Research Article **Open Access**

Apoloniusz Tyszka*

Is there a computable upper bound for the height of a solution of a Diophantine equation with a unique solution in positive integers?

https://doi.org/10.1515/comp-2017-0003
Received April 6, 2017; accepted June 6, 2017

Abstract: Let $B_n = \{x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,n\}\} \cup \{x_i + 1 = x_k : i,k \in \{1,\ldots,n\}\}$ denote the system of equations in the variables $x_1,\ldots,x_n$. For a positive integer n, let $\xi(n)$ denote the smallest positive integer b such that for each system of equations $\mathcal{S} \subseteq B_n$ with a unique solution in positive integers $x_1,\ldots,x_n$, this solution belongs to $[1,b]^n$. Let $g(1) = 1$, and let $g(n+1) = 2^{2^{g(n)}}$ for every positive integer n. We conjecture that $\xi(n) \leqslant g(2n)$ for every positive integer n. We prove: (1) the function $\xi\colon \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ is computable in the limit; (2) if a function $f\colon \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ has a single-fold Diophantine representation, then there exists a positive integer m such that $f(n) < \xi(n)$ for every integer $n > m$; (3) the conjecture implies that there exists an algorithm which takes as input a Diophantine equation $D(x_1,\ldots,x_p) = 0$ and returns a positive integer d with the following property: for every positive integers $a_1,\ldots,a_p$, if the tuple $(a_1,\ldots,a_p)$ solely solves the equation $D(x_1,\ldots,x_p) = 0$ in positive integers, then $a_1,\ldots,a_p \leqslant d$; (4) the conjecture implies that if a set $\mathcal{M} \subseteq \mathbb{N}$ has a single-fold Diophantine representation, then $\mathcal{M}$ is computable; (5) for every integer $n > 9$, the inequality $\xi(n) < \left(2^{2^{n-5}} - 1\right)^{2^{n-5}} + 1$ implies that $2^{2^{n-5}} + 1$ is composite.

Keywords: Diophantine equation with a unique solution in positive integers, Fermat prime, single-fold Diophantine representation, upper bound for the height of a solution

1 Introduction

A Diophantine equation is a polynomial equation with integer coefficients. When we solve a Diophantine equation, we implicitly assume that we are looking for solutions among rationals or among integers or among non-negative integers or among positive integers. Most theorems in computability theory say about the non-existence of algorithms for problems concerning Diophantine equations. For example, there is no algorithm to decide whether or not a Diophantine equation has an integer solution, which was proved by Russian mathematician Yuri Matiyasevich in 1970, see [4]. In another formulation, it means that the set of Diophantine equations which are solvable in integers is not computable, although it is recursively enumerable. It is also undecidable whether a Diophantine equation has infinitely or finitely many solutions in positive integers, see [1]. The same is true when we consider integer solutions or non-negative integer solutions. Moreover, the set of Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable, see [9, p. 104, Corollary 1] and [10, p. 240].

In this article, we propose a conjecture which implies that there exists an algorithm which takes as input a Diophantine equation $D(x_1,\ldots,x_p) = 0$ and returns a positive integer d with the following property: for every positive integers $a_1,\ldots,a_p$, if the tuple $(a_1,\ldots,a_p)$ solely solves the equation $D(x_1,\ldots,x_p) = 0$ in positive integers, then $a_1,\ldots,a_p \leqslant d$. Since the height of an integer tuple $(c_1,\ldots,c_p)$ is defined as $\max(|c_1|,\ldots,|c_p|)$, our claim asserts that the height of the tuple $(a_1,\ldots,a_p)$ does not exceed d.

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

2 A conjecture on integer arithmetic

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

$$\begin{aligned} B_n \quad = \quad & \{x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,n\}\} \cup \\ & \{x_i + 1 = x_k : i,k \in \{1,\ldots,n\}\} \end{aligned}$$

denote the system of equations in the variables $x_1,\ldots,x_n$. For a positive integer n, let $\xi(n)$ denote the smallest positive integer b such that for each system of equations $\mathcal{S} \subseteq B_n$ with a unique solution in positive integers $x_1,\ldots,x_n$, this solution belongs to $[1,b]^n$. We do not know whether or not there exists a computable function $\gamma\colon \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ such that the inequality $\xi(n) \leqslant \gamma(n)$ holds for every sufficiently large positive integer n.

Theorem 1. *The function $\xi\colon \mathbb{N}\setminus\{0\} \to \mathbb{N}\setminus\{0\}$ is computable in the limit.*

Proof. The flowchart in Figure 1 describes an algorithm which computes $\xi(n)$ in the limit. □

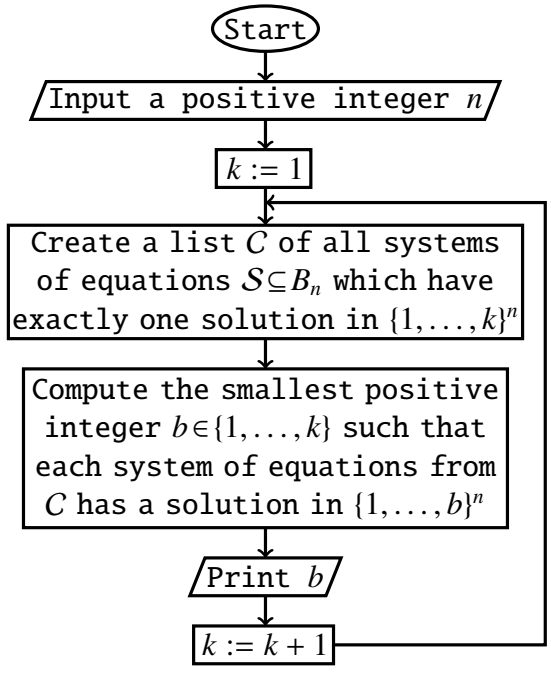

Figure 1: An infinite computation of $\xi(n)$

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

Conjecture 1. *If a system of equations $\mathcal{S} \subseteq B_n$ has exactly one solution in positive integers $x_1,\ldots,x_n$, then $x_1,\ldots,x_n \leqslant g(2n)$. In other words, $\xi(n) \leqslant g(2n)$ for every positive integer n.*

Observations 1 and 2 justify Conjecture 1.

Observation 1. *For every system of equations $\mathcal{S} \subseteq B_n$ which involves all the variables $x_1,\ldots,x_n$, the following new system of equations*

$$\begin{gathered} \left(\bigcup_{x_i \cdot x_j = x_k \in S} \{x_i \cdot x_j = x_k\} \right) \cup \\ \left\{ 2^{2^{x_k}} = y_k : k \in \{1,\ldots,n\} \right\} \cup \\ \bigcup_{x_i + 1 = x_k \in S} \{y_i \cdot y_i = y_k\} \end{gathered}$$

is equivalent to $\mathcal{S}$. If the system of equations $\mathcal{S}$ has exactly one solution in positive integers $x_1,\ldots,x_n$, then the new system of equations has exactly one solution in positive integers $x_1,\ldots,x_n,y_1,\ldots,y_n$.

Proof. It follows from Lemma 1. □

Observation 2. *For every positive integer n, the following system of equations*

$$\begin{cases} x_1 \cdot x_1 = x_1 \\ \forall i \in \{1,\ldots,n-1\}\ 2^{2^{x_i}} = x_{i+1} \text{ (if } n > 1) \end{cases}$$

has exactly one solution in positive integers, namely $(g(1),\ldots,g(n))$.

Conjecture 2 generalizes Conjecture 1.

Conjecture 2. *If a system of equations $\mathcal{S} \subseteq B_n$ has only finitely many solutions in positive integers $x_1,\ldots,x_n$, then $x_1,\ldots,x_n \leqslant g(2n)$.*

3 Algebraic lemmas lead to the main theorem

By introducing new auxiliary variables each Diophantine equation can be algorithmically transformed into an equivalent finite system of equations of the forms: variable equals one, variable plus variable equals variable, and variable times variable equals variable. This theorem can be strengthened and stated as follows: each Diophantine equation can be algorithmically transformed into an equivalent finite system of equations of the forms: variable plus one equals variable, and variable times variable

equals variable. The strengthened theorem (Lemma 4) is a consequence of Julia Robinson's theorem of 1949. She showed that addition is definable in terms of successor and multiplication. The question of the possibility of such a definition was posed by Polish mathematician Andrzej Mostowski.

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

$$\begin{aligned} E_n \quad = \quad & \{1 = x_k : \ k \in \{1, \ldots, n\}\} \cup \\ & \{x_i + x_j = x_k : \ i, j, k \in \{1, \ldots, n\}\} \cup \\ & \{x_i \cdot x_j = x_k : \ i, j, k \in \{1, \ldots, n\}\} \end{aligned}$$

Th. Skolem proved that every Diophantine equation can be algorithmically transformed into an equivalent system of Diophantine equations of degree at most 2, see [8, pp. 2–3] and [4, pp. 3–4]. The following result strengthens Skolem's theorem.

Lemma 2. *([13, p. 720]) Let*

$$D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$$

Assume that $\deg(D, x_i) \geqslant 1$ *for each* $i \in \{1, \ldots, p\}$. *We can compute a positive integer* $n > p$ *and a system of equations* $\mathcal{T} \subseteq E_n$ *which satisfies the following two conditions:*

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

$$\begin{aligned} & \forall \tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K} \Big(D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \iff \\ & \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \boldsymbol{K} \, (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \ solves \ \mathcal{T} \Big) \end{aligned}$$

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

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

Let α, β, and γ denote variables.

Lemma 3. *([7, p. 100]) For each positive integers* x, y, z, $x + y = z$ *if and only if*

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

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

Proof. The new 9 variables express the following polynomials:

$$\begin{gathered} zx, \quad zx + 1, \quad zy, \quad zy + 1, \quad z^2, \quad xy, \\ xy + 1, \quad z^2(xy + 1), \quad z^2(xy + 1) + 1. \end{gathered}$$

□

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

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

$$\begin{gathered} D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \iff \\ \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \mathbb{N} \setminus \{0\} \\ (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \ solves \ \mathcal{T} \end{gathered}$$

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* $\mathcal{T}$.

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

Proof. Let the system of equations $\mathcal{T}$ be given by Lemma 2. We replace in $\mathcal{T}$ each equation of the form $1 = x_k$ by the equation $x_k \cdot x_k = x_k$. Next, we apply Corollary 1 and replace in $\mathcal{T}$ each equation of the form $x_i + x_j = x_k$ by an equivalent system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. □

Lemma 4 implies Theorem 2.

Theorem 2. *Conjecture 1 implies that there exists an algorithm which takes as input a Diophantine equation* $D(x_1, \ldots, x_p) = 0$ *and returns a positive integer* d *with the following property: for every positive integers* $a_1, \ldots, a_p$, *if the tuple* $(a_1, \ldots, a_p)$ *solely solves the equation* $D(x_1, \ldots, x_p) = 0$ *in positive integers, then* $a_1, \ldots, a_p \leqslant d$.

Theorem 3. *Conjecture 1 implies that there exists an algorithm which takes as input a Diophantine equation* $D(x_1, \ldots, x_p) = 0$ *and returns a positive integer* d *with the following property: for every non-negative integers* $a_1, \ldots, a_p$, *if the tuple* $(a_1, \ldots, a_p)$ *solely solves the equation* $D(x_1, \ldots, x_p) = 0$ *in non-negative integers, then* $a_1, \ldots, a_p \leqslant d$.

Proof. We apply Theorem 2 to the equation $D(x_1 - 1, \ldots, x_p - 1) = 0$. □

4 Single-fold Diophantine representations

The Davis-Putnam-Robinson-Matiyasevich theorem states that every recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a Diophantine representation, that is

$$(a_1, \ldots, a_n) \in \mathcal{M} \iff$$
$$\exists x_1, \ldots, x_m \in \mathbb{N} \ W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \quad (\mathrm{R})$$

for some polynomial W with integer coefficients, see [4]. The polynomial W can be computed, if we know the Turing machine M such that, for all $(a_1, \ldots, a_n) \in \mathbb{N}^n$, M halts on $(a_1, \ldots, a_n)$ if and only if $(a_1, \ldots, a_n) \in \mathcal{M}$, see [4]. The representation (R) is said to be single-fold, if for any $a_1, \ldots, a_n \in \mathbb{N}$ the equation $W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ has at most one solution $(x_1, \ldots, x_m) \in \mathbb{N}^m$. The representation (R) is said to be finite-fold, if for any $a_1, \ldots, a_n \in \mathbb{N}$ the equation $W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ has only finitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$. Yu. Matiyasevich conjectured that each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a single-fold (finite-fold) Diophantine representation, see [2, pp. 341–342] and [5, p. 42]. Currently, he seems agnostic on his conjectures, see [6, p. 749]. In [12, p. 581], the author explains why Matiyasevich's conjectures although widely known are less widely accepted.

Theorem 4. *(cf. [11, Theorem 5, p. 711]) Conjecture 1 implies that if a set $\mathcal{M} \subseteq \mathbb{N}$ has a single-fold Diophantine representation, then $\mathcal{M}$ is computable. In particular, Conjecture 1 contradicts Matiyasevich's conjecture on single-fold Diophantine representations.*

Proof. Let a set $\mathcal{M} \subseteq \mathbb{N}$ have a single-fold Diophantine representation. It means that there exists a polynomial $W(x, x_1, \ldots, x_m)$ with integer coefficients such that

$$\forall b \in \mathbb{N} \Big(b \in \mathcal{M} \iff$$
$$\exists x_1, \ldots, x_m \in \mathbb{N} \ W(b, x_1, \ldots, x_m) = 0 \Big)$$

and for every $b \in \mathbb{N}$ the equation $W(b, x_1, \ldots, x_m) = 0$ has at most one solution $(x_1, \ldots, x_m) \in \mathbb{N}^m$. By Theorem 3, there exists a computable function $\theta\colon \mathbb{N} \to \mathbb{N}$ such that for every $b, x_1, \ldots, x_m \in \mathbb{N}$ the equality $W(b, x_1, \ldots, x_m) = 0$ implies $\max(x_1, \ldots, x_m) \leqslant \theta(b)$. Hence, we can decide whether or not a non-negative integer b belongs to $\mathcal{M}$ by checking whether or not the equation $W(b, x_1, \ldots, x_m) = 0$ has an integer solution in the box $[0, \theta(b)]^m$. □

Observation 3. *Theorem 4 remains true if we change the bound $g(2n)$ in Conjecture 1 to any other computable bound $\delta(n)$.*

Theorem 5. *If a function $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ has a single-fold Diophantine representation, then there exists a positive integer m such that $f(n) < \xi(n)$ for every integer $n > m$.*

Proof. There exists a polynomial $W(x_1, x_2, x_3, \ldots, x_r)$ with integer coefficients such that for each positive integers x_1, x_2,

$$(x_1, x_2) \in f \iff \exists x_3, \ldots, x_r \in \mathbb{N} \setminus \{0\}$$
$$W(x_1, x_2, x_3 - 1, \ldots, x_r - 1) = 0$$

and for each positive integers x_1, x_2 at most one tuple $(x_3, \ldots, x_r)$ of positive integers satisfies $W(x_1, x_2, x_3 - 1, \ldots, x_r - 1) = 0$. By Lemma 4, there exists an integer $s \geqslant 3$ such that for every positive integers x_1, x_2,

$$(x_1, x_2) \in f \iff$$
$$\exists x_3, \ldots, x_s \in \mathbb{N} \setminus \{0\} \Psi(x_1, x_2, x_3, \ldots, x_s) \qquad (\mathrm{E})$$

where $\Psi(x_1, x_2, x_3, \ldots, x_s)$ is a conjunction of formulae of the forms $x_i + 1 = x_k$ and $x_i \cdot x_j = x_k$, the indices i, j, k belong to $\{1, \ldots, s\}$, and for each positive integers x_1, x_2 at most one tuple $(x_3, \ldots, x_s)$ of positive integers satisfies $\Psi(x_1, x_2, x_3, \ldots, x_s)$. Let $[\cdot]$ denote the integer part function, and let an integer n be greater than $m = 2s + 2$. Then,

$$n \geqslant \left[\frac{n}{2}\right] + \frac{n}{2} > \left[\frac{n}{2}\right] + s + 1$$

and $n - \left[\frac{n}{2}\right] - s - 2 \geqslant 0$. Let T_n denote the following system of equations with n variables:

$$\begin{cases} \text{all equations occurring in } \Psi(x_1, x_2, x_3, \ldots, x_s) \\ \forall i \in \left\{1, \ldots, n - \left[\frac{n}{2}\right] - s - 2\right\} \ u_i \cdot u_i = u_i \\ t_1 \cdot t_1 = t_1 \\ \forall i \in \left\{1, \ldots, \left[\frac{n}{2}\right] - 1\right\} \ t_i + 1 = t_{i+1} \\ t_2 \cdot t_{\left[\frac{n}{2}\right]} = u \\ u + 1 = x_1 \\ \text{(if } n \text{ is odd)} \\ t_1 \cdot u = x_1 \\ \text{(if } n \text{ is even)} \\ x_2 + 1 = y \end{cases}$$

By the equivalence (E), the system of equations T_n is solvable in positive integers, $2 \cdot \left[\frac{n}{2}\right] = u$, $n = x_1$, and

$$f(n) = f(x_1) = x_2 < x_2 + 1 = y$$

Since $T_n \subseteq B_n$ and T_n has at most one solution in positive integers, $y \leqslant \xi(n)$. Hence, $f(n) < \xi(n)$. □

Corollary 2. *If the function $\xi\colon \mathbb{N}\setminus\{0\}\to\mathbb{N}\setminus\{0\}$ is dominated by a computable function, then Matiyasevich's conjecture on single-fold Diophantine representations is false. In particular, Conjecture 1 contradicts Matiyasevich's conjecture on single-fold Diophantine representations.*

5 Fermat primes

Observation 4. *Only $x_1 = 1$ solves the equation $x_1 \cdot x_1 = x_1$ in positive integers. Only $x_1 = 1$ and $x_2 = 2$ solve the system $\{x_1 \cdot x_1 = x_1,\ x_1 + 1 = x_2\}$ in positive integers. For each integer $n \geqslant 3$, the following system of equations*

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

has a unique solution in positive integers, namely $\left(1, 2, 4, 16, 256, \ldots, 2^{2^{n-3}}, 2^{2^{n-2}}\right)$.

Corollary 3. *We have: $\xi(1) = 1$ and $\xi(2) = 2$. The inequality $\xi(n) \geqslant 2^{2^{n-2}}$ holds for every integer $n \geqslant 3$.*

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 ([3, 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 ([3, p. 1]). It is not known whether or not there are any other Fermat primes ([3, p. 206]).

Theorem 6. *If $n \in \mathbb{N}\setminus\{0\}$ and $2^{2^n}+1$ is prime, then the following system of equations*

$$\begin{cases} \forall i \in \{1,\ldots,n\}\ x_i \cdot x_i &= x_{i+1} \\ x_1 + 1 &= x_{n+2} \\ x_{n+2} + 1 &= x_{n+3} \\ x_{n+1} + 1 &= x_{n+4} \\ x_{n+3} \cdot x_{n+5} &= x_{n+4} \end{cases}$$

has a unique solution $(a_1,\ldots,a_{n+5})$ in non-negative integers. The numbers $a_1,\ldots,a_{n+5}$ are positive and $\max(a_1,\ldots,a_{n+5}) = a_{n+4} = \left(2^{2^n}-1\right)^{2^n}+1$.

Proof. The system of equations equivalently expresses that $(x_1+2)\cdot x_{n+5} = x_1^{2^n}+1$. Since

$$x_1^{2^n}+1 = \left((x_1+2)-2\right)^{2^n}+1 =$$

$$2^{2^n}+1+(x_1+2)\cdot\sum_{k=1}^{2^n}\binom{2^n}{k}\cdot(x_1+2)^{k-1}\cdot(-2)^{2^n-k}$$

we get

$$(x_1+2)\cdot\left(x_{n+5}-\sum_{k=1}^{2^n}\binom{2^n}{k}\cdot(x_1+2)^{k-1}\cdot(-2)^{2^n-k}\right) = 2^{2^n}+1$$

Hence, x_1+2 divides $2^{2^n}+1$. Since $x_1+2 \geqslant 2$ and $2^{2^n}+1$ is prime, we get $x_1+2 = 2^{2^n}+1$ and $x_1 = 2^{2^n}-1$. Next, $x_{n+1} = x_1^{2^n} = \left(2^{2^n}-1\right)^{2^n}$ and

$$x_{n+4} = x_{n+1}+1 = \left(2^{2^n}-1\right)^{2^n}+1$$

Explicitly, the whole solution is given by

$$\begin{cases} \forall i \in \{1,\ldots,n+1\}\ a_i &= \left(2^{2^n}-1\right)^{2^{i-1}} \\ a_{n+2} &= 2^{2^n} \\ a_{n+3} &= 2^{2^n}+1 \\ a_{n+4} &= \left(2^{2^n}-1\right)^{2^n}+1 \\ a_{n+5} = 1+\sum_{k=1}^{2^n}\binom{2^n}{k}\cdot\left(2^{2^n}+1\right)^{k-1}\cdot(-2)^{2^n-k} \end{cases}$$

□

Corollary 4. *For every integer $n > 5$, if $2^{2^{n-5}}+1$ is prime, then*

$$\xi(n) \geqslant \left(2^{2^{n-5}}-1\right)^{2^{n-5}}+1$$

In particular,

$$\xi(9) \geqslant \left(2^{2^{9-5}}-1\right)^{2^{9-5}}+1 =$$

$$\left(2^{16}-1\right)^{16}+1 > \left(2^{16}-2^{15}\right)^{16} =$$

$$\left(2^{15}\right)^{16} = 2^{240} > 2^{2^{9-2}}$$

The numbers $2^{2^{n-5}}+1$ are prime when $n \in \{6,7,8\}$, but

$$\left(2^{2^{6-5}}-1\right)^{2^{6-5}}+1 = 10 < 65536 = 2^{2^{6-2}}$$

$$\left(2^{2^{7-5}}-1\right)^{2^{7-5}}+1=50626<4294967296=2^{2^{7-2}}$$

$$\left(2^{2^{8-5}}-1\right)^{2^{8-5}}+1=$$
$$17878103347812890626<18446744073709551616=2^{2^{8-2}}$$

Corollary 5. *For every integer $n>9$, the inequality $\xi(n)<\left(2^{2^{n-5}}-1\right)^{2^{n-5}}+1$ implies that $2^{2^{n-5}}+1$ is composite.*

6 Two stronger conjectures

Conjecture 3 strengthens Conjecture 1.

Conjecture 3. *If $n\in\{3,\ldots,8\}$, then $\xi(n)=2^{2^{n-2}}$. If $n\geqslant 9$, then $\xi(n)\leqslant\left(2^{2^{n-5}}-1\right)^{2^{n-5}}+1$.*

Theorem 7. *(cf. [11, Theorem 2, p. 709]) For each positive integer n, the following system of equations*

$$\begin{cases}\forall i\in\{1,\ldots,n\}\ x_i\cdot x_i = x_{i+1}\\ x_{n+2}+1=x_1\\ x_{n+3}+1=x_{n+2}\\ x_{n+3}\cdot x_{n+4}=x_{n+1}\\ x_{n+5}\cdot x_{n+5}=x_{n+5}\\ x_{n+5}+1=x_{n+6}\\ x_{n+6}\cdot x_{n+7}=x_1\\ x_{n+6}\cdot x_{n+8}=x_{n+9}\\ x_{n+9}+1=x_{n+4}\end{cases}$$

has a unique solution $(a_1,\ldots,a_{n+9})$ in positive integers. The numbers $a_1,\ldots,a_{n+9}$ satisfy:

$$\begin{aligned}\forall i\in\{1,\ldots,n+1\}\ a_i &= \left(2+2^{2^n}\right)^{2^{i-1}}\\ a_{n+2}&=1+2^{2^n}\\ a_{n+3}&=2^{2^n}\\ a_{n+4}&=\left(1+2^{2^n}-1\right)^{2^n}\\ a_{n+5}&=1\\ a_{n+6}&=2\\ a_{n+7}&=1+2^{2^n}-1\\ a_{n+8}&=\frac{\left(1+2^{2^n}-1\right)^{2^n}-1}{2}\\ a_{n+9}&=\left(1+2^{2^n}-1\right)^{2^n}-1\end{aligned}$$

Proof. The tuple $(a_1,\ldots,a_{n+9})$ consists of positive integers and solves the system of equations. We prove that this solution is unique in positive integers. The equations

$$\begin{aligned}x_{n+5}\cdot x_{n+5}&=x_{n+5}\\ x_{n+5}+1&=x_{n+6}\\ x_{n+6}\cdot x_{n+7}&=x_1\end{aligned}$$

imply that x_1 is even. The equations

$$\begin{aligned}x_{n+5}\cdot x_{n+5}&=x_{n+5}\\ x_{n+5}+1&=x_{n+6}\\ x_{n+6}\cdot x_{n+8}&=x_{n+9}\\ x_{n+9}+1&=x_{n+4}\end{aligned}$$

imply that x_{n+4} is odd. The equations

$$\begin{aligned}\forall i\in\{1,\ldots,n\}\ x_i\cdot x_i&=x_{i+1}\\ x_{n+2}+1&=x_1\\ x_{n+3}+1&=x_{n+2}\\ x_{n+3}\cdot x_{n+4}&=x_{n+1}\end{aligned}$$

imply that $x_1=x_{n+3}+2\geqslant 3$ and $x_1^{2^n}=(x_1-2)\cdot x_{n+4}$. This equality and the polynomial identity

$$x_1^{2^n}=2^{2^n}+(x_1-2)\cdot\left(2^{2^n-1}+\sum_{k=1}^{2^n-1}2^{2^n-1-k}\cdot x_1^k\right)$$

imply that x_1-2 divides 2^{2^n} and

$$x_{n+4}=\frac{x_1^{2^n}}{x_1-2}=\frac{2^{2^n}}{x_1-2}+\underbrace{2^{2^n-1}+\sum_{k=1}^{2^n-1}2^{2^n-1-k}\cdot x_1^k}_{\text{the sum of two even numbers as } x_1 \text{ is even}}\qquad (\mathrm{L})$$

Since $x_1\geqslant 3$ and x_1-2 divides 2^{2^n}, $x_1=2+2^k$, where $k\in\left[0,2^n\right]\cap\mathbb{Z}$. Since x_{n+4} is odd, the equality (L) implies that $\frac{2^{2^n}}{x_1-2}$ is odd. Hence, $x_1=2+2^{2^n}$. Consequently, $x_i=a_i$ for every $i\in\{1,\ldots,n+9\}$. □

Corollary 6. *The inequality $\xi(n)\geqslant\left(2+2^{2^{n-9}}\right)^{2^{n-9}}$ holds for every integer $n\geqslant 10$.*

Conjecture 4. *The equality $\xi(n)=\left(2+2^{2^{n-9}}\right)^{2^{n-9}}$ holds for every sufficiently large positive integer n.*

References

[1] Davis M., On the number of solutions of Diophantine equations, Proc. Amer. Math. Soc. 35 (1972), no. 2, 552–554.

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

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

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

[5] Matiyasevich Yu., Hilbert's tenth problem: what was done and what is to be done; in: Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math. 270, 1–47, Amer. Math. Soc., Providence, RI, 2000.

[6] Matiyasevich Yu., Towards finite-fold Diophantine representations, J. Math. Sci. (N. Y.) vol. 171, no. 6, 2010, 745–752.

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

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

[9] Smorynski C., A note on the number of zeros of polynomials and exponential polynomials, J. Symbolic Logic 42 (1977), no. 1, 99–106.

[10] Smorynski C., Logical number theory, vol. I, Springer, Berlin, 1991.

[11] Tyszka A., A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions, Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (eds. M. Ganzha, L. Maciaszek, M. Paprzycki); Annals of Computer Science and Information Systems, vol. 5, 709–716, IEEE Computer Society Press, 2015.

[12] Tyszka A., All functions $g\colon \mathbb{N} \to \mathbb{N}$ which have a single-fold Diophantine representation are dominated by a limit-computable function $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{N}$ which is implemented in *MuPAD* and whose computability is an open problem; in: Computation, cryptography, and network security (eds. N. J. Daras and M. Th. Rassias), Springer, Cham, Switzerland, 2015, 577–590.

[13] Tyszka A., Conjecturally computable functions which unconditionally do not have any finite-fold Diophantine representation, Inform. Process. Lett. 113 (2013), no. 19–21, 719–722.