On the Relationship Between
Matiyasevich’s and Smoryński’s Theorems

Agnieszka Peszek\textsuperscript{1}, Apoloniusz Tyszka\textsuperscript{2}

Abstract

Let $R$ be a non-zero subring of $\mathbb{Q}$ with or without 1. We assume that for every positive integer $n$ there exists a computable surjection from $\mathbb{N}$ onto $R^n$. Every $R \in \{\mathbb{Z}, \mathbb{Q}\}$ satisfies these conditions. Matiyasevich’s theorem states that there is no algorithm to decide whether or not a given Diophantine equation has a solution in non-negative integers. Smoryński’s theorem states that the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable. We prove: (1) Smoryński’s theorem easily follows from Matiyasevich’s theorem, (2) Hilbert’s Tenth Problem for solutions in $R$ has a positive solution if and only if the set of all Diophantine equations with a finite number of solutions in $R$ is recursively enumerable. “Hilbert’s Tenth Problem for solutions in $R$” is the problem of whether there exists an algorithm which for any given Diophantine equation with integer coefficients, can decide whether the equation has a solution with all unknowns taking values in $R$.

Keywords: computable set, Davis-Putnam-Robinson-Matiyasevich theorem, Diophantine equation which has at most finitely many solutions, Hilbert’s Tenth Problem for solutions in a subring of $\mathbb{Q}$, Matiyasevich’s theorem, recursively enumerable set, Smoryński’s theorem.

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License

\textsuperscript{1}University of Agriculture, Faculty of Production and Power Engineering, Balicka 116B, 30-149 Kraków, Poland, Email: Agnieszka.Peszek@urk.edu.pl

\textsuperscript{2}University of Agriculture, Faculty of Production and Power Engineering, Balicka 116B, 30-149 Kraków, Poland, Email: rttyszka@cyf-kr.edu.pl
1 Introduction

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

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

(R)

for some polynomial $W$ with integer coefficients, see [7]. The representation (R) is said to be infinite-fold if for every $a \in \mathcal{M}$ the equation $W(a, x_1, \ldots, x_m) = 0$ has infinitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$. 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 [4], [6], [7, p. 163], and [11, p. 243].

Martin Davis’ theorem states that the set of all Diophantine equations which have at most finitely many solutions in positive integers is not recursive, see [1]. Craig Smoryński’s theorem states that the set of all Diophantine equations which have at most finitely many solutions in non-negative integers is not recursively enumerable, see [10, p. 104, Corollary 1] and [11, p. 240]. Yuri Matiyasevich’s theorem states that there is no algorithm to decide whether or not a given Diophantine equation has a solution in non-negative integers [7]. The same is true for solutions in integers and for solutions in positive integers [7].

Matiyasevich’s theorem easily follows from the Davis-Putnam-Robinson-Matiyasevich theorem without the use of Smoryński’s theorem [7]. Similarly, the stronger version of the Davis-Putnam-Robinson-Matiyasevich theorem implies that Matiyasevich’s theorem holds for Diophantine equations which have at most $k$ variables, where $k \geq 9$, see [7]. In section 3, we show that Smoryński’s theorem easily follows from Matiyasevich’s theorem.

Let $R$ be a non-zero subring of $\mathbb{Q}$ with or without 1. We assume that for every positive integer $n$ there exists a computable surjection from $\mathbb{N}$ onto $R^n$. Every $R \in \{\mathbb{Z}, \mathbb{Q}\}$ satisfies these conditions. In section 4, we show that Hilbert’s Tenth Problem for solutions in $R$ has a positive solution if and only if the set of all Diophantine equations with a finite number of solutions in $R$ is recursively enumerable. “Hilbert’s Tenth Problem for solutions in $R$” is the problem of whether there exists an algorithm which for any given Diophantine equation with integer coefficients, can decide whether the equation has a solution with all unknowns taking values in $R$. 
2 Basic Lemmas

Let $\mathcal{P}$ denote the set of prime numbers, and let

$$\mathcal{P} = \{p_1, q_1, r_1, p_2, q_2, r_2, p_3, q_3, r_3, \ldots\},$$

where $p_1 < q_1 < r_1 < p_2 < q_2 < r_2 < p_3 < q_3 < r_3 < \ldots$.

**Lemma 1** For a non-negative integer $x$, let $\prod_{i=1}^{\infty} p_i^{\alpha_i} \cdot q_i^{\beta_i} \cdot r_i^{\gamma_i}$ be the prime decomposition of $x + 1$. For every positive integer $n$, the mapping which sends $x \in \mathbb{N}$ into

$$\left((-1)^{\alpha_1} \cdot \frac{\beta_1}{\gamma_1 + 1}, \ldots, (-1)^{\alpha_n} \cdot \frac{\beta_n}{\gamma_n + 1}\right) \in \mathbb{Q}^n$$

is a computable surjection from $\mathbb{N}$ onto $\mathbb{Q}^n$.

**Lemma 2** (cf. [8, Lemma 15, p. 257]). A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers (alternatively, integers, positive integers, rationals) $x_1, \ldots, x_p$ 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 (respectively, integers, positive integers, rationals) $x_1, \ldots, x_{p+1}$.

**Proof:** We present the proof for solutions in non-negative integers. Let $A_1$ denote the following statement: A Diophantine equation $D(x_1, \ldots, x_p) = 0$ has no solutions in non-negative integers $x_1, \ldots, x_p$. Let $A_2$ denote the following statement: The equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has at most finitely many solutions in non-negative integers $x_1, \ldots, x_{p+1}$. We need to prove that

$$(A_1 \Rightarrow A_2) \land (A_2 \Rightarrow A_1)$$

We present the proof that $A_1$ implies $A_2$. The statement $A_1$ implies that the set of all tuples $(x_1, \ldots, x_{p+1}) \in \mathbb{N}^{p+1}$ which satisfy $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ is empty. The empty set is finite. We present the proof that $A_2$ implies $A_1$. Assume, on the contrary, that non-negative integers $a_1, \ldots, a_p$ satisfy $D(a_1, \ldots, a_p) = 0$. Then,

$$\forall x_{p+1} \in \mathbb{N} \quad D(a_1, \ldots, a_p) + 0 \cdot x_{p+1} = 0$$

Therefore, infinitely many tuples $(x_1, \ldots, x_{p+1}) \in \mathbb{N}^{p+1}$ solve the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$, a contradiction. The proof for solutions in integers (positive integers, rationals) is analogous. $\square$
Lemma 3 (cf. Smoryński’s theorem in [8, p. 258]). If the set of all Diophantine equations which have at most finitely many solutions in non-negative integers (alternatively, integers, positive integers, rationals) is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in non-negative integers (respectively, integers, positive integers, rationals).

Proof: We present the proof for solutions in non-negative integers. Suppose that \( \{S_i = 0\}_{i=0}^{\infty} \) is a computable sequence of all Diophantine equations which have at most finitely many solutions in non-negative integers. By Lemma 2, 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. The flowchart algorithm uses a computable surjection \( \varphi : \mathbb{N} \to \mathbb{N}^p \).

![Flowchart 1](image)

The flowchart algorithm always terminates because there exists a non-negative integer \( i \) such that
\[
(D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = S_i) \lor (D(\varphi(i)) = 0)
\]
Indeed, for every Diophantine equation \( D(x_1, \ldots, x_p) = 0 \), the flowchart algorithm finds a solution in non-negative integers, or finds the equation \( D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0 \) on the infinite list \([S_0, S_1, S_2, \ldots]\) if the equation \( D(x_1, \ldots, x_p) = 0 \) is not solvable in non-negative integers.

For solutions in integers, we choose a computable surjection \( \varphi : \mathbb{N} \rightarrow \mathbb{Z}^p \), modify the definition of the sequence \( \{S_i = 0\}_{i=0}^{\infty} \), and modify the two print instructions. For solutions in positive integers, we choose a computable surjection \( \varphi : \mathbb{N} \rightarrow (\mathbb{N} \setminus \{0\})^p \), modify the definition of the sequence \( \{S_i = 0\}_{i=0}^{\infty} \), and modify the two print instructions. For solutions in rationals, we apply Lemma 1 and choose a computable surjection \( \varphi : \mathbb{N} \rightarrow \mathbb{Q}^p \), modify the definition of the sequence \( \{S_i = 0\}_{i=0}^{\infty} \), and modify the two print instructions. \( \square \)

The proof in [8, p. 258] uses a computable surjection from \( \mathbb{N} \setminus \{0, 1\} \) onto \( \mathbb{N}^p \) which is explicitly defined.

### 3 Main Results

**Theorem 1** (cf. [8, Theorem 12, p. 258]). The set of all Diophantine equations which have at most finitely many solutions in non-negative integers (integers, positive integers) is not recursively enumerable.

**Proof:** It follows from Lemma 3 and Matiyasevich’s theorem. \( \square \)

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 non-zero monomial which is divided by \( x_i \), if \( D(x_1, \ldots, x_p) \) is written as the sum of a minimal number of monomials.

**Lemma 4** 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 \( (2x_{p+1} + 1) \cdot D(x_1, \ldots, x_p) = 0 \) has at most finitely many solutions in non-negative integers \( x_1, \ldots, x_{p+1} \).

**Lemma 5** 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 \( (2x_{p+1} + 1) \cdot D(x_1, \ldots, x_p) \) truly depends on all the variables \( x_1, \ldots, x_{p+1} \).
**Theorem 2** The equations which belong to $E$ and which have at most finitely many solutions in non-negative integers form a set which is not recursively enumerable.

**Proof:** We reformulate Lemma 3 for Diophantine equations which belong to $E$. The proof, which uses Lemmas 3–5, is analogous to the proof of Theorem 1.

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 3** For every integer $k \geq 9$, 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.

Start

Input a Diophantine equation $D(x_1, \ldots, x_p) = 0$, where $p \leq k$

$j := 0$

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

No

$j := j + 1$

Yes

$i := 0$

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

No

$i := i + 1$

Yes

Is $D(\varphi(i)) = 0$?

No

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 2
By the stronger version of the Davis-Putnam-Robinson-Matiyasevich 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 $\{G_i = 0\}_{i=0}^{\infty}$ is a computable sequence of all equations from $Dioph(k)$. Then, the execution of Flowchart 2 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 $x_1, \ldots, x_p$. The flowchart algorithm uses a computable surjection $\varphi: \mathbb{N} \to \mathbb{N}^p$.

Thus we have a contradiction to Matiyasevich’s theorem. The flowchart algorithm always terminates because there exist non-negative integers $i$ and $j$ such that

$$(D(x_1, \ldots, x_p) = D_j) \land ((W(j, x_1, \ldots, x_9) = G_i) \lor (D(\varphi(i)) = 0)) \quad \square$$

4 Hilbert’s Tenth Problem for Solutions in a Subring of $\mathbb{Q}$

Hilbert’s Tenth Problem for solutions in $\mathbb{Q}$ remains unsolved, see [2] and [7]. Harvey Friedman conjectures that the set of all Diophantine equations which have only finitely many rational solutions is not recursively enumerable, see [3]. For solutions in rationals, Lemma 3 claims that a negative solution to Hilbert’s Tenth Problem for solutions in $\mathbb{Q}$ implies that the set of all Diophantine equations with a finite number of rational solutions is not recursively enumerable. We show the converse implication, see Theorem 5.

Guess ([5, p. 16]). The question of whether or not a given Diophantine equation has at most finitely many rational solutions is decidable with an oracle that decides whether or not a given Diophantine equation has a rational solution.

Originally, Minhyong Kim formulated the Guess as follows: for rational solutions, the finiteness problem is decidable relative to the existence problem.

Assume that $K$ is an infinite subset of $\mathbb{Q}$ and for every positive integer $n$ there exists a computable surjection from $\mathbb{N}$ onto $K^n$, cf. Lemma 1.
Theorem 4 If the set of all Diophantine equations which have at most finitely many solutions in \( K \) is recursively enumerable, then there exists an algorithm which decides whether or not a given Diophantine equation has a solution in \( K \).

Proof: The proof is analogous to the proof of Lemma 3.

In the next three lemmas we assume that \( \{0\} \subset R \subset \mathbb{Q} \) and \( r \cdot \mathbb{Z} \subset R \) for every \( r \in R \). Every non-zero subring \( R \) of \( \mathbb{Q} \) satisfies these conditions even if \( 1 \notin R \).

Lemma 6 There exists a non-zero integer \( m \in R \).

Proof: There exist \( m, n \in \mathbb{Z} \setminus \{0\} \) such that \( \frac{m}{n} \in R \). Hence, \( m = \frac{m}{n} \cdot n \in (\mathbb{Z} \setminus \{0\}) \cap R \).

Lemma 7 Let \( m \in (\mathbb{Z} \setminus \{0\}) \cap R \). We claim that for every \( b \in R \), \( b \neq 0 \) if and only if the equation

\[
y \cdot b - m^2 - \sum_{i=1}^{4} y_i^2 = 0
\]

is solvable in \( y, y_1, y_2, y_3, y_4 \in R \).

Proof: If \( b = 0 \), then for every \( y, y_1, y_2, y_3, y_4 \in R \),

\[
y \cdot b - m^2 - y_1^2 - y_2^2 - y_3^2 - y_4^2 = -m^2 - y_1^2 - y_2^2 - y_3^2 - y_4^2 \leq -m^2 < 0
\]

If \( b \neq 0 \), then \( b = \frac{p}{q} \), where \( p \in \mathbb{N} \setminus \{0\} \) and \( q \in \mathbb{Z} \setminus \{0\} \). In this case, we define \( y \) as \( m^2 \cdot q \) and observe that

\[
m^2 \cdot q = (m \cdot q) \cdot m \in R
\]

as \( m \cdot q \in R \) and \( m \in \mathbb{Z} \). Hence,

\[
y \cdot b = (m^2 \cdot q) \cdot \frac{p}{q} = m^2 \cdot p \in m^2 \cdot (\mathbb{N} \setminus \{0\})
\]

By Lagrange’s four-square theorem, there exist \( t_1, t_2, t_3, t_4 \in \mathbb{N} \) such that

\[
\frac{y \cdot b - m^2}{m^2} = t_1^2 + t_2^2 + t_3^2 + t_4^2
\]

Therefore,

\[
y \cdot b - m^2 - (m \cdot t_1)^2 - (m \cdot t_2)^2 - (m \cdot t_3)^2 - (m \cdot t_4)^2 = 0,
\]

where \( m \cdot t_1, m \cdot t_2, m \cdot t_3, m \cdot t_4 \in R \).
Lemma 8 We can uniquely express every rational number \( r \) as \( \frac{\hat{r}}{r} \), where \( \hat{r} \in \mathbb{Z}, r \in \mathbb{N} \setminus \{0\} \), and the integers \( \hat{r} \) and \( r \) are relatively prime. If \( r \in R \), then \( \frac{\hat{r}}{r} \in R \).

Proof: For every \( r \in R \), \( \frac{\hat{r}}{r} = r \cdot \frac{\hat{r}}{r} \in r \cdot \mathbb{Z} \subseteq R \). □

Starting from this moment up to the end of the article we assume that \( R \) is a non-zero subring of \( \mathbb{Q} \) with or without 1. We assume also that for every positive integer \( n \) there exists a computable surjection from \( \mathbb{N} \) onto \( R^n \). By Lemma 1, \( R = \mathbb{Q} \) satisfies these conditions. The same is true for \( R = \mathbb{Z} \).

Lemma 9 For every \( \theta : \mathbb{N} \rightarrow R^n \), for every \( x_1, \ldots, x_n \in R \), and for every \( k \in \mathbb{N} \), the following product

\[
\prod_{(r_1, \ldots, r_n) \in \{\theta(0), \ldots, \theta(k)\}} \sum_{i=1}^{n} (x_i \cdot r_i - \frac{\hat{r}_i}{r_i})^2
\]

(1)

differs from 0 if and only if \( (x_1, \ldots, x_n) \notin \{\theta(0), \ldots, \theta(k)\} \). Product (1) belongs to \( R \).

Proof: The last claim follows from Lemma 8. □

Theorem 5 A positive solution to Hilbert’s Tenth Problem for solutions in \( R \) implies that the set of all Diophantine equations with a finite number of solutions in \( R \) is recursively enumerable.

Proof: We assume a positive solution to Hilbert’s Tenth Problem for solutions in \( R \). By Lemma 6, there exists a non-zero integer \( m \in R \). By Lemmas 7–9, the algorithm in Flowchart 3 halts if and only if a Diophantine equation \( D(x_1, \ldots, x_n) = 0 \) has at most finitely many solutions in \( R \). □

The algorithm in Flowchart 3 depends on \( m \in (\mathbb{Z} \setminus \{0\}) \cap R \).

Lemma 10 We can compute some element of \( (\mathbb{Z} \setminus \{0\}) \cap R \).

Proof: We compute the smallest \( i \in \mathbb{N} \) such that \( \theta(i) \) starts with a non-zero integer. This integer belongs to \( (\mathbb{Z} \setminus \{0\}) \cap R \). □

Lemma 10 leads to a constructive proof of Theorem 5. Theorems 4 and 5 imply the next theorem.

Theorem 6 Hilbert’s Tenth Problem for solutions in \( R \) has a positive solution if and only if the set of all Diophantine equations with a finite number of solutions in \( R \) is recursively enumerable.
For $R = \mathbb{Z}$, Theorem 6 claims that Matiyasevich’s theorem for solutions in integers implies Smoryński’s theorem for solutions in integers, and vice versa.

Theorems 4-6 hold under weaker assumptions, see [9].

Acknowledgement. Agnieszka Peszek prepared the flowcharts in TikZ. Apoloniusz Tyszka wrote the article. Both authors are grateful to an anonymous referee for here or his useful comments.

References


[2] M. Davis. Representation Theorems for Recursively Enumerable Sets and a Conjecture Related to Poonen’s Large Subring of $\mathbb{Q}$. Journal...
Relationship Between Matiyasevich’s and Smoryński’s Theorems


© Scientific Annals of Computer Science 2019