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 $M$ with a non-zero coefficient such that $x_i$ divides $M$, (5) the set of all Diophantine equations which have at most $k$ variables (where $k \geq 9$) 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.
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.
Input a Diophantine equation \(D(x_1, \ldots, x_p) = 0\)

\[ W(x_1, \ldots, x_{p+1}) := D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} \]

\[ i := 2 \]

Yes

Is \(W(x_1, \ldots, x_{p+1}) = S_i\) ?

No

Compute prime numbers \(B_1, \ldots, B_n\) and positive integers \(b_1, \ldots, b_n\) such that \(i = B_1^{b_1} \cdots B_n^{b_n}\) and \(B_1 < \ldots < B_n\)

Is \(p \leq n\) ?

No

Is \(D(b_1 - 1, \ldots, b_p - 1) = 0\) ?

No

Yes

Print "The equation \(D(x_1, \ldots, x_p) = 0\) is solvable in non-negative integers"

Yes

Print "The equation \(D(x_1, \ldots, x_p) = 0\) is not solvable in non-negative integers"

Stop

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 \(E\) 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.
Proof. Suppose that \( \{T_i = 0\}_{i=2}^{\infty} \) 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**

Start

Input a Diophantine equation \( D(x_1, \ldots, x_p) = 0 \)

\[ W(x_1, \ldots, x_{p+1}) := D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} \]

\[ i := 2 \]

Yes

Is \( W(x_1, \ldots, x_{p+1}) = T_i \)?

No

Compute prime numbers \( B_1, \ldots, B_n \) and positive integers \( b_1, \ldots, b_n \) such that \( i = B_1^{b_1} \cdots B_n^{b_n} \) and \( B_1 < \ldots < B_n \)

Is \( p \leq n \)?

No

Is \( D(b_1, \ldots, b_p) = 0 \)?

No

Yes

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is solvable in positive integers"

Stop

Yes

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is not solvable in positive integers"

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 \( E \) which have at most finitely many solutions in positive integers is not recursively enumerable.
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 \( \{ U_i = 0 \}_{i=2}^{\infty} \) 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.

Start

Input a Diophantine equation \( D(x_1, \ldots, x_p) = 0 \)

\[ W(x_1, \ldots, x_{p+1}) := D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} \]

\[ i := 2 \]

Yes

Is \( W(x_1, \ldots, x_{p+1}) = U_i \)?

No

Compute prime numbers \( B_1, \ldots, B_n \) and positive integers \( b_1, \ldots, b_n \) such that \( i = B_1^{b_1} \cdots B_n^{b_n} \) and \( B_1 < \ldots < B_n \)

\[ \forall i \in \{1, \ldots, n\} \quad \begin{cases} a_i := -1 \quad (\text{if } B_i \equiv 0 \pmod{3}) \\ a_i := -1 \quad (\text{if } B_i \equiv 1 \pmod{3}) \\ a_i := 1 \quad (\text{if } B_i \equiv 2 \pmod{3}) \end{cases} \]

Is \( p \leq n \)?

Yes

Is \( D(a_1 \cdot (b_1 - 1), \ldots, a_p \cdot (b_p - 1)) = 0 \)?

Yes

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is solvable in integers"

No

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is not solvable in integers"

Stop

Flowchart 3
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 $\text{Dioph}(k)$ 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 $k \geq 9$, the set $\text{Dioph}(k)$ 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 $\{G_i = 0\}_{i=2}^{\infty}$ is a computable sequence of all equations from $\text{Dioph}(k)$. Then, the execution of Flowchart 4 decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ (where $p \leq k$) has a solution in non-negative integers $x_1, \ldots, x_p$. Thus we have a contradiction to Matiyasevich’s theorem.
Input a Diophantine equation
\[ D(x_1, \ldots, x_p) = 0, \text{ where } p \leq k \]

\[ j := 0 \]

Is \( D(x_1, \ldots, x_p) = D_j \)?

No

\[ j := j + 1 \]

Yes

\[ i := 2 \]

Is \( W(j, x_1, \ldots, x_9) = G_i \)?

No

Yes

\[ i := i + 1 \]

Compute prime numbers \( B_1, \ldots, B_n \) and positive integers \( b_1, \ldots, b_n \) such that \( i = B_1^{b_1} \ldots B_n^{b_n} \) and \( B_1 < \ldots < B_n \)

Is \( p \leq n \)?

No

Is \( D(b_1 - 1, \ldots, b_p - 1) = 0 \)?

No

Yes

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is not solvable in non-negative integers"

Yes

Print "The equation \( D(x_1, \ldots, x_p) = 0 \) is solvable in non-negative integers"

Stop

Flowchart 4

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