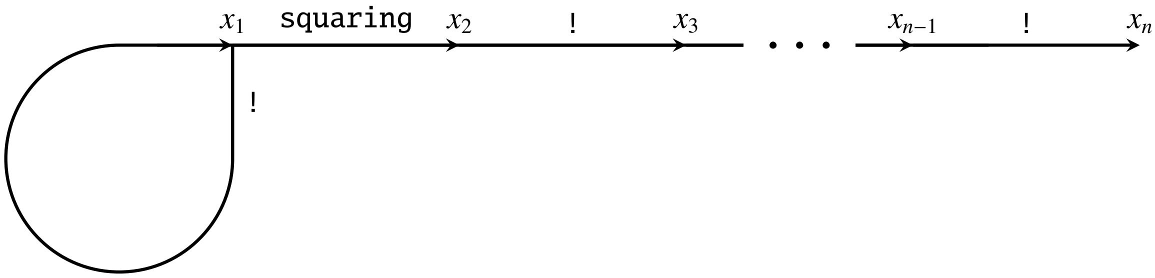

Fig. 1 Construction of the system $\mathcal{V}_n$

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

Let
$$H_n = \Big\{x_i! = x_k :\ i, k \in \{1, \ldots, n\}\Big\} \cup \Big\{x_i \cdot x_j = x_k :\ i, j, k \in \{1, \ldots, n\}\Big\}$$
For a positive integer n, let Γ_n denote the following statement: if a system $\mathcal{S} \subseteq H_n$ has at most finitely many solutions in integers $x_1, \ldots, x_n$ greater than 1, then each such solution $(x_1, \ldots, x_n)$ satisfies $\min(x_1, \ldots, x_n) \leqslant f(n)$. We conjecture that the statements $\Gamma_1, \ldots, \Gamma_{16}$ are true. For every positive integer n, the system H_n has a finite number of subsystems. Therefore, every statement Γ_n is true with an unknown integer bound that depends on n.

Lemma 2. *For every integers x and y greater than* 1*, $x! \cdot y = y!$ if and only if $x + 1 = y$.*

Lemma 3. *If $x \geqslant 4$, then* $\dfrac{(x-1)!+1}{x} > 1$.

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

2. 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 [6]. It is conjectured that $x! + 1$ is a square only for $x \in \{4, 5, 7\}$, see [7, 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 2 and the diagram in Figure 2 explain the construction of the system $\mathcal{A}$.

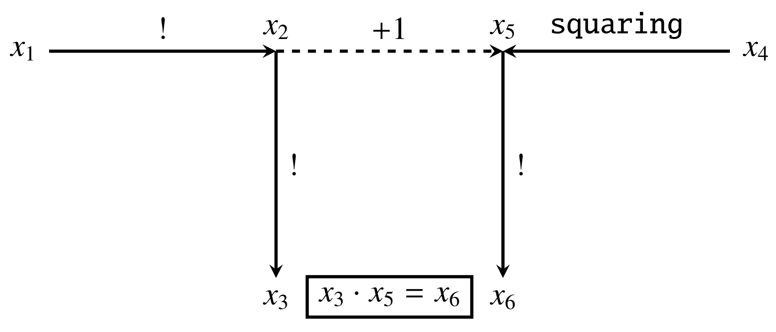

Fig. 2 Construction of the system $\mathcal{A}$

Lemma 5. *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 $x_1 = \min(x_1, \ldots, x_6)$.

Proof. It follows from Lemma 2. □

Theorem 1. *If the equation $x_1! + 1 = x_4^2$ has only finitely many solutions in positive integers, then the statement Γ_6 implies that each such solution (x_1, x_4) satisfies $x_1 \leqslant f(6)$.*

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 5, there exists a unique tuple $(x_2, x_3, x_5, x_6) \in (\mathbb{N} \setminus \{0, 1\})^4$ such that the tuple $(x_1, \ldots, x_6)$ solves the system $\mathcal{A}$. Lemma 5 guarantees that $x_1 = min(x_1, \ldots, x_6)$. By the antecedent and Lemma 5, the system $\mathcal{A}$ has only finitely many solutions in integers $x_1, \ldots, x_6$ greater than 1. Therefore, the statement Γ_6 implies that $x_1 = \min(x_1, \ldots, x_6) \leqslant f(6)$. □

3. 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 [5, pp. 37–38].

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

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

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

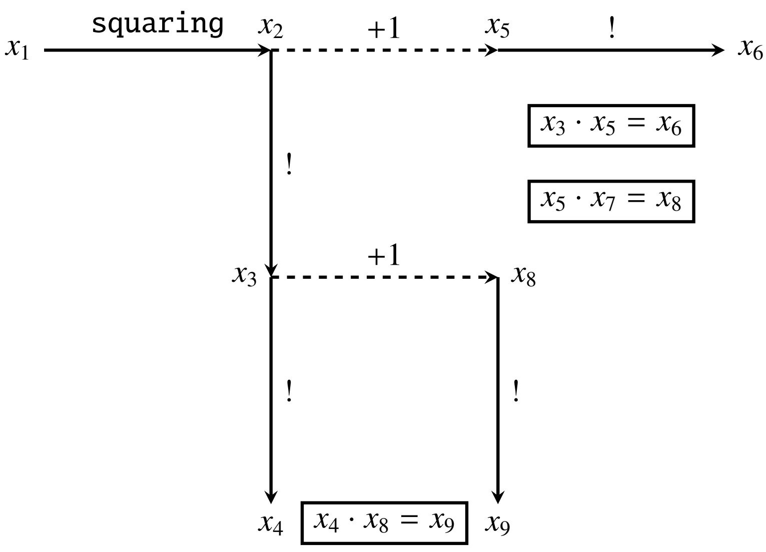

Fig. 3 Construction of the system $\mathcal{B}$

Lemma 6. *For every integer $x_1 \geqslant 2$, the system $\mathcal{B}$ is solvable in integers $x_2, \ldots, x_9$ greater than 1 if and only if $x_1^2 + 1$ is prime. In this case, the integers $x_2, \ldots, x_9$ are uniquely determined* *by the following equalities:*

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

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

Proof. By Lemmas 2 and 3, for every integer $x_1 \geqslant 2$, the system $\mathcal{B}$ is solvable in integers $x_2, \ldots, x_9$ greater than 1 if and only if x_1^2+1 divides $(x_1^2)!+1$. Hence, the claim of Lemma 6 follows from Lemma 4. □

Theorem 2. *The statement* Γ_9 *proves the 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 6, there exists a unique tuple $(x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0,1\})^8$ such that the tuple $(x_1, x_2, \ldots, x_9)$ solves the system $\mathcal{B}$. Lemma 6 guarantees that $\min(x_1, \ldots, x_9) = x_1$. Since $\mathcal{B} \subseteq H_9$, the statement Γ_9 and the inequality $\min(x_1, \ldots, x_9) = x_1 > f(9)$ imply that the system $\mathcal{B}$ has infinitely many solutions $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0,1\})^9$. According to Lemma 6, there are infinitely many primes of the form n^2+1. □

Corollary 1. *Assuming the statement* Γ_9*, a single query to an oracle for the halting problem decides the problem of the infinitude of primes of the form* n^2+1.

4. 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 [5, 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 4 explain the construction of the system C.

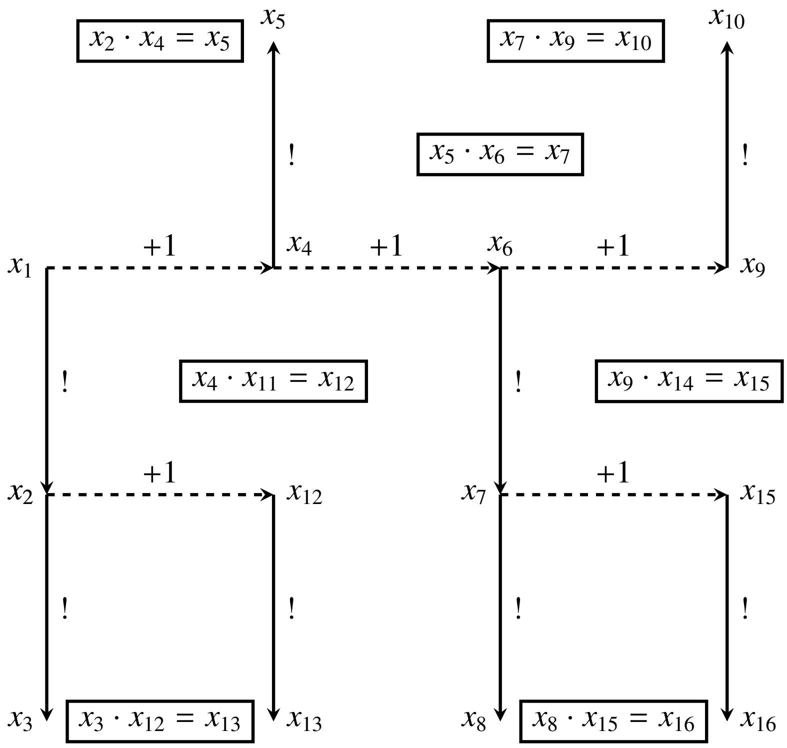

Fig. 4 Construction of the system C

Lemma 7. *If $x_4 = 2$, then the system C has no solutions in integers $x_1, \ldots, x_{16}$ greater than* 1.

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

Lemma 8. *If $x_4 = 3$, then the system C has no solutions in integers $x_1, \ldots, x_{16}$ 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 $x_{11} = 1$. □

Lemma 9. *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 $\min(x_1, \ldots, x_{16}) = x_1 = x_9 - 3$.

Proof. By Lemmas 2 and 3, 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

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

Hence, the claim of Lemma 9 follows from Lemma 4. □

Theorem 3. *The statement* Γ_{16} *proves the 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 9, 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 $(x_1, \ldots, x_{16})$ solves the system C. Lemma 9 guarantees that $\min(x_1, \ldots, x_{16}) = x_1 = x_9 - 3 > f(16)$. Since $C \subseteq H_{16}$, the statement Γ_{16} and the inequality $\min(x_1, \ldots, x_{16}) > f(16)$ imply that the system C has infinitely many solutions in integers $x_1, \ldots, x_{16}$ greater than 1. According to Lemmas 7–9, there are infinitely many twin primes. □

Corollary 2. *(cf. [1]). Assuming the statement* Γ_{16}*, a single query to an oracle for the halting problem decides the twin prime problem.*

5. 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 [4, 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 [4, p. 1].

Open Problem. ([4, 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 [3, p. 23].

Lemma 10. *([4, 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 3. *Since* $k \cdot 2^{n+1} + 1 \geqslant 2^{n+1} + 1 \geqslant n + 3$*, 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

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

The following subsystem of G_n

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

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

For a positive integer n, let Ψ_n denote the following statement: if a system $S \subseteq G_n$ has at most finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $\min(x_1, \ldots, x_n) \leqslant g(n)$. We conjecture that the statements $\Psi_1, \ldots, \Psi_{13}$ are true. For every positive integer n, the system G_n has a finite number of subsystems. Therefore, every statement Ψ_n is true with an unknown integer bound that depends on n.

Lemma 11. *For every positive integers b and c, $b + 1 = c$ if and only if $2^{2^b} \cdot 2^{2^b} = 2^{2^c}$.*

Theorem 4. *The statement Ψ_{13} proves the 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

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

in positive integers. By Lemma 11, 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 5.

$$\begin{tikzcd}
 & x \arrow[d, "2^{2^{(\cdot)}}"] & x+1 \arrow[d, "2^{2^{(\cdot)}}"] \arrow[dddd, bend left] \\
 & 2^{2^x} \arrow[r, "\texttt{squaring}"] & 2^{2^{x+1}} \\
 & y \arrow[d, "2^{2^{(\cdot)}}"] & y+1 \arrow[d, "2^{2^{(\cdot)}}"] \arrow[dd, bend left, "\texttt{multiplying}"] \\
 & 2^{2^y} \arrow[r, "\texttt{squaring}"] & 2^{2^{y+1}} \\
z \arrow[r, "2^{2^{(\cdot)}}"] & 2^{2^z} \arrow[d, "2^{2^{(\cdot)}}"] & 2^{2^z}+1 \arrow[d, "2^{2^{(\cdot)}}"] \\
 & 2^{2^{2^{2^z}}} \arrow[r, "\texttt{squaring}"] & 2^{2^{2^{2^z}+1}}
\end{tikzcd}$$

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

Assume that $2^{2^n}+1$ is composite for some integer $n > g(13)$. By this and Corollary 3, 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 Ψ_{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. □

Corollary 4. *Assuming the statement Ψ_{13}, a single query to an oracle for the halting problem decides whether or not the set of composite Fermat numbers is infinite.*

6. The implication from the title

If a set $\mathcal{W} \subseteq \mathbb{N} \setminus \{0\}$ satisfies

$$\forall n \left(n \in \mathcal{W} \Longrightarrow \{n,\ 2n,\ 3n,\ \ldots\} \subseteq \mathcal{W}\right)$$

then the implication from the title holds for $\mathcal{W}$ with $t(\mathcal{W}) = 0$. If $\mathcal{W}$ equals the set of positive integers n such that n^2+1 is prime, then Theorem 2 suggests a possibility that the implication from the title holds for $\mathcal{W}$ with $t(\mathcal{W}) = f(9)$. If $\mathcal{W}$ equals the set of twin primes, then Theorem 3 suggests a possibility that the implication from the title holds for $\mathcal{W}$ with $t(\mathcal{W}) = f(16)+3$. If $\mathcal{W}$ equals the set of positive integers n such that $2^{2^n}+1$ is composite, then Theorem 4 suggests a possibility that the implication from the title holds for $\mathcal{W}$ with $t(\mathcal{W}) = g(13)$.

References

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

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

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

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

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

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

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

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