Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 709–716

DOI: 10.15439/2015F41
ACSIS, Vol. 5

A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions

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**

$$f(n) = \begin{cases} 1 & \text{if} \quad n = 1 \\ 2^{2^{n-2}} & \text{if} \quad n \in \{2,3,4,5\} \\ \left(2 + 2^{2^{n-4}}\right)^{2^{n-4}} & \text{if} \quad n \in \{6,7,8,\ldots\} \end{cases}$$

We conjecture that if a system

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

has only finitely many solutions in positive integers $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $x_1,\ldots,x_n \leqslant f(n)$. We prove that the function f cannot be decreased and the conjecture implies that there is an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of integer (non-negative integer, positive integer, rational) solutions, if the solution set is finite. We show that if the conjecture is true, then this can be partially confirmed by the execution of a brute-force algorithm.

***Index Terms*—bound for integer solutions, Diophantine equation, finite-fold Diophantine representation, height of a solution, integer arithmetic.**

IN THIS article, we present a conjecture on integer arithmetic which implies a positive answer to all versions of the following open problem:

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

The height of a rational number $\frac{p}{q}$ is defined by $\max(|p|,|q|)$ provided $\frac{p}{q}$ is written in lowest terms. The height of a rational tuple $(x_1,\ldots,x_n)$ is defined as the maximum of n and the heights of the numbers $x_1,\ldots,x_n$.

Theorem 1. *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*

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

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

Theorem 2. *For each positive integer n, the following system*

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

is soluble in positive integers and has only finitely many integer solutions. Each integer solution $(x_1,\ldots,x_{n+4})$ satisfies $|x_1|,\ldots,|x_{n+4}| \leqslant \left(2+2^{2^n}\right)^{2^n}$. The maximal solution in positive integers is given by

$$\begin{cases} \forall i \in \{1,\ldots,n+1\}\ x_i &= \left(2+2^{2^n}\right)^{2^{i-1}} \\ x_{n+2} &= 1 + 2^{2^n} \\ x_{n+3} &= 2^{2^n} \\ x_{n+4} &= \left(1 + 2^{2^n} - 1\right)^{2^n} \end{cases}$$

Proof. The system equivalently expresses that $(x_1 - 2) \cdot x_{n+4} = x_1^{2^n}$. By this and the polynomial identity

$$x_1^{2^n} = 2^{2^n} + (x_1 - 2) \cdot \sum_{k=0}^{2^n - 1} 2^{2^n - 1 - k} \cdot x_1^k$$

we get that $x_{n+3} = x_1 - 2$ divides 2^{2^n} and $x_{n+4} = \dfrac{x_1^{2^n}}{x_1 - 2}$. Hence, $x_1 \in \left[2 - 2^{2^n}, 2 + 2^{2^n}\right] \cap \mathbb{Z}$, the system has only finitely many integer solutions, and $|x_1|,\ldots,|x_{n+4}| \leqslant \left(2+2^{2^n}\right)^{2^n}$. □

In [10, p. 719], the author proposed the upper bound $2^{2^{n-1}}$ for positive integer solutions to any system

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

which has only finitely many solutions in positive integers $x_1, \dots, x_n$. The bound $2^{2^{n-1}}$ is not correct for any $n \geqslant 8$ because the following system

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

provides a counterexample for any $k \geqslant 3$. In [11, p. 96], the author proposed the upper bound $2^{2^{n-1}}$ for modulus of integer solutions to any system

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

which has only finitely many solutions in integers $x_1, \dots, x_n$. The bound $2^{2^{n-1}}$ is not correct for any $n \geqslant 9$ because the following system

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

provides a counterexample for any $k \geqslant 4$. Let

$$f(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2^{2^{n-2}} & \text{if } n \in \{2, 3, 4, 5\} \\ \left(2 + 2^{2^{n-4}}\right)^{2^{n-4}} & \text{if } n \in \{6, 7, 8, \dots\} \end{cases}$$

Conjecture. *If a system*

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

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

Theorems 1 and 2 imply that the function f cannot be decreased. Let $\mathcal{R}ng$ denote the class of all rings $\boldsymbol{K}$ that extend $\mathbb{Z}$, and let

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

Th. Skolem proved that any Diophantine equation can be algorithmically transformed into an equivalent system of Diophantine equations of degree at most 2, see [6, pp. 2–3] and [2, pp. 3–4]. The following result strengthens Skolem's theorem.

Lemma 1. *([10, p. 720]) Let* $D(x_1, \dots, x_p) \in \mathbb{Z}[x_1, \dots, x_p]$. *Assume that* $\deg(D, x_i) \geqslant 1$ *for each* $i \in \{1, \dots, p\}$. *We can compute a positive integer* $n > p$ *and a system* $T \subseteq E_n$ *which satisfies the following two conditions:*

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

$$\forall \tilde{x}_1, \dots, \tilde{x}_p \in \boldsymbol{K} \; \Big(D(\tilde{x}_1, \dots, \tilde{x}_p) = 0 \Longleftrightarrow$$

$$\exists \tilde{x}_{p+1}, \dots, \tilde{x}_n \in \boldsymbol{K} \; (\tilde{x}_1, \dots, \tilde{x}_p, \tilde{x}_{p+1}, \dots, \tilde{x}_n) \text{ solves } T\Big)$$

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

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

For a positive integer n, let $S(n)$ denote the successor of n.

Lemma 2. *Let* T *be a finite system of equations of the forms:* $x = 1$, $x + y = z$, *and* $x \cdot y = z$. *If the equation* $x = 1$ *belongs to* T, *then the system* $T \cup \{x \cdot x = x\} \setminus \{x = 1\}$ *has the same solutions in positive integers.*

Lemma 3. *Let* T *be a finite system of equations of the forms:* $S(x) = y$, $x + y = z$, *and* $x \cdot y = z$. *If the equation* $x + y = z$ *belongs to* T *and the variables* z_1, z_2, $\widetilde{z_1}$, $\widetilde{z_2}$, $\widetilde{v}$, u, t, $\widetilde{t}$, v *are new, then the following system*

$$T \cup \{z \cdot x = z_1, \; z \cdot y = z_2, \; S(z_1) = \widetilde{z_1}, \; S(z_2) = \widetilde{z_2}, \; \widetilde{z_1} \cdot \widetilde{z_2} = \widetilde{v},$$

$$z \cdot z = u, \; x \cdot y = t, \; S(t) = \widetilde{t}, \; u \cdot \widetilde{t} = v, \; S(v) = \widetilde{v}\} \setminus \{x + y = z\}$$

has the same solutions in positive integers and a smaller number of additions.

Proof. According to [5, p. 100], for each positive integers x, y, z, $x + y = z$ if and only if

$$S(z \cdot x) \cdot S(z \cdot y) = S((z \cdot z) \cdot S(x \cdot y))$$

Indeed, the above equality is equivalent to

$$\left(z^2 \cdot x \cdot y + 1\right) + z \cdot (x + y) = \left(z^2 \cdot x \cdot y + 1\right) + z^2$$

□

Lemmas 1–3 imply the next theorem.

Theorem 3. *If we assume the Conjecture and a Diophantine equation* $D(x_1, \dots, x_p) = 0$ *has only finitely many solutions in positive integers, then an upper bound for these solutions can be computed.*

Corollary 1. *If we assume the Conjecture and a Diophantine equation* $D(x_1, \dots, x_p) = 0$ *has only finitely many solutions in non-negative integers, then an upper bound for these solutions can be computed by applying Theorem 3 to the equation* $D(x_1 - 1, \dots, x_p - 1) = 0$.

Corollary 2. *If we assume the Conjecture and a Diophantine equation* $D(x_1, \dots, x_p) = 0$ *has only finitely many integer solutions, then an upper bound for their modulus can be computed by applying Theorem 3 to the equation*

$$\prod_{(i_1, \dots, i_p) \in \{1, 2\}^p} D((-1)^{i_1} \cdot (x_1 - 1), \dots, (-1)^{i_p} \cdot (x_p - 1)) = 0$$

Lemma 4. *([10, p. 720]) If there is a computable upper bound for the modulus of integer solutions to a Diophantine equation with a finite number of integer solutions, then there is a computable upper bound for the heights of rational solutions to a Diophantine equation with a finite number of rational solutions.*

Theorem 4. *The Conjecture implies that there is a computable upper bound for the heights of rational solutions to a Diophantine equation with a finite number of rational solutions.*

Proof. It follows from Corollary 2 and Lemma 4. □

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

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

for some polynomial W with integer coefficients, see [2]. 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 [2]. 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 conjectures that each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a finite-fold Diophantine representation, see [1, pp. 341–342], [3, p. 42], and [4, p. 745]. Matiyasevich's conjecture implies a negative answer to the Problem, see [3, p. 42].

Theorem 5. *(cf. [10, p. 721]) The Conjecture implies that if a set $\mathcal{M} \subseteq \mathbb{N}$ has a finite-fold Diophantine representation, then $\mathcal{M}$ is computable.*

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

$$\forall b \in \mathbb{N} \left(b \in \mathcal{M} \Longleftrightarrow \exists x_1,\ldots,x_m \in \mathbb{N} \quad W(b,x_1,\ldots,x_m) = 0\right)$$

and for any $b \in \mathbb{N}$ the equation $W(b,x_1,\ldots,x_m) = 0$ has only finitely many solutions $(x_1,\ldots,x_m) \in \mathbb{N}^m$. By Corollary 1, there is a computable function $g\colon \mathbb{N} \to \mathbb{N}$ such that for each $b,x_1,\ldots,x_m \in \mathbb{N}$ the equality $W(b,x_1,\ldots,x_m) = 0$ implies $\max(x_1,\ldots,x_m) \leqslant g(b)$. 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 $[0,g(b)]^m$. □

In this paragraph, we follow [9] and we explain why Matiyasevich's conjecture although widely known is less widely accepted. Let us say that a set $\mathcal{M} \subseteq \mathbb{N}^n$ has a bounded Diophantine representation, if there exists a polynomial W with integer coefficients such that

$$(a_1,\ldots,a_n) \in \mathcal{M} \Longleftrightarrow \exists x_1,\ldots,x_m \in \{0,\ldots,\max(a_1,\ldots,a_n)\}$$
$$W(a_1,\ldots,a_n,x_1,\ldots,x_m) = 0$$

Of course, any bounded Diophantine representation is finite-fold and any subset of $\mathbb{N}$ with a bounded Diophantine representation is computable. A simple diagonal argument shows that there exists a computable subset of $\mathbb{N}$ without any bounded Diophantine representation, see [1, p. 360]. The authors of [1] suggest a possibility (which contradicts Matiyasevich's conjecture) that each subset of $\mathbb{N}$ which has a finite-fold Diophantine representation has also a bounded Diophantine representation, see [1, p. 360].

For a positive integer n, let $\tau(n)$ denote the smallest positive integer b such that for each system

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

with a finite number of solutions in positive integers $x_1,\ldots,x_n$, all these solutions belong to $[1,b]^n$. By Theorems 1 and 2, $f(n) \leqslant \tau(n)$ for every positive integer n. The Conjecture implies that $f(n) = \tau(n)$ for every positive integer n.

Theorem 6. *(cf. [9, Theorem 4]) If a function $h\colon \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ has a finite-fold Diophantine representation, then there exists a positive integer m such that $h(n) < \tau(n)$ 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,

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

and for each positive integers x_1,x_2 at most finitely many tuples $(x_3,\ldots,x_r)$ of positive integers satisfy $W(x_1,x_2,x_3-1,\ldots,x_r-1) = 0$. By Lemmas 1–3, there is an integer $s \geqslant 3$ such that for any positive integers x_1,x_2,

$$(x_1,x_2) \in h \Longleftrightarrow$$
$$\exists x_3,\ldots,x_s \in \mathbb{N} \setminus \{0\} \quad \Psi(x_1,x_2,x_3,\ldots,x_s) \qquad \texttt{(E)}$$

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 finitely many tuples $(x_3,\ldots,x_s)$ of positive integers satisfy $\Psi(x_1,x_2,x_3,\ldots,x_s)$. Let $[\cdot]$ denote the integer part function, and let an integer n is 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 with n variables:

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

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

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

Since T_n has at most finitely many solutions in positive integers, $y \leqslant \tau(n)$. Hence, $h(n) < \tau(n)$. □

Below is the excerpt from page 135 of the book [7]:

Folklore. If a Diophantine equation has only finitely many solutions then those solutions are small in 'height' when compared to the parameters of the equation.

This folklore is, however, only widely believed because of the large amount of experimental evidence which now exists to support it.

Below is the excerpt from page 12 of the article [8]:

Note that if a Diophantine equation is solvable, then we can prove it, since we will eventually find a solution by searching through the countably many possibilities (but we do not know beforehand how far we have to search). So the really hard problem is to prove that there are no solutions when this is the case. A similar problem arises when there are finitely many solutions and we want to find them all. In this situation one expects the solutions to be fairly small. So usually it is not so hard to find all solutions; what is difficult is to show that there are no others.

That is, mathematicians are intuitively persuaded that solutions are small when there are finitely many of them. It seems that there is a reason which is common to all the equations. Such a reason might be the Conjecture whose consequences we have already presented.

For a positive integer b, let $\Phi(b)$ denote the Conjecture restricted to systems whose all solutions in positive integers are not greater than b. Obviously,

$$\Phi(1) \Leftarrow \Phi(2) \Leftarrow \Phi(3) \Leftarrow \ldots$$

and the Conjecture is equivalent to $\forall b \in \mathbb{N} \setminus \{0\}\ \Phi(b)$. The Conjecture is true for $n = 1$ and $n = 2$. Therefore, the sentence $\Phi(4)$ is true. For each positive integer n, there are only finitely many systems

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

Hence, for each positive integer n there exists a positive integer m such that the Conjecture restricted to systems with at most n variables is equivalent to the sentence $\Phi(m)$.

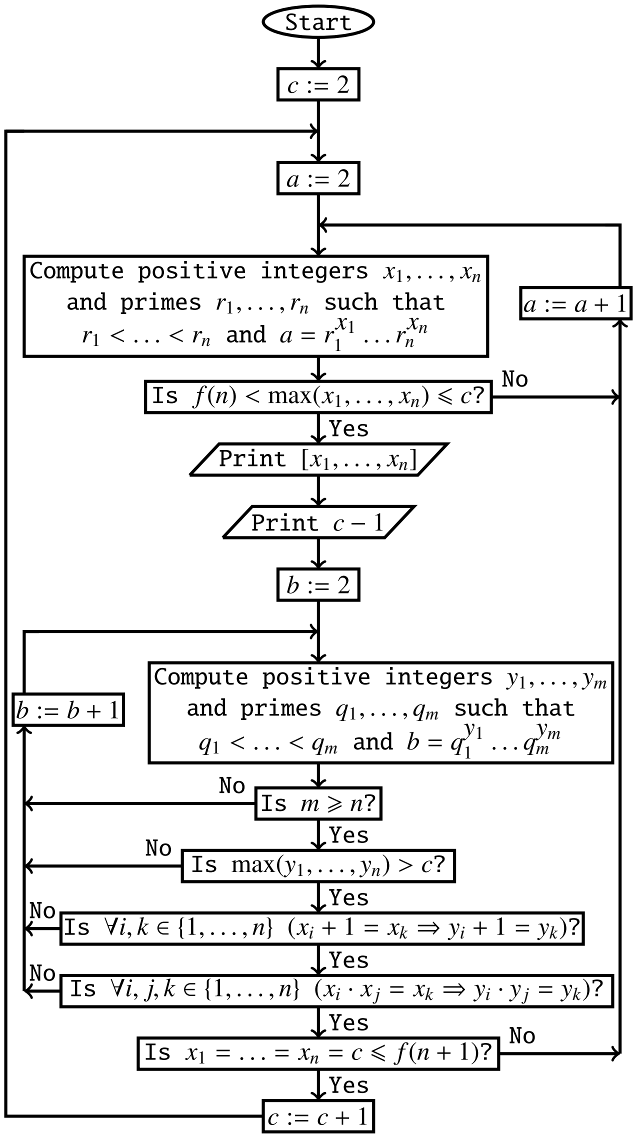
Theorem 7. *The Conjecture is equivalent to the following conjecture on integer arithmetic: if positive integers* $x_1, \ldots, x_n$ *satisfy* $\max(x_1, \ldots, x_n) > f(n)$, *then there exist positive integers* $y_1, \ldots, y_n$ *such that*

$$\Big(\max(x_1, \ldots, x_n) < \max(y_1, \ldots, y_n)\Big) \wedge$$

$$\Big(\forall i, k \in \{1, \ldots, n\}\ (x_i + 1 = x_k \Longrightarrow y_i + 1 = y_k)\Big) \wedge$$

$$\Big(\forall i, j, k \in \{1, \ldots, n\}\ (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k)\Big)$$

The execution of the following flowchart never terminates.



Theorem 8. *If the Conjecture is true, then the execution of the flowchart provides an infinite sequence* $X_1, c_1, X_2, c_2, X_3, c_3, \ldots$ *where* $\{c_1, c_2, c_3, \ldots\} = \mathbb{N} \setminus \{0\}$, $c_1 \leqslant c_2 \leqslant c_3 \leqslant \ldots$ *and each* X_i *is a tuple of positive integers. Each returned number* c_i *indicates that the performed computations confirm the sentence* $\Phi(c_i)$. *If the Conjecture is false, then the execution provides a similar finite sequence* $X_1, c_1, \ldots, X_k, c_k$ *on the output. In this case, for the tuple* $X_k = (x_1, \ldots, x_n)$ *an appropriate tuple* $(y_1, \ldots, y_n)$ *does not exist,* $\{c_1, \ldots, c_k\} = [1, c_k] \cap \mathbb{N}$, $c_1 \leqslant \ldots \leqslant c_k$, *the sentences* $\Phi(1), \Phi(2), \Phi(3), \ldots, \Phi(c_k)$ *are true, and the sentences* $\Phi(c_k + 1), \Phi(c_k + 2), \Phi(c_k + 3), \ldots$ *are false.*

Proof. Let p_n denote the n^{th} prime number ($p_1 = 2$, $p_2 = 3$, etc.), and let c stands for any integer greater than 1. The function f is strictly increasing and there exists the smallest positive integer n such that $c \leqslant f(n+1)$. Hence, if positive integers $x_1, \ldots, x_i$ satisfy $f(i) < \max(x_1, \ldots, x_i) \leqslant c$, then $i \leqslant n$ and $2 \leqslant p_1^{x_1} \ldots p_i^{x_i} \leqslant p_1^c \ldots p_n^c$. Therefore, if the sentence $\Phi(c)$ is true, then the flowchart algorithm checks all tuples of positive integers needed to confirm the sentence $\Phi(c)$. □

The following *MuPAD* code implements a simplified flowchart's algorithm which checks the following conjunction

$$\Big(m \geqslant n\Big) \wedge \Big(\max(y_1, \ldots, y_n) > c\Big) \wedge$$

$$\Big(\forall i, k \in \{1, \ldots, n\}\ (x_i + 1 = x_k \Longrightarrow y_i + 1 = y_k)\Big) \wedge$$

$$\Big(\forall i, j, k \in \{1, \ldots, n\}\ (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k)\Big)$$

instead of four separate conditions.

```
c:=2:
while TRUE do
a:=2:
repeat
S:=op(ifactor(a)):
n:=(nops(S)-1)/2:
u:=min(S[2*i+1] $i=1..n):
v:=max(S[2*i+1] $i=1..n):
X:=[S[2*i+1] $i=1..n]:
if n=1 then f:=1 end_if:
if n>1 then f:=2^(2^(n-2)) end_if:
if n>5 then f:=(2+2^(2^(n-4)))^(2^(n-4))
end_if:
g:=2^(2^(n-1)):
if n>4 then g:=(2+2^(2^(n-3)))^(2^(n-3))
end_if:
if f<v and v<=c then
print(X):
print(c-1):
b:=2:
repeat
T:=op(ifactor(b)):
m:=(nops(T)-1)/2:
Y:=[T[2*i+1] $i=1..m]:
r:=min(m-n+1,max(Y[i] $i=1..m)-c):
for i from 1 to min(n,m) do
for j from 1 to min(n,m) do
for k from 1 to min(n,m) do
if X[i]+1=X[k] and Y[i]+1<>Y[k] then
r:=0 end_if:
if X[i]*X[j]=X[k] and Y[i]*Y[j]<>Y[k] then
r:=0 end_if:
end_for:
end_for:
end_for:
b:=b+1:
until r>0 end_repeat:
end_if:
a:=a+1:
until c=u and c=v and c<=g end_repeat:
c:=c+1:
end_while:
```

We attempt to confirm the sentence $\Phi(256)$. Since the execution of the flowchart algorithm (or its any variant) proceeds slowly, we must confirm the sentence $\Phi(256)$ in a different way. For integers $a_1, \ldots, a_n$, let $P(a_1, \ldots, a_n)$ denote the following system of equations:

$$\begin{cases} x_i + 1 &= x_k \quad (\text{if } a_i + 1 = a_k) \\ x_i \cdot x_j &= x_k \quad (\text{if } a_i \cdot a_j = a_k) \end{cases}$$

Lemma 5. *For each positive integer n, there exist positive integers $a_1, \ldots, a_n$ such that $a_1 \leqslant \ldots \leqslant a_n = \tau(n)$ and the system $P(a_1, \ldots, a_n)$ has only finitely many solutions in positive integers. Each such numbers $a_1, \ldots, a_n$ satisfy $a_1 < \ldots < a_n$.*

Proof. If $a_1 < \ldots < a_n$ does not hold, then we remove the first duplicate and insert $a_n + 1$ after a_n. Since $a_n + 1 > a_n = \tau(n)$, we get a contradiction. □

Let $\mathcal{F}$ denote the family of all systems $P(a_1, a_2, a_3)$, where integers a_1, a_2, a_3 satisfy $1 < a_1 < a_2 < a_3$.

Theorem 9. *The Conjecture is true for $n = 3$.*

Proof. By Lemma 5, there exist positive integers a_1, a_2, a_3 such that $a_1 < a_2 < a_3 = \tau(3)$ and the system $P(a_1, a_2, a_3)$ has only finitely many solutions in positive integers. If $a_1 = 1$, then $a_2 = 2$ and $a_3 \in \{3, 4\}$. Let $a_1 > 1$. Since $a_1 < a_2 < a_3$, we get $a_1 \cdot a_1 < a_1 \cdot a_2 < a_2 \cdot a_2$. Hence,

$$\text{card}\Big(P(a_1, a_2, a_3) \cap \Big\{x_1 \cdot x_1 = x_3,\ x_1 \cdot x_2 = x_3,\ x_2 \cdot x_2 = x_3\Big\}\Big) \leqslant 1$$

Each integer a_1 satisfies $a_1 + 1 \neq a_1 \cdot a_1$. Hence,

$$\text{card}\Big(P(a_1, a_2, a_3) \cap \Big\{x_1 + 1 = x_2,\ x_1 \cdot x_1 = x_2\Big\}\Big) \leqslant 1$$

Since $a_1 < a_2 < a_3$, the equation $x_1 + 1 = x_3$ does not belong to $P(a_1, a_2, a_3)$. By these observations, the following table shows all solutions in positive integers to any system that belongs to $\mathcal{F}$.

	$\emptyset$	$\{x_1{\cdot}x_1{=}x_3\}$	$\{x_1{\cdot}x_2{=}x_3\}$	$\{x_2{\cdot}x_2{=}x_3\}$
$\emptyset \cup$	any triple (s,t,u) solves this system	any triple $\left(s,t,s^2\right)$ solves this system	any triple $(s,t,s{\cdot}t)$ solves this system	any triple $\left(s,t,t^2\right)$ solves this system
$\{x_1{+}1{=}x_2\} \cup$	any triple $(s,s{+}1,u)$ solves this system	any triple $\left(s,s{+}1,s^2\right)$ solves this system	any triple $(s,s{+}1,s{\cdot}(s{+}1))$ solves this system	any triple $\left(s,s{+}1,(s{+}1)^2\right)$ solves this system
$\{x_1{\cdot}x_1{=}x_2\} \cup$	any triple $\left(s,s^2,u\right)$ solves this system	$\notin \mathcal{F}$	any triple $\left(s,s^2,s^3\right)$ solves this system	any triple $\left(s,s^2,s^4\right)$ solves this system
$\{x_2{+}1{=}x_3\} \cup$	any triple $(s,t,t{+}1)$ solves this system	any triple $\left(s,s^2{-}1,s^2\right)$ solves this system	$\notin \mathcal{F}$	$\notin \mathcal{F}$
$\{x_1{+}1{=}x_2,\ x_2{+}1{=}x_3\} \cup$	any triple $(s,s{+}1,s{+}2)$ solves this system	only the triple $(2,3,4)$ solves this system	$\notin \mathcal{F}$	$\notin \mathcal{F}$
$\{x_1{\cdot}x_1{=}x_2,\ x_2{+}1{=}x_3\} \cup$	any triple $\left(s,s^2,s^2{+}1\right)$ solves this system	$\notin \mathcal{F}$	$\notin \mathcal{F}$	$\notin \mathcal{F}$

The table indicates that the system

$$\left\{x_1 + 1 = x_2,\ x_2 + 1 = x_3,\ x_1 \cdot x_1 = x_3\right\} =$$
$$\left\{x_1 + 1 = x_2,\ x_2 + 1 = x_3\right\} \cup \left\{x_1 \cdot x_1 = x_3\right\}$$

has a unique solution in positive integers, namely $(2,3,4)$. The other presented systems do not belong to $\mathcal{F}$ or have infinitely many solutions in positive integers. □

Corollary 3. *Since the Conjecture is true for* $n \in \{1,2,3\}$*, the sentence* $\Phi(16)$ *is true.*

Theorem 10. *The sentence* $\Phi(256)$ *is true.*

Proof. By Corollary 3, it suffices to consider quadruples of positive integers. The next *MuPAD* code returns 63 quadruples (a_i,b_i,c_i,d_i) of positive integers, where $a_i < b_i < c_i < d_i \leqslant 256$ and $\max(a_i,b_i,c_i,d_i) = d_i > 16$. These quadruples have the following property: if positive integers a,b,c,d satisfy $a < b < c < d \leqslant 256$ and $\max(a,b,c,d) = d > 16$, then there exists $i \in \{1,\dots,63\}$ such that $P(a,b,c,d) \subseteq P(a_i,b_i,c_i,d_i)$.

```
TEXTWIDTH:=60:
S:={}:
G:=[]:
T:={}:
H:=[]:
for a from 1 to 256 do
for b from 1 to 256 do
for c from 1 to 256 do
Y:=[1,a+1,a*a,a*b]:
for l from 1 to 4 do
X:=sort([a,b,c,Y[l]]):
u:=nops({a,b,c,Y[l]}):
v:=max(a,b,c,Y[l]):
if u=4 and 16<v and v<257 then
M:={}:
for i from 1 to 4 do
for j from i to 4 do
for k from 1 to 4 do
if X[i]+1=X[k] then
M:=M union {[i,k]} end_if:
if X[i]*X[j]=X[k] then
M:=M union {[i,j,k]} end_if:
end_for:
end_for:
end_for:
d:=nops(S union {M})-nops(S):
if d=1 then
S:=S union {M}:
G:=append(G,M):
T:=T union {X}:
H:=append(H,X):
end_if:
end_if:
end_for:
end_for:
end_for:
end_for:
for w from 1 to nops(G) do
for z from 1 to nops(G) do
p:=nops(G[w] minus G[z]):
q:=nops(G[z] minus G[w]):
if p=0 and 0<q then T:=T minus {H[w]}
end_if:
end_for:
end_for:
print(T):
```

The next table displays the quadruples $[a_1,b_1,c_1,d_1],\dots,[a_{63},b_{63},c_{63},d_{63}]$ and shows that for each $i \in \{1,\dots,63\}$ the system $P(a_i,b_i,c_i,d_i)$ has infinitely many solutions in positive integers, which completes the proof by Lemma 5. □

$(1, 2, 3, t)$ $[1, 2, 3, 17]$	$(1, 2, 4, t)$ $[1, 2, 4, 17]$	$(2, 3, 4, t)$ $[2, 3, 4, 17]$
$\left(t, t+1, t(t+1), t(t+1)^2\right)$ $[2, 3, 6, 18]$	$(1, 2, t, 2t)$ $[1, 2, 9, 18]$	$(1, t, t+1, t(t+1))$ $[1, 4, 5, 20]$
$\left(t, t^2, t^2+1, t^2\left(t^2+1\right)\right)$ $[2, 4, 5, 20]$	$\left(t, t+1, (t+1)^2, t(t+1)^2\right)$ $[2, 3, 9, 18]$	$(t, t+1, t+2, (t+1)(t+2))$ $[3, 4, 5, 20]$
$\left(1, 2, t, t^2\right)$ $[1, 2, 5, 25]$	$\left(1, t, t+1, (t+1)^2\right)$ $[1, 4, 5, 25]$	$(t, t+1, t+2, t(t+1))$ $[4, 5, 6, 20]$
$(1, 2, t, t+1)$ $[1, 2, 16, 17]$	$\left(t, t^2, t^2+1, \left(t^2+1\right)^2\right)$ $[2, 4, 5, 25]$	$\left(1, t, t+1, t^2\right)$ $[1, 5, 6, 25]$
$\left(t, t+1, t+2, (t+2)^2\right)$ $[3, 4, 5, 25]$	$\left(1, t, t^2, t^2+1\right)$ $[1, 4, 16, 17]$	$\left(t, t^2, t^4, t^4+1\right)$ $[2, 4, 16, 17]$
$(t, t+1, t+2, t(t+2))$ $[4, 5, 6, 24]$	$\left(1, t, t^2, t^3\right)$ $[1, 3, 9, 27]$	$\left(t, t+1, (t+1)^2, (t+1)^2+1\right)$ $[3, 4, 16, 17]$
$\left(t, t+1, t+2, (t+1)^2\right)$ $[4, 5, 6, 25]$	$\left(t, t+1, (t+1)^2, (t+1)^3\right)$ $[2, 3, 9, 27]$	$\left(t, t+1, t^2, t^2+1\right)$ $[4, 5, 16, 17]$
$\left(t, t+1, t^2, t^3\right)$ $[3, 4, 9, 27]$	$\left(t, t+1, t+2, t^2\right)$ $[5, 6, 7, 25]$	$\left(t, t^2-1, t^2, t\left(t^2-1\right)\right)$ $[3, 8, 9, 24]$
$\left(t, t+1, t^2, t(t+1)\right)$ $[4, 5, 16, 20]$	$\left(t, t^2, t^3, t^5\right)$ $[2, 4, 8, 32]$	$\left(t, t+1, t(t+1), t^2(t+1)^2\right)$ $[2, 3, 6, 36]$
$\left(t, t^2-1, t^2, t^3\right)$ $[3, 8, 9, 27]$	$(t, t+1, t(t+1)-1, t(t+1))$ $[4, 5, 19, 20]$	$(1, t, t+1, t+2)$ $[1, 15, 16, 17]$
$\left(t, t^2, t^2+1, t^3\right)$ $[3, 9, 10, 27]$	$\left(t, t+1, t^2, (t+1)^2\right)$ $[4, 5, 16, 25]$	$(t, t+1, t(t+1), t(t+1)+1)$ $[4, 5, 20, 21]$
$\left(t, t+1, t^2, (t+1)t^2\right)$ $[3, 4, 9, 36]$	$\left(t, t^2, t^2+1, t\left(t^2+1\right)\right)$ $[3, 9, 10, 30]$	$\left(t, t^2-1, t^2, t^2+1\right)$ $[4, 15, 16, 17]$
$\left(t, t^2, t^4, t^5\right)$ $[2, 4, 16, 32]$	$\left(t, t+1, t(t+1), (t+1)^2\right)$ $[4, 5, 20, 25]$	$\left(1, t, t^2-1, t^2\right)$ $[1, 5, 24, 25]$
$\left(t, t+1, t(t+1), t^2(t+1)\right)$ $[3, 4, 12, 36]$	$\left(t, t^2, t^2+1, t^2+2\right)$ $[4, 16, 17, 18]$	$\left(t, t+1, (t+1)^2-1, (t+1)^2\right)$ $[4, 5, 24, 25]$
$\left(t, t+1, t^2-1, t^2\right)$ $[5, 6, 24, 25]$	$(t, t+1, t+2, t+3)$ $[14, 15, 16, 17]$	$\left(t, t^2, t^3-1, t^3\right)$ $[3, 9, 26, 27]$
$\left(t, t^2, t^3, t^3+1\right)$ $[3, 9, 27, 28]$	$\left(t, t^2-2, t^2-1, t^2\right)$ $[5, 23, 24, 25]$	$\left(t, t^2, t^3, t^6\right)$ $[2, 4, 8, 64]$
$\left(t, t^2-1, t^2, \left(t^2-1\right)^2\right)$ $[3, 8, 9, 64]$	$\left(t, t^2, t^4, t^6\right)$ $[2, 4, 16, 64]$	$\left(t, t^2-1, t^2, \left(t^2-1\right)t^2\right)$ $[3, 8, 9, 72]$
$\left(t^2, t^3, t^4, t^6\right)$ $[4, 8, 16, 64]$	$\left(1, t, t^2, t^4\right)$ $[1, 3, 9, 81]$	$\left(t, t+1, (t+1)^2, (t+1)^4\right)$ $[2, 3, 9, 81]$
$\left(t, t+1, t^2, t^4\right)$ $[3, 4, 9, 81]$	$\left(t, t^2-1, t^2, t^4\right)$ $[3, 8, 9, 81]$	$\left(t, t^2, t^2+1, t^4\right)$ $[3, 9, 10, 81]$
$\left(t, t^2, t^3, t^4\right)$ $[3, 9, 27, 81]$	$\left(t, t^2, t^4-1, t^4\right)$ $[3, 9, 80, 81]$	$\left(t, t^2, t^4, t^8\right)$ $[2, 4, 16, 256]$

Of course, the Conjecture restricted to integers $n \in \{1,2,3,4\}$ is intuitively obvious and implies Theorem 10. Formally, the Conjecture remains unproven for $n = 4$. We explain why a hypothetical brute-force proof of the Conjecture for $n = 4$ is much longer than the proof of Theorem 10. By Lemma 5, it suffices to consider only the systems $P(a,b,c,d)$, where positive integers a,b,c,d satisfy $a < b < c < d$.

`Case 1:` $a = 1$. Obviously,

$$\mathrm{card}\Big(\big\{x_1 + 1 = x_2\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

and

$$\mathrm{card}\Big(\big\{x_3 + 1 = x_4\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $b + 1 < b \cdot b$, we get

$$\mathrm{card}\Big(\big\{x_2 + 1 = x_3,\ x_2 \cdot x_2 = x_3\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $b \cdot b < b \cdot c < c \cdot c$, we get

$$\mathrm{card}\Big(\big\{x_2 \cdot x_2 = x_4,\ x_2 \cdot x_3 = x_4,\ x_3 \cdot x_3 = x_4\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

The above inequalities allow one to determine $(1+1) \cdot (1+1) \cdot (2+1) \cdot (3+1) = 48$ systems which need to be solved.

`Case 2:` $a > 1$. Obviously,

$$\mathrm{card}\Big(\big\{x_2 + 1 = x_3\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $a + 1 < a \cdot a$, we get

$$\mathrm{card}\Big(\big\{x_1 + 1 = x_2,\ x_1 \cdot x_1 = x_2\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $c + 1 < a \cdot c$, we get

$$\mathrm{card}\Big(\big\{x_3 + 1 = x_4,\ x_1 \cdot x_3 = x_4\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $a \cdot a < a \cdot b < b \cdot b$, we get

$$\mathrm{card}\Big(\big\{x_1 \cdot x_1 = x_3,\ x_1 \cdot x_2 = x_3,\ x_2 \cdot x_2 = x_3\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

Since $a \cdot a < a \cdot b < b \cdot b < b \cdot c < c \cdot c$, we get

$$\mathrm{card}\Big(\big\{x_1 \cdot x_1 = x_4,\ x_1 \cdot x_2 = x_4,\ x_2 \cdot x_2 = x_4, \\ x_2 \cdot x_3 = x_4,\ x_3 \cdot x_3 = x_4\big\} \cap P(a,b,c,d)\Big) \leqslant 1$$

The above inequalities allow one to determine $(1+1) \cdot (2+1) \cdot (2+1) \cdot (3+1) \cdot (5+1) = 432$ systems which need to be solved.

MuPAD is a computer algebra system whose syntax is modelled on *Pascal*. The commercial version of *MuPAD* is no longer available as a stand-alone product, but only as the *Symbolic Math Toolbox* of *MATLAB*. Fortunately, the presented codes can be executed by *MuPAD Light*, which was offered for free for research and education until autumn 2005.

References

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

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

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

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

[5] J. Robinson, *Definability and decision problems in arithmetic,* J. Symbolic Logic 14 (1949), 98–114; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., 1996, 7–23.

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

[7] N. P. Smart, *The algorithmic resolution of Diophantine equations,* Cambridge University Press, Cambridge, 1998, http://dx.doi.org/10.1017/CBO9781107359994.

[8] M. Stoll, *How to solve a Diophantine equation,* in: An invitation to mathematics: From competitions to research (eds. M. Lackmann and D. Schleicher), Springer, Berlin-Heidelberg-New York, 2011, 9–19, http://dx.doi.org/10.1007/978-3-642-19533-4_2.

[9] A. Tyszka, *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, Berlin-Heidelberg-New York, 2015, 577–590, http://dx.doi.org/10.1007/978-3-319-18275-9_24.

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

[11] A. Tyszka, *Does there exist an algorithm which to each Diophantine equation assigns an integer which is greater than the modulus of integer solutions, if these solutions form a finite set?* Fund. Inform. 125 (2013), no. 1, 95–99, http://dx.doi.org/10.3233/FI-2013-854.