A new proof of Smoryński's theorem

Apoloniusz Tyszka

Abstract. We prove: (1) the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable, (2) the set of all Diophantine equations which have at most finitely many solutions in positive integers is not recursively enumerable, (3) the set of all Diophantine equations which have at most finitely many integer solutions is not recursively enumerable, (4) analogous theorems hold for Diophantine equations $D(x_1, \ldots, x_p) = 0$, where $p \in \mathbb{N} \setminus \{0\}$ and for every $i \in \{1, \ldots, p\}$ the polynomial $D(x_1, \ldots, x_p)$ involves a monomial $\mathcal{M}$ with a non-zero coefficient such that x_i divides $\mathcal{M}$, (5) the set of all Diophantine equations which have at most k variables (where $k \geqslant 9$) and at most finitely many solutions in non-negative integers is not recursively enumerable.

Key words and phrases: Davis-Putnan Robinson-Matiyasevich theorem, Diophantine equation which has at most finitely many solutions in non-negative integers, Diophantine equation which has at most finitely many solutions in positive integers, Diophantine equation which has at most finitely many integer solutions, Hilbert's Tenth Problem, Matiyasevich's theorem, recursively enumerable set, Smoryński's theorem.

2010 Mathematics Subject Classification: 03D25, 11U05.

There is no algorithm to decide whether or not a given Diophantine equation has an integer solution ([4]). The same is true for solutions in non-negative integers and for solutions in positive integers ([4]). The set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable, see [5, p. 104, Corollary 1] and [6, p. 240]. Let $\mathcal{E}$ denote the set of all Diophantine equations $D(x_1, \ldots, x_p) = 0$ such that $p \in \mathbb{N} \setminus \{0\}$ and the polynomial $D(x_1, \ldots, x_p)$ truly depends on all the variables $x_1, \ldots, x_p$. The last phrase means that for every $i \in \{1, \ldots, p\}$ the polynomial $D(x_1, \ldots, x_p)$ involves a monomial $\mathcal{M}$ with a non-zero coefficient such that x_i divides $\mathcal{M}$.

Lemma 1. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers $x_1, \ldots, x_p$ if and only if the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_{p+1}$.*

Lemma 1a. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers $x_1, \ldots, x_p$ if and only if the equation $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p) = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_{p+1}$.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 September 2017 doi:10.20944/preprints201709.0127.v2

Lemma 2. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in positive integers $x_1, \ldots, x_p$ if and only if the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in positive integers $x_1, \ldots, x_{p+1}$.*

Lemma 2a. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in positive integers $x_1, \ldots, x_p$ if and only if the equation $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p) = 0$ has at most finitely many solutions in positive integers $x_1, \ldots, x_{p+1}$.*

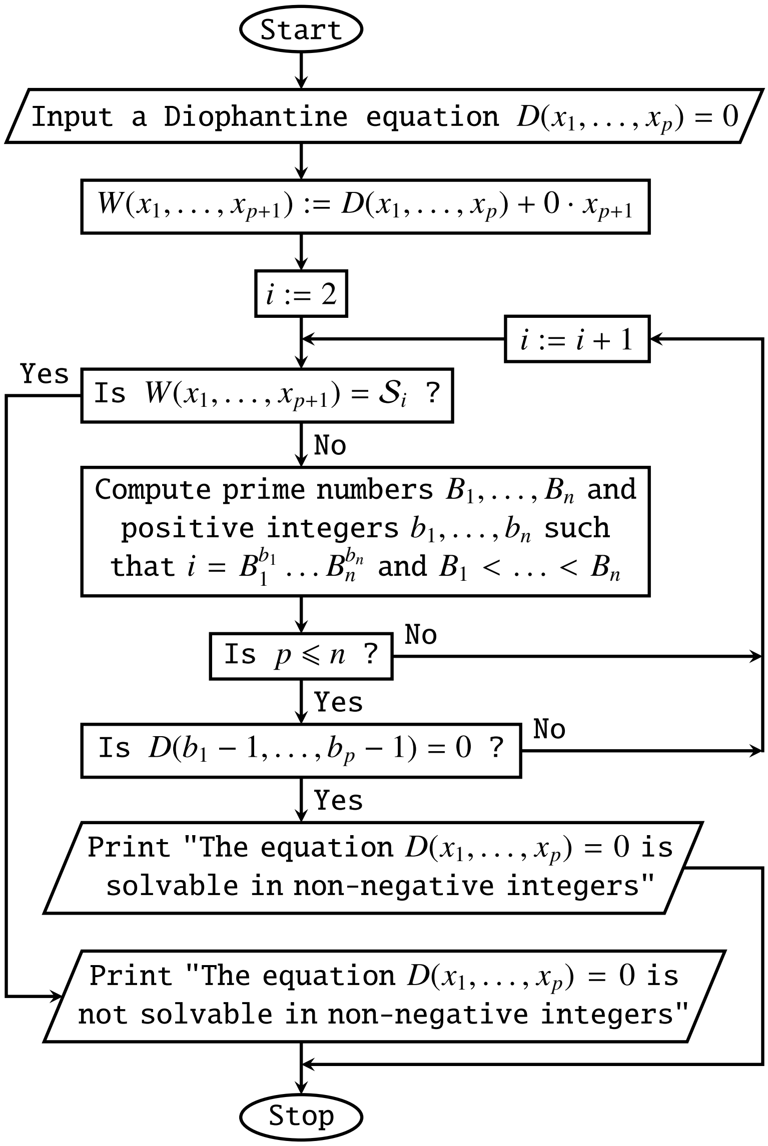
Lemma 3. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in integers $x_1, \ldots, x_p$ if and only if the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in integers $x_1, \ldots, x_{p+1}$.*

Lemma 3a. *A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in integers $x_1, \ldots, x_p$ if and only if the equation $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p) = 0$ has at most finitely many solutions in integers $x_1, \ldots, x_{p+1}$.*

Lemma 4. *If a polynomial $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$ truly depends on all the variables $x_1, \ldots, x_p$, then the polynomial $\left(2x_{p+1} + 1\right) \cdot D(x_1, \ldots, x_p)$ truly depends on all the variables $x_1, \ldots, x_{p+1}$.*

Theorem 1. *If the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in non-negative integers.*

Proof. Suppose that $\{S_i = 0\}_{i=2}^{\infty}$ is a computable sequence of all Diophantine equations which have at most finitely many solutions in non-negative integers. The algorithm presented in Flowchart 1 uses a computable surjection from $\mathbb{N} \setminus \{0, 1\}$ onto $\mathbb{N}^p$. By this and Lemma 1, the execution of Flowchart 1 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has a solution in non-negative integers.



Flowchart 1

□

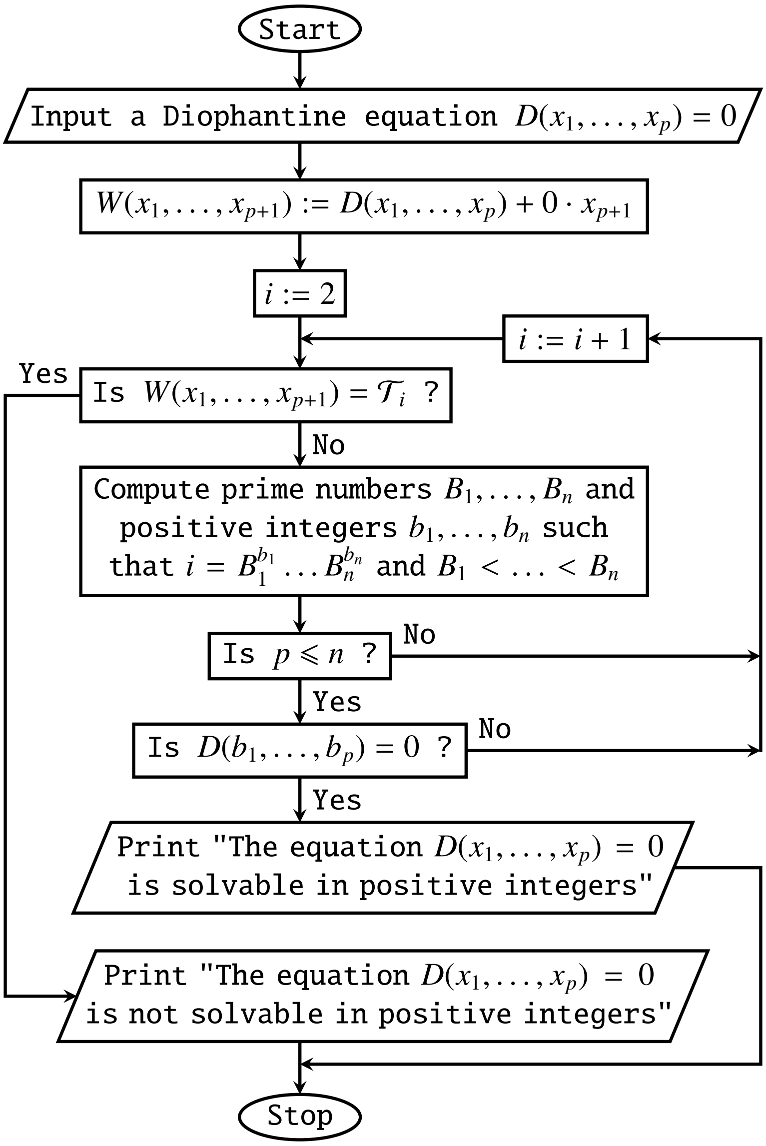
Corollary 1. *By Matiyasevich's theorem, the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable.*

Theorem 2. *The analogous reasoning with Lemmas 1a and 4 shows that the set of all equations from $\mathcal{E}$ which have at most finitely many solutions in non-negative integers is not recursively enumerable.*

Theorem 3. *If the set of all Diophantine equations which have at most finitely many solutions in positive integers is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in positive integers.*

 doi:10.20944/preprints201709.0127.v2

Proof. Suppose that $\{\mathcal{T}_i = 0\}_{i=2}^{\infty}$ is a computable sequence of all Diophantine equations which have at most finitely many solutions in positive integers. The algorithm presented in Flowchart 2 uses a computable surjection from $\mathbb{N} \setminus \{0, 1\}$ onto $(\mathbb{N} \setminus \{0\})^p$. By this and Lemma 2, the execution of Flowchart 2 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has a solution in positive integers.



Flowchart 2

□

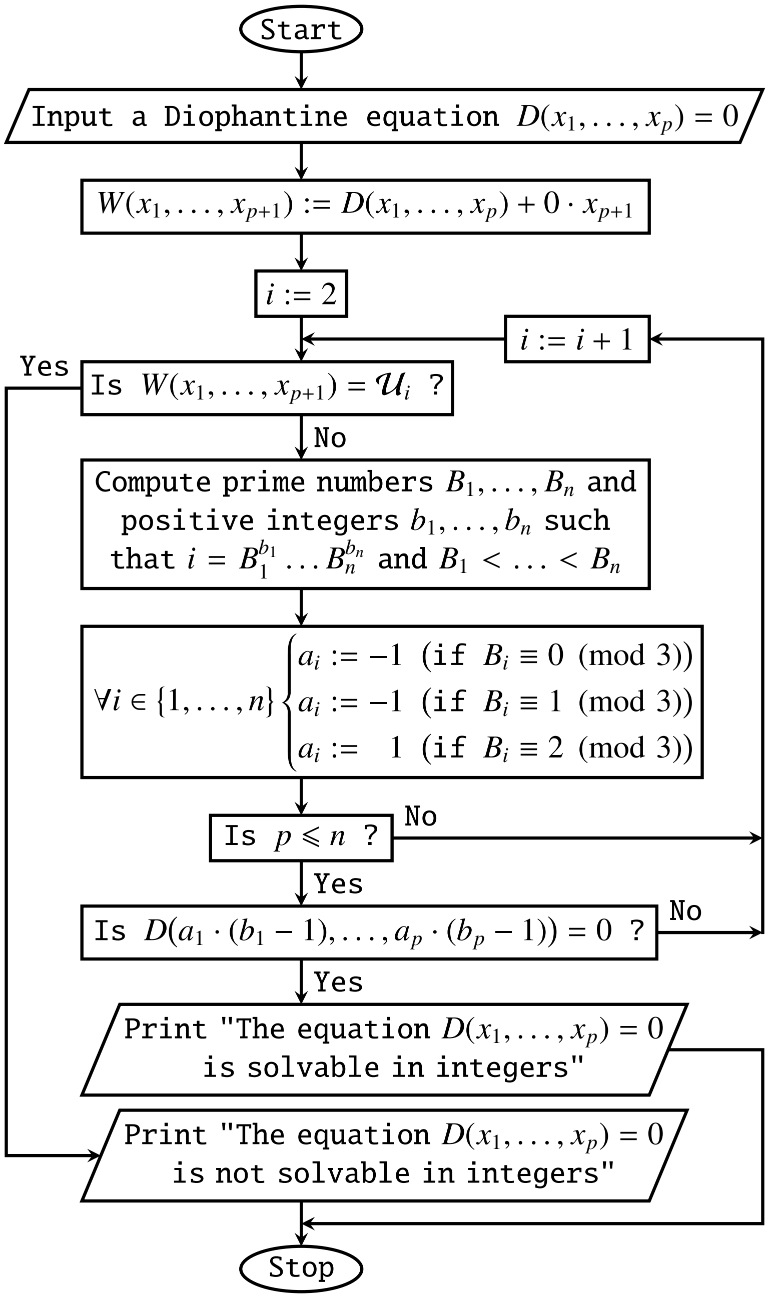
Corollary 2. *By Matiyasevich's theorem, the set of all Diophantine equations which have at most finitely many solutions in positive integers is not recursively enumerable.*

Theorem 4. *The analogous reasoning with Lemmas 2a and 4 shows that the set of all equations from $\mathcal{E}$ which have at most finitely many solutions in positive integers is not recursively enumerable.*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 September 2017 doi:10.20944/preprints201709.0127.v2

Theorem 5. *If the set of all Diophantine equations which have at most finitely many integer solutions is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has an integer solution.*

Proof. Suppose that $\{\mathcal{U}_i = 0\}_{i=2}^{\infty}$ is a computable sequence of all Diophantine equations which have at most finitely many integer solutions. There are infinitely many prime numbers of the form $3k+1$ and there are infinitely many prime numbers of the form $3k+2$, see [1, p. 80]. Hence, the algorithm presented in Flowchart 3 uses a computable surjection from $\mathbb{N} \setminus \{0,1\}$ onto $\mathbb{Z}^p$. By this and Lemma 3, the execution of Flowchart 3 decides whether or not a Diophantine equation $D(x_1,\ldots,x_p)=0$ has an integer solution.



Flowchart 3

□

 doi:10.20944/preprints201709.0127.v2

Corollary 3. *By Matiyasevich's theorem, the set of all Diophantine equations which have at most finitely many integer solutions is not recursively enumerable.*

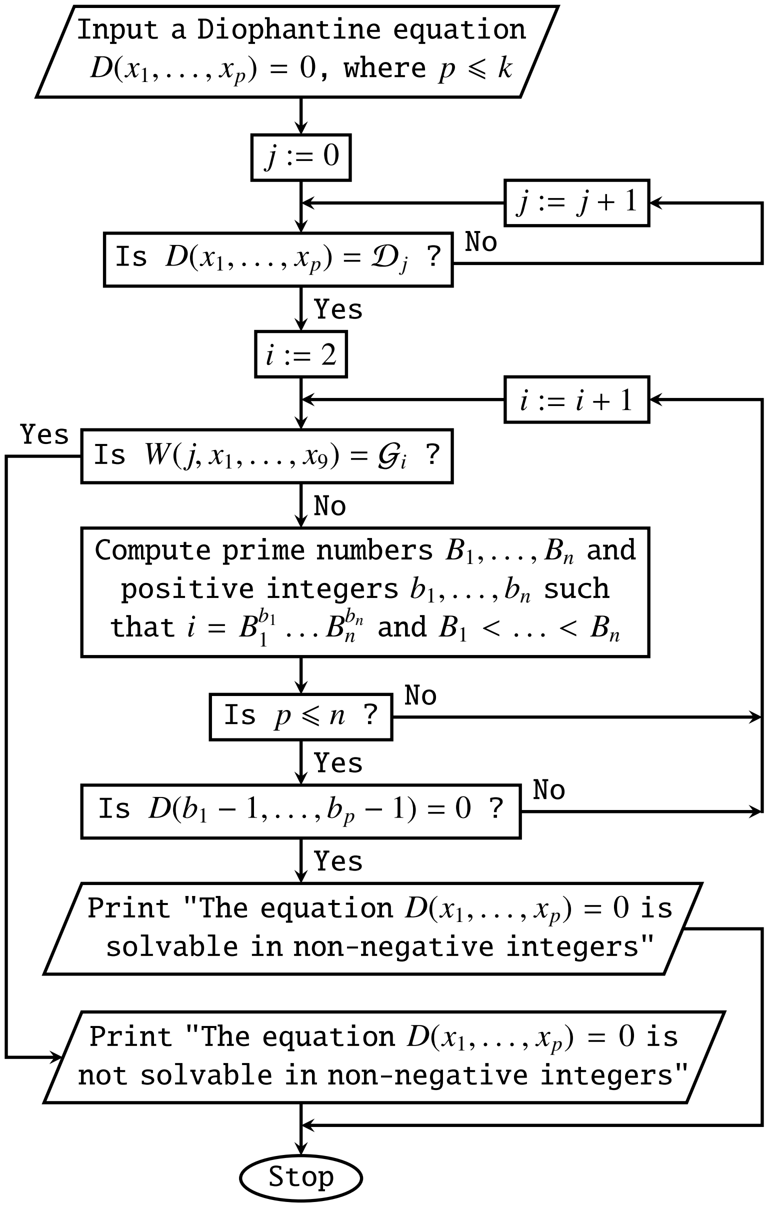
Theorem 6. *The analogous reasoning with Lemmas 3a and 4 shows that the set of all equations from $\mathcal{E}$ which have at most finitely many integer solutions is not recursively enumerable.*

For a positive integer k, let $Dioph(k)$ denote the set of all Diophantine equations which have at most k variables and at most finitely many solutions in non-negative integers.

Theorem 7. *For every integer $k \geqslant 9$, the set $Dioph(k)$ is not recursively enumerable.*

Proof. Let $\{D_j = 0\}_{j=0}^{\infty}$ be a computable sequence of all Diophantine equations which have at most k variables. A stronger version of the Davis-Putnam-Robinson-Matiyasevich theorem states that each recursively enumerable subset of $\mathbb{N}$ has an infinite-fold Diophantine representation with 9 variables, see [2], [3], [4, p. 163], and [6, p. 243]. By applying this theorem, there exists a polynomial $W(x, x_1, \ldots, x_9) \in \mathbb{Z}[x, x_1, \ldots, x_9]$ such that for every non-negative integer j, the equation $D_j = 0$ is solvable in non-negative integers if and only if the equation $W(j, x_1, \ldots, x_9) = 0$ has infinitely many solutions in non-negative integers $x_1, \ldots, x_9$. Equivalently, for every non-negative integer j, the equation $D_j = 0$ has no solutions in non-negative integers if and only if the equation $W(j, x_1, \ldots, x_9) = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_9$. Suppose, on the contrary, that $\{\mathcal{G}_i = 0\}_{i=2}^{\infty}$ is a computable sequence of all equations from $Dioph(k)$. Then, the execution of Flowchart 4 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ (where $p \leqslant k$) has a solution in non-negative integers $x_1, \ldots, x_p$. Thus we have a contradiction to Matiyasevich's theorem.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 September 2017 doi:10.20944/preprints201709.0127.v2



Flowchart 4

□

References

[1] B. Fine and G. Rosenberger, *Number theory: An introduction via the distribution of primes,* Birkhäuser, Boston, MA, 2007.

[2] J. P. Jones, *Universal Diophantine equation*, J. Symbolic Logic 47 (1982), no. 3, 549–571.

[3] Yu. Matiyasevich, *Some purely mathematical results inspired by mathematical logic,* in: Proceedings of Fifth International Congress on Logic, Methodology and Philosophy of Science, London, Ontario, 1975, Reidel, Dordrecht, 1977, 121-127.

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

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

[6] C. Smoryński, *Logical number theory, vol. I,* Springer, Berlin, 1991.

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