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

Apoloniusz Tyszka

Abstract

We define computable functions $g, h : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$. For an integer $n \geq 3$, let $\Psi_n$ denote the following statement: if a system $S \subseteq \{x_1! = x_2 : (i, k) \in \{1, \ldots, n\} \land (i \neq k)\} \cup \{x_i, x_j : x_k : i, j, k \in \{1, \ldots, n\}\}$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leq g(n)$. For a positive integer $n$, let $\Gamma_n$ denote the following statement: if a system $S \subseteq \{x_1 \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\} \cup \{2^{2x_1} = x_k : i, k \in \{1, \ldots, n\}\}$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leq h(n)$. We prove: (1) if the equation $x^2 + 1 = y^2$ has only finitely many solutions in integers, then the statement $\Psi_5$ guarantees that each such solution $(x, y)$ belongs to the set $(\{5, 6, 7, 8\})$. (2) the statement $\Psi_9$ proves the following implication: if there exists a positive integer $x$ such that $x^2 + 1$ is prime and $x^2 + 1 \geq g(7)$, then there are infinitely many primes of the form $n^2 + 1$. (3) the statement $\Psi_9$ proves the following implication: if there exists an integer $x \geq g(6)$ such that $x^2 + 1$ is prime, then there are infinitely many primes of the form $n^2 + 1$. (4) the statement $\Psi_{16}$ proves the following implication: if there exists a twin prime greater than $g(14)$, then there are infinitely many twin primes. (5) the statement $\Gamma_{13}$ proves the following implication: if $n \in \mathbb{N} \setminus \{0\}$ and $2^{2n} + 1$ is composite and greater than $h(12)$, then $2^{2n} + 1$ is composite for infinitely many positive integers $n$.

Key words and phrases: Brocard’s problem, Brocard-Ramanujan equation, composite Fermat numbers, Dickson’s conjecture, halting of a Turing machine, prime numbers of the form $n^2 + 1$, prime numbers of the form $n! + 1$, Richert’s lemma, twin prime conjecture

2010 Mathematics Subject Classification: 03B30, 11A41.

1 Introduction

A twin prime is a prime number that differs from another prime number by 2. The twin prime conjecture states that there are infinitely many twin primes, see [15, p. 39]. The following statement

(1) “For every non-negative integer $n$ there exist prime exist numbers $p$ and $q$ such that $p + 2 = q$ and $p \in \{10^p, 10^q + 1\}$”

is a $\Pi_1$ statement which strengthens the twin prime conjecture, see [X, p. 43], cf. [5, pp. 337–338]. Statement (1) is equivalent to the non-halting of a Turing machine. C. H. Bennett claims that most mathematical conjectures can be settled indirectly by proving stronger $\Pi_1$ statements, see [1].

In this article, we study sets $X \subseteq \mathbb{N}$ for which we know an algorithm that computes a threshold number $t(X) \in \mathbb{N}$ such that $X$ is infinite if and only if $X$ contains an element greater than $t(X)$. If $X$ is computable, then this property implies that the infinity of $X$ is equivalent to the halting of a Turing machine. If a set $X \subseteq \mathbb{N}$ is empty or infinite, then any non-negative integer $m$ is a threshold number of $X$. If a set $X \subseteq \mathbb{N}$ is non-empty and finite, then all threshold numbers of $X$ form the set $\{\max(X), \max(X) + 1, \max(X) + 2, \ldots\}$.

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 $\gamma : \mathbb{N}^{m+1} \to \mathbb{N}$ 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.

The classes of the infinite recursively enumerable sets and of the infinite recursive sets are not recursively enumerable, see [16] p. 234].

**Corollary 1.** If an algorithm $\text{Alg}_{1}$ for every recursive set $\mathcal{R} \subseteq \mathbb{N}$ finds a non-negative integer $\text{Alg}_{1}(\mathcal{R})$, then there exists a finite set $\mathcal{W} \subseteq \mathbb{N}$ such that $\mathcal{W} \cap [\text{Alg}_{1}(\mathcal{W}) + 1, \infty) \neq \emptyset$. If an algorithm $\text{Alg}_{2}$ for every recursively enumerable set $\mathcal{R} \subseteq \mathbb{N}$ finds a non-negative integer $\text{Alg}_{2}(\mathcal{R})$, then there exists a finite set $\mathcal{W} \subseteq \mathbb{N}$ such that $\mathcal{W} \cap [\text{Alg}_{2}(\mathcal{W}) + 1, \infty) \neq \emptyset$.

## 2 Basic definitions and lemmas

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

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

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

![Fig. 1 Construction of the system $\mathcal{U}_n$](image)

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

Let

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

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

**Hypothesis 1.** The statements $\Psi_3, \ldots, \Psi_{16}$ are true.
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

**Theorem 4.** Every statement $\Psi_n$ 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. \qed

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

*Proof.* It follows from Lemma[1] because $\mathcal{U}_n \subseteq B_n$. \qed

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

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

**Lemma 3.** For every positive integers $x$ and $y$, $x \cdot \Gamma(x) = \Gamma(y)$ if and only if

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

**Lemma 4.** For every positive integers $x$ and $y$, $x + 1 = y$ if and only if

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

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

**Lemma 6.** (Wilson’s theorem, [7 p. 89]). For every integer $x \geq 3$, $x$ is prime if and only if $x$ divides $(x - 1)! + 1$.

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

Let

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

**Hypothesis 2.** ([25 p. 109]). If a system $S \subseteq G_n$ has only finitely many solutions in non-negative integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leq h(2n)$.

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


**Observation 1.** (cf. [25 p. 110, Observation 1]). For every system $S \subseteq G_n$ which involves all the variables $x_1, \ldots, x_n$, the following new system

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

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

*Proof.* It follows from Lemma[4] \qed

**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 $n \geq 3$, the following system

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

has exactly two solutions in positive integers, namely $(1, \ldots, 1)$ and $(f(1), \ldots, f(n))$. \qed
On sets \( X \subseteq \mathbb{N} \) for which we know an algorithm ...

For a positive integer \( n \), let \( \Phi_n \) denote the following statement: *if a system*

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

*has only finitely many solutions in positive integers \( x_1, \ldots, x_n \), then each such solution \((x_1, \ldots, x_n)\) satisfies \( x_1, \ldots, x_n \leq f(n) \).*

**Theorem 6.** *The statement \( \forall n \in \mathbb{N} \setminus \{0\} \Phi_n \) implies Hypothesis 3.*

**Proof.** It follows from Lemma 4.

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

\[
E_n = \{ 1 = x_k : k \in \{1, \ldots, n\} \} \cup \{ x_i + x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \cup \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \}
\]

Th. Skolem proved that every Diophantine equation can be algorithmically transformed into an equivalent system of Diophantine equations of degree at most 2, see [21] pp. 2–3 and [12] pp. 3–4. The following result strengthens Skolem’s theorem.

**Lemma 7.** ([23] p. 720). *Let \( D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p] \). Assume that \( \deg(D, x_i) \geq 1 \) 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 \( K \in \mathcal{R} \cup \{ \mathbb{N}, \mathbb{N} \setminus \{0\} \} \), then

\[
\forall \tilde{x}_1, \ldots, \tilde{x}_p \in K \left( D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \iff \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in K (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \text{ solves } T \right)
\]

**Condition 2.** If \( K \in \mathcal{R} \cup \{ \mathbb{N}, \mathbb{N} \setminus \{0\} \} \), then for each \( \tilde{x}_1, \ldots, \tilde{x}_p \in K \) with \( D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \), there exists a unique tuple \((\tilde{x}_{p+1}, \ldots, \tilde{x}_n) \in K^{n-p}\) 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 \( K \in \mathcal{R} \cup \{ \mathbb{N}, \mathbb{N} \setminus \{0\} \} \), the equation \( D(x_1, \ldots, x_p) = 0 \) and the system \( T \) have the same number of solutions in \( K \).*

Let \( \alpha, \beta, \) and \( \gamma \) denote variables.

**Lemma 8.** ([12] p. 100). *For each positive integers \( x, y, z \), \( x + y = z \) if and only if

\[
(2x + 1)(2y + 1) = z^2(xy + 1) + 1
\]

**Corollary 2.** *We can express the equation \( x + y = z \) as an equivalent system \( F \), where \( F \) involves \( x, y, z \) and 9 new variables, and where \( F \) 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. [25] p. 110, Lemma 4*). *Let \( D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p] \). Assume that \( \deg(D, x_i) \geq 1 \) 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 \( \tilde{x}_1, \ldots, \tilde{x}_p \),

\[
D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \iff \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \mathbb{N} \setminus \{0\} (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \text{ solves } T
\]

**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.*
On sets \( X \subseteq \mathbb{N} \) for which we know an algorithm ...

**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 2 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 \( \alpha \cdot \beta = \gamma \). \( \square \)

**Theorem 7.** 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. \( \square \)

**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?

Matyasevich’s conjecture on finite-fold Diophantine representations ([14]) implies a negative answer to Open Problem 1 see [13, 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 [11, p. 300].

### 4 Brocard’s problem

Let \( \mathcal{A} \) denote the following system of equations:

\[
\begin{align*}
    x_1! &= x_2 \\
    x_2! &= x_3 \\
    x_5! &= x_6 \\
    x_4 \cdot x_4 &= x_5 \\
    x_3 \cdot x_5 &= x_6
\end{align*}
\]

Lemma 2 and the diagram in Figure 2 explain the 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:

\[
\begin{align*}
    x_2 &= x_1! \\
    x_3 &= (x_1!)! \\
    x_5 &= x_1! + 1 \\
    x_6 &= (x_1! + 1)!
\end{align*}
\]

**Proof.** It follows from Lemma 2. \( \square \)
It is conjectured that \( x_1! + 1 \) is a perfect square only for \( x \in \{4, 5, 7\} \), see [26, p. 297]. A weak form of Szpiro’s conjecture implies that there are only finitely many solutions to the equation \( x_1! + 1 = y^2 \), see [17].

**Theorem 8.** If the equation \( x_1! + 1 = x_2^2 \) has only finitely many solutions in positive integers, then the statement \( \Psi_6 \) 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 \( x_1! + 1 = x_2^2 \). Then, \( x_1, x_4 \in \mathbb{N} \setminus \{0, 1\} \). By Lemma 10, the system \( \mathbf{A} \) is solvable in positive integers \( x_2, x_3, x_5, x_6 \). Since \( \mathbf{A} \subseteq \mathbf{B}_6 \), the statement \( \Psi_6 \) implies that \( x_6 = (x_1! + 1)! \leq g(6) = g(5)! \). Hence, \( x_1! + 1 \leq g(5) = g(4)! \). Consequently, \( x_1 < g(4) = 24 \). If \( x_1 \in \{1, \ldots, 23\} \), then \( x_1! + 1 \) is a perfect square only for \( x_1 \in \{4, 5, 7\} \). \( \square \)

### 5 Are there infinitely many prime numbers of the form \( n^2 + 1 \)?

Let \( \mathbf{B} \) denote the following system of equations:

\[
\begin{align*}
x_2! &= x_3 \\
x_3! &= x_4 \\
x_5! &= x_6 \\
x_6! &= x_9 \\
x_1 \cdot x_1 &= x_2 \\
x_3 \cdot x_5 &= x_6 \\
x_4 \cdot x_8 &= x_9 \\
x_5 \cdot x_7 &= x_8
\end{align*}
\]

Lemma 11 and the diagram in Figure 3 explain the construction of the system \( \mathbf{B} \).

**Fig. 3** Construction of the system \( \mathbf{B} \)

**Lemma 11.** For every integer \( x_1 \geq 2 \), the system \( \mathbf{B} \) is solvable in positive integers \( x_2, \ldots, x_9 \) if and only if \( x_1^2 + 1 \) is prime. In this case, the integers \( x_2, \ldots, x_9 \) are uniquely determined by the following equalities:

\[
\begin{align*}
x_2 &= x_1^2 \\
x_3 &= (x_1^2)! \\
x_4 &= ((x_1^2)!)! \\
x_5 &= x_1^2 + 1 \\
x_6 &= ((x_1^2)!)! + 1 \\
x_7 &= \frac{x_3^2 + 1}{x_5^2 + 1} \\
x_8 &= (x_3^2)! + 1 \\
x_9 &= (x_3^2)! + 1
\end{align*}
\]
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

Proof. By Lemma 2 for every integer $x_1 \geq 2$, the system $\mathcal{B}$ is solvable in positive integers $x_2, \ldots, x_9$ if and only if $x_1^2 + 1$ divides $(x_1^2)! + 1$. Hence, the claim of Lemma 12 follows from Lemma 6. □

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

Proof. If a tuple $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ solves the system $\mathcal{B}$ and $x_1 = 1$, then $x_1, \ldots, x_9 \leq 2$. 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, $x_9 = x_8! \leq 2$. □

Edmund Landau’s conjecture states that there are infinitely many primes of the form $n^2 + 1$, see [15, pp. 37–38].

**Theorem 9.** The statement $\Psi_9$ proves the following implication: if there exists an integer $x_1 \geq 2$ 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 $(x_2, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$ such that the tuple $(x_1, x_2, \ldots, x_9)$ solves the system $\mathcal{B}$. Since $x_1^2 + 1 > g(7)$, we obtain that $x_1^2 \geq g(7)$. Hence, $(x_1^2)! > g(7)! = g(8)$. Consequently,

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

Since $\mathcal{B} \subseteq \mathcal{B}_0$, the statement $\Psi_9$ and the inequality $x_9 > g(9)$ imply that the system $\mathcal{B}$ has infinitely many solutions $(x_1, \ldots, x_9) \in (\mathbb{N} \setminus \{0\})^9$. According to Lemmas 11 and 12 there are infinitely many primes of the form $n^2 + 1$. □

**6 Are there infinitely many prime numbers of the form $n! + 1$?**

It is conjectured that there are infinitely many primes of the form $n! + 1$, see [2] p. 443 and [22].

**Theorem 10.** The statement $\Psi_9$ proves the following implication: if there exists an integer $x_1 \geq g(6)$ such that $x_1! + 1$ is prime, then there are infinitely many primes of the form $n! + 1$.

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

**7 The twin prime conjecture and Dickson’s conjecture**

Let $C$ denote the following system of equations:

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

Lemma 2 and the diagram in Figure 4 explain the 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:

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

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

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

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

$$
(x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})
$$
On sets \( X \subseteq \mathbb{N} \) for which we know an algorithm ...

Proof. If a tuple \((x_1, \ldots, x_{16}) \in (\mathbb{N} \setminus \{0\})^{16}\) solves the system \( C \) and

\[
(x_4 \in \{1, 2\}) \lor (x_9 \in \{1, 2\})
\]

then \(x_1, \ldots, x_{16} \leq 7!\). Indeed, for example, if \(x_4 = 2\) then \(x_6 = x_4 + 1 = 3\). Hence, \(x_7 = x_6! = 6\). Therefore, \(x_{15} = x_{15} + 1 = 7\). Consequently, \(x_{16} = x_{15}! = 7!\).

\[\square\]

Theorem 11. The statement \( \Psi_{16} \) 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 \(x_9 - 1 \geq g(14)\). Therefore, \((x_9 - 1)! \geq g(14)! = g(15)\).

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 \( \Psi_{16} \) 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.

\[\square\]

Let \( \mathbb{P}(x) \) denote the predicate "\( x \) is a prime number". Dickson’s conjecture ([15, p. 36], [27, p. 109]) implies that the existential theory of \((\mathbb{N}, =, +, \mathbb{P})\) is decidable, see [27, Theorem 2, p. 109]. For a positive integer \(n\), let \( \Theta_n \) denote the following statement: for every system \( S \subseteq \{x_i + 1 = x_j : i, j \in \{1, \ldots, n\}\} \cup \{\mathbb{P}(x_i) : i \in \{1, \ldots, n\}\} \) the solvability of \( S \) in non-negative integers is decidable.

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

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

\[
\exists u, v \in \mathbb{N} \ ((u + u = v) \land \mathbb{P}(v) \land (x + u = y))
\]

\[\square\]

Theorem 12. 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

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

(2)

If sentence (2) is false, then the twin prime conjecture is false. If sentence (2) is true, then there exists a twin prime greater than \( g(14) \). In this case, the twin prime conjecture follows from Theorem 11.

\[\square\]

8  A hypothesis which implies that any prime number \( p > 24 \) proves that there are infinitely many prime numbers

For a positive integer \( n \), let \( \Gamma(n) \) denote \((n - 1)!\). Let \( \lambda(5) = \Gamma(5) \), and let \( \lambda(n + 1) = \Gamma(\lambda(n)) \) for every integer \( n \geq 5 \). For an integer \( n \geq 5 \), let \( J_n \) denote the following system of equations:

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

Lemma 8 and the diagram in Figure 5 explain the construction of the system \( J_n \).
On sets \( X \subseteq \mathbb{N} \) for which we know an algorithm...

For every integer \( n \geq 5 \), 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 \( n \geq 5 \), let \( \Delta_n \) denote the following statement: if a system \( S \subseteq \{ \Gamma(x_i) = x_k : i, k \in \{1, \ldots, n\} \} \cup \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \) has only finitely many solutions in positive integers \( x_1, \ldots, x_n \), then each such solution \((x_1, \ldots, x_n)\) satisfies \( x_1, \ldots, x_n \leq \lambda(n) \).

Hypothesis 4. The statements \( \Delta_5, \ldots, \Delta_{14} \) are true.

Lemmas [3] and [6] imply that the statements \( \Delta_n \) have essentially the same consequences as the statements \( \Psi_n \).

Theorem 13. The statement \( \Delta_6 \) implies that any prime number \( p > 24 \) proves that there are infinitely many prime numbers.

Proof. It follows from Lemmas [3] and [6]. We leave the details to the reader. \( \square \)

9 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. ([70, 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 [9, p. 23].

Theorem 14. ([24]). An unproven inequality stated in [24] implies that \( 2^{2^n} + 1 \) is composite for every integer \( n \geq 5 \).

Let \( \mathcal{J}_n = \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \cup \{ 2^{2^x_i} = x_k : i, k \in \{1, \ldots, n\} \} \)

Lemma 16. The following subsystem of \( \mathcal{J}_n \)

\[
\begin{align*}
    x_1 \cdot x_1 &= x_1 \\
    \forall i \in \{1, \ldots, n-1\} 2^{2^x_i} &= x_{i+1}
\end{align*}
\]

has exactly one solution \((x_1, \ldots, x_n) \in (\mathbb{N} \setminus \{0\})^n\), namely \((h(1), \ldots, h(n))\).
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

For a positive integer $n$, let $\Gamma_n$ 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 $x_1, \ldots, x_n \leq h(n)$. The statement $\Gamma_n$ says that for subsystems of $H_n$ the largest known solution is indeed the largest possible.

**Hypothesis 5.** 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 [11, p. 300].

**Lemma 17.** For every positive integer $n$, the system $H_n$ has a finite number of subsystems.

**Theorem 15.** Every statement $\Gamma_n$ is true with an unknown integer bound that depends on $n$.

**Proof.** It follows from Lemma [17].

**Theorem 16.** The statement $\Gamma_{13}$ proves the following implication: if $z \in \mathbb{N} \setminus \{0\}$ and $2^{2z} + 1$ is composite and greater than $h(12)$, then $2^{2z} + 1$ is composite for infinitely many positive integers $z$.

**Proof.** Let us consider the equation

\[(x + 1)(y + 1) = 2^{2z} + 1\]  \hspace{1cm} (3)

in positive integers. By Lemma [5], we can transform equation (3) 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 $2^{2x} = \gamma$, see the diagram in Figure 6.

![Fig. 6 Construction of the system $\mathcal{G}$](image)

Since $2^{2z} + 1 > h(12)$, we obtain that $2^{22^{22z}+1} > h(13)$. By this, the statement $\Gamma_{13}$ implies that the system $\mathcal{G}$ has infinitely many solutions in positive integers. It means that there are infinitely many composite Fermat numbers.
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

## 10 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 18.** (\[6\], \[18\], \[20, p. 152\]). Let $(m_i)_{i=1}^\infty$ be an increasing sequence of positive integers such that for some positive integer $k$ the inequality $m_{i+1} \leq 2m_i$ 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 $T$ denote the set of all positive integers $i$ such that every integer $j \geq i$ is expressible as a sum of one or more distinct elements of the set $(m_1, m_2, m_3, \ldots)$. Obviously, $T = \emptyset$ or $T = [d, \infty) \cap \mathbb{N}$ for some positive integer $d$.

**Corollary 3.** If the sequence $(m_i)_{i=1}^\infty$ is computable and the algorithm in Figure 7 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 7 terminates, then the set $T$ is infinite. In this case, the algorithm is Figure 7 prints all positive integers which are not expressible as a sum of one or more distinct elements of the set $(m_1, m_2, m_3, \ldots)$.

**Fig. 7** The algorithm which uses Richert’s lemma
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

**Theorem 17.** (Theorem 2.3). If there exists $\varepsilon > 0$ such that the inequality $m_{i+1} \leq (2 - \varepsilon) \cdot m_i$ holds for every sufficiently large $i$, then the algorithm in Figure 7 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 4.** If there exists $\varepsilon > 0$ such that the inequality $m_{i+1} \leq (2 - \varepsilon) \cdot m_i$ holds for every sufficiently large $i$, then the algorithm in Figure 7 terminates if and only if the set $T$ is infinite.

We show how the algorithm in Figure 7 works for a concrete sequence $\{m_i\}_{i=1}^{\infty}$. Let $\lfloor \cdot \rfloor$ denote the integer part function. For a positive integer $i$, let $t_i = \frac{(i + 19)^i + 19}{(i + 19)! \cdot 2^i + 19}$, and let $m_i = \lfloor t_i \rfloor$.

**Lemma 19.** The inequality $m_{i+1} \leq 2m_i$ holds for every positive integer $i$.

**Proof.** For every positive integer $i$,

$$\frac{m_i}{m_{i+1}} = \frac{\lfloor t_i \rfloor}{\lfloor t_{i+1} \rfloor} > \frac{t_i - 1}{t_{i+1}} = \frac{t_i}{t_{i+1}} - \frac{1}{t_{i+1}} \geq \frac{t_i}{t_{i+1}} - \frac{1}{t_2} = 2 \cdot \frac{i + 20}{i + 19} \left(1 - \frac{1}{i + 20}\right)^{i+20} - \frac{21! \cdot 2^{21}}{2^{-21}} > 2 \left(1 - \frac{1}{21}\right)^{21} - \frac{21! \cdot 2^{21}}{2^{-21}} = 4087158528442715204485120000 - \frac{5842587018385982521381124421}{12}$$

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

**Theorem 18.** The algorithm in Figure 7 terminates for the sequence $\{m_i\}_{i=1}^{\infty}$.

**Proof.** By Lemma 19, we take $k = 2$ as the initial value of $k$. The following MuPAD code

```plaintext
k:=2:
repeat
A:=\{floor((i+19)^(i+19)/((i+19)!*2^(i+19))) $i=1\ldots 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\ldots nops(B)\}:
end_for:
G:=\{y $y=B[1]\ldots B[nops(B)]+1\} minus B:
H:=\{G[n+1]-G[n] $n=1\ldots 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\ldots 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\ldots nops(B)\}:
end_for:
print(\{n $n=1\ldots b\} minus B):
```

implements the algorithm in Figure 7 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:

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, \ldots\}$$
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...
On sets $X \subseteq \mathbb{N}$ for which we know an algorithm ...

Corollary 5. $T = [2762, \infty) \cap \mathbb{N}$.

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.

References


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