university of groningen / faculty of science and engineering / mathematics and applied mathematics

# To Solve is Not to Solve: Hilbert's Tenth Problem over $\mathbb{Z}$ and Rings of Integers

Bachelor's Project Mathematics

June 2025

Student: I.C.Roest

First supervisor: Dr. E.Özman

Second assessor: Prof.dr. L.C.Verbrugge

When David Hilbert posed his famous 23 questions, he shaped the mathematical research of the 20th century and beyond. This thesis focuses on Hilbert's Tenth Problem, a decision problem that asks whether there exists a general algorithm to solve any given Diophantine equation over the integers. In 1970, this problem was proven to be undecidable: there is no such algorithm. We present a detailed and accessible account of this proof. We then explore generalizations of this problem over other rings, particularly rings of integers. This version was proven undecidable only extremely recently, in December 2024. We investigate this new proof and see how it differs from the original approach over the integers.

# Contents

# 1 Introduction

Are there limits to what mathematics can do? Can it describe everything, or are there things we may never know? Some questions have been around for so long, have seen so many failed attempts, that we might give up hope. Sometimes, a proof arises against all odds, and the mathematical world sees some magic. Think of Andrew Wiles' famous proof of Fermat's Last Theorem, a problem stated centuries ago, the proof of which helped to develop and connect entire fields of mathematics. However, there are also problems for which we are still in the dark, like the Twin Prime Conjecture. Are we not looking hard enough? Or are we looking in vain? These questions lie at the heart of *undecidability*: knowing that we cannot know.

When David Hilbert posed his 23 questions at the International Congress of Mathematicians in 1900, his incentive was to shape the mathematical research of the 20th century and broaden its horizon. At that time, he did not know that one of his questions would not have the solution he imagined. This question is the tenth, and he stated it as follows:

> Give a computing algorithm which tells of a given Diophantine equation with integer coefficients whether or not it has a solution in the integers [1].

Diophantine equations are polynomial equations for which we determine of which algebraic structure the coefficients are elements. In this case, we consider the coefficients to be integers. The above problem, in a way, did what Hilbert envisioned: it connected the fields of logic, number theory, and computability theory in a way that was unknown before. When Hilbert stated it, the concept of an algorithm was not even defined, and he initially described it as a computation consisting of a finite number of steps. However, what Hilbert did not imagine, is that his tenth problem does not have a solution at all: there is no such algorithm. This is the same as saying that the problem is *undecidable*. A problem is decidable if there is some computational method that gives us a guaranteed solution in finite time, usually either *YES* or *NO*, or 1 or 0.

The quest to an answer to Hilbert's Tenth Problem started with Alan Turing. He formalized the notion of an algorithm within the concept of a Turing machine: a machine with infinite memory and computational capacity that can perform any conceivable computation in an algorithmic way. An important discovery in this development is the Halting problem, which shows that there are some things that even a Turing machine cannot compute! In other words, some problems are inherently undecidable. This discovery allowed mathematicians to consider the possibility that other problems could be undecidable, including Hilbert's Tenth Problem [2].

Many mathematicians ventured to solve Hilbert's Tenth Problem, but there are a few who made the largest contributions. It was known at the time that if Diophantine sets are equivalent to recursively enumerable sets, then undecidability follows. Diophantine sets are sets that can be represented by Diophantine equations, and recursively enumerable sets are sets for which a Turing machine can list all of its elements, but not necessarily decide whether something is *not* an element of the set. In the 1950s and 1960s, mathematicians Hilary Putnam and Martin Davis worked towards simplifying expressions for recursively enumerable sets to approach Diophantine sets. At around the same time, mathematician Julia Robinson used a different method. She formulated a hypothesis about the existence of a Diophantine set with particular properties. If this hypothesis was shown to be true, then the undecidability of Hilbert's Tenth Problem would immediately follow. The crux was describing exponentiation with Diophantine equations.
Decades later, in 1970, Russian mathematician Yuri Matiyasevich found a Diophantine set that confirms Julia Robinson's hypothesis, and hereby found the answer: Hilbert's Tenth Problem is undecidable [3].

It is an inherent wish in mathematics to generalize obtained results. Hilbert's Tenth Problem is proven to be undecidable when we work over the integers $\mathbb{Z}$. A natural question that follows is whether, and how, this result changes when we consider more general rings, for example $\mathbb{Z}[\sqrt{2}]$ or $\mathbb{Z}[i]$.

The aim of this thesis is to give an overview of the proof of Hilbert's Tenth Problem over $\mathbb{Z}$. This is done in Section 2. We continue by considering Hilbert's Tenth Problem over rings of integers of a number field. We first try to apply the proof methods of Robinson, Matiyasevich, Davis, and Putnam to Hilbert's Tenth Problem over $\mathbb{Z}[\sqrt{2}]$ in Section 3, but we encounter several problems. However, this attempt does pave the way to a new concept: Diophantine definition. This strong notion helps us to transfer the undecidability result from the integers to certain other rings, by in some sense mimicking the behavior of $\mathbb{Z}$ inside these other rings [4]. In Section 4, we formalize this concept, along with Hilbert's Tenth Problem over a general ring R, and we determine which rings allow a Diophantine definition. We continue by explicitly constructing such a definition for real, quadratic rings of integers, thereby proving the undecidability of Hilbert's Tenth Problem over such rings. This is done using the original proof by J. Denef from 1975. We finish this thesis by discussing the undecidability proof over rings of integers of a general number field. This result is particularly interesting, because it was proven very recently, by two independent research groups: in December 2024, and in January 2025.

In Hilbert's Tenth Problem, two fields of mathematics come together: number theory and logic. In particular computability theory, which is considered a subfield of mathematical logic. Indeed, the study of Diophantine equations and their solutions belongs to the field of number theory, while recursively enumerable sets, and more generally decidability are a part of logic. It is interesting that, while many fields of mathematics are considered to be separate, more often than not these fields have seemingly hidden connections. An additional aim of this thesis is therefore to give an audience to both number theory and logic, and to consider Hilbert's Tenth Problem from both of their perspectives.

## 2 Hilbert's Tenth Problem over $\mathbb{Z}$

Hilbert stated his tenth problem over the integers: $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$. However, it was soon discovered that we can stay positive: Hilbert's Tenth Problem over $\mathbb{Z}$ is equivalent to Hilbert's Tenth Problem over $\mathbb{N}$, where we take $\mathbb{N} = \{1, 2, \dots\}$, and throughout this thesis we typically call elements of $\mathbb{N}$ positive integers. So, we only have to look at the positive integers, but why? Let us first state the following important number theory result.

**Theorem 2.1** ([5] Lagrange's four square theorem)**.** *Take $n \in \mathbb{N}$. Then there exist $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{1}$$

This theorem states that every positive integer can be written as a sum of four squares. There are many different proofs available, and one can be found in [5].

If we prove that no algorithm exists to determine whether a polynomial with integer coefficients has a solution in the positive integers, then it immediately follows that no algorithm exists for integer solutions either. Suppose that we want to know whether the polynomial

$$h(x_1, \dots, x_n) = 0 \tag{2}$$

with integer coefficients has a solution in the positive integers. We can test whether

$$h(1 + k_1^2 + l_1^2 + m_1^2 + n_1^2, \dots, 1 + k_n^2 + l_n^2 + m_n^2 + n_n^2) = 0 \tag{3}$$

has integer solutions $(k_1, l_1, m_1, n_1, \dots, k_n, l_n, m_n, n_n)$. This indeed follows from Theorem 2.1 [1]. Therefore, in the remainder of this section, we consider Hilbert's Tenth Problem over $\mathbb{N}$: we consider Diophantine equations with integer coefficients for which we are interested in *positive* integer solutions.

As mentioned in the introduction, the aim of this thesis is to not only prove the undecidability of Hilbert's Tenth Problem, but also to do this from both a logical and a number-theoretic perspective. To make sure we have a sturdy formal basis for this, let us revisit some definitions from first-order logic. For this part we use the following sources: [6, Chapter 12], [7, Chapter 9], [8, Chapter 3.2], and [9].

The *language* of first-order logic consists of:

- Variables: $x_1, x_2, x_3, \dots$
- Constants: $a_1, a_2, a_3, \dots$
- For every positive integer $n$, $n$-ary predicate symbols: $P_n^1, P_n^2, \dots$. These can be used to show properties or relations of, or between, constants and variables
- Logical connectives: $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$. These mean, respectively: "and", "or", "not", "implies", and "equivalent"
- Quantifiers: $\forall, \exists$. These mean "for all" and "there exists", and are called the universal and existential quantifier, respectively
- Parentheses: $(,)$

We can use the above vocabulary to build terms and formulas.

**Definition 2.1** (Term)**.** We call any constant or variable a *term*.

We define (well-formed) formulas in first-order logic inductively as follows.

**Definition 2.2** (First-order formula)**.**

- If $t_1, \ldots, t_n$ are terms and $P$ an $n$-ary is an predicate symbol, then $Pt_1 \ldots t_n$ is an (atomic) formula.
- If $A$ and $B$ are formulas, then $(A \wedge B), (A \vee B), \neg A, (A \to B),$ and $(A \leftrightarrow B)$ are also formulas.
- If $A$ is a formula and $x$ is a variable, then $\forall x A$ and $\exists x A$ are also formulas.
- Nothing is a formula unless it is generated by repeated applications of the above rules.

**Example 2.1.** Let us take $x, y, z$ to be variables, $a$ to be a constant, and $P$ and $Q$ to be a unary and a binary predicate respectively. In this case, an example of a first-order formula is

$$\exists x \forall y (\neg (P(a) \wedge Q(x, y)) \vee Q(a, y)). \tag{4}$$

You might be familiar with first-order logic, since it is often taught in an introductory logic course. It is a formal language that is designed to unambiguously talk and reason about the world around us [7]. However, we can narrow our view slightly. Let us say we want to talk and reason specifically about rings! In this case, our language changes, and we call it the language of rings. It looks like this [10]:

- Variables: $x_1, x_2, x_3, \ldots$
- Constants: $0, 1$
- Binary predicates $=, +, \cdot$
- Logical connectives: $\wedge, \vee, \neg$
- Quantifiers: $\forall, \exists$
- Parentheses: $(,)$

Note that implies $(\to)$ and equivalent $(\leftrightarrow)$ are not being used. In the language of rings, terms are defined the same as in Definition 2.1, and the way we define formulas is similar. For clarity, we do explicitly define formulas here [8, Definition 2.7].

**Definition 2.3** (First-order formula in the language of rings)**.**

- Let $t_1$ and $t_2$ be terms, and let be $P$ a binary predicate symbol. Then $Pt_1t_2$ is an (atomic) formula.
- If $A$ and $B$ are formulas, then $(A \wedge B), (A \vee B),$ and $\neg A$ are also formulas.
- If $A$ is a formula and $x$ is a variable, then $\forall x A$ and $\exists x A$ are also formulas.
- Nothing is a formula unless it is generated by repeated applications of the above rules.

**Example 2.2.** For instance, a first-order formula in the language of rings is

$$\exists u \forall y (\neg (x + y^2 = u - 2) \wedge \exists v (v = y + x + u^3)). \tag{5}$$

In the remainder of this thesis we come across such formulas in disguise, for example in Example 2.4. In Section 4.1, we recall our formal definition and use it to define new concepts.

## 2.1 Diophantine equations and sets

In this section, we introduce some necessary knowledge to understand the statement of Hilbert's Tenth Problem: Diophantine equations and Diophantine sets. Diophantine equations and sets are named after Diophantus, who is mostly known for his book *Arithmatica*, and is sometimes considered the father of algebra. He lived in Alexandria, but interestingly, it is not precisely known when. Historians have placed his life somewhere between 150 CE and 500 CE [11].

Let us consider some definitions and examples.

**Definition 2.4** ([12] Polynomial equation)**.** Let $n \in \mathbb{N}$, let $x_1, \ldots, x_n$ be variables, and let $R$ be a ring. Let $f, g \in R[x_1, \ldots, x_n]$. The equation

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \tag{6}$$

is called a polynomial equation.

*Remark* 1. Note that Equation (6) can be rewritten slightly. Let $\boldsymbol{x}$ denote $x_1, \ldots, x_n$. Take $h \in R[\boldsymbol{x}]$ such that $h(\boldsymbol{x}) = f(\boldsymbol{x}) - g(\boldsymbol{x})$. Then,

$$h(\boldsymbol{x}) = 0 \tag{7}$$
$$\iff f(\boldsymbol{x}) - g(\boldsymbol{x}) = 0 \tag{8}$$
$$\iff f(\boldsymbol{x}) = g(\boldsymbol{x}). \tag{9}$$

Hence, $h(\boldsymbol{x}) = 0$ is also a polynomial equation, since it is equivalent to Equation (6). We use these different ways of writing interchangeably throughout this thesis.

**Example 2.3** (Polynomial equation: the square)**.** We can denote $x$ being the square of $y$, where $x, y \in \mathbb{N}$, as:

$$x = y^2. \tag{10}$$

A *Diophantine equation* is a polynomial equation for which we specify what the coefficients are, meaning of what ring or field they are elements. Moreover, we specify in what type of solutions we are interested. In this section, we consider Diophantine equations with integer coefficients for which we are only interested in integer solutions. Recall that in our case, this is equivalent to looking at positive integer coefficients and solutions, as is discussed at the beginning of this section.

*Remark* 2. Let us emphasize at this point that exponentiation (such as $x = 2^y$, or $z = x^y$) is not allowed in Diophantine equations!

Example 2.3 is a nice, concise way to denote a square, but what if we want to talk about squares more generally? Let us revisit this example. Instead of stating that $x$ is *the* square of $y$, we want to state that $x$ is *a* square of *some* positive integer.

**Example 2.4** (A square: more generally)**.** We denote $x$ being a square as

$$\exists y(x = y^2), \tag{11}$$

with $x, y \in \mathbb{N}$.

The way to read Equation (11) is: there exists some positive integer $y$ such that $x$ is the square of $y$. This example already gives an inkling about a concept that is closely linked to Diophantine equations: Diophantine sets. See, $\exists y(x = y^2)$ is an expression in itself, but it also *represents* something: the notion of $x$ being a square.
What does this have to do with Diophantine sets? Simply put, Diophantine sets encode what a Diophantine equation represents; a Diophantine equation is a *representation* of a Diophantine set. A Diophantine set consists of positive integers for which the corresponding Diophantine equation can be satisfied.

**Definition 2.5** ([1] Diophantine set)**.** Let $n \in \mathbb{N}$, $m \in \mathbb{Z}_{\geq 0}$, and let $S \subset \mathbb{N}^n$ be a subset. We call $S$ a *Diophantine (sub)set* if there is a polynomial $h \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$(x_1, \ldots, x_n) \in S \iff \exists y_1 \ldots \exists y_m (h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0). \tag{12}$$

We additionally require $y_1, \ldots, y_m \in \mathbb{N}$.

*Remark* 3. An alternative but equivalent notation for $S$ is

$$S = \{(x_1, \ldots, x_n) \in \mathbb{N}^n : \exists y_1 \ldots \exists y_m (h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0)\}. \tag{13}$$

The above definition means that the elements of a Diophantine set are precisely the $n$-tuples for which the corresponding Diophantine equation has one or more integer solutions $(y_1, \ldots, y_m)$. Let us clarify Definition 2.5 in our familiar square example.

**Example 2.5** (Diophantine set: the set of squares)**.** Recall Equation (11) from Example 2.4:

$$\exists y (x = y^2).$$

Note that it is equivalent to $\exists y (x - y^2 = 0)$. Applying Definition 2.5 directly, we have $n = m = 1$. Let $S \subset \mathbb{N}$; $S$ is a Diophantine set if

$$x \in S \iff \exists y (x - y^2 = 0). \tag{14}$$

This means that a positive integer $x$ is an element of $S$ if, and only if, $x$ is the square of some positive integer $y$. This means that the set $S$ is the set of squares of positive integers, and the Diophantine equation in (10) represents $S$.

Let us discuss another example: Pythagorean triples.

**Example 2.6** ([13] Pythagorean triples)**.** A triple $(x, y, z) \in \mathbb{N}^3$ is called a Pythagorean triple if

$$x^2 + y^2 = z^2. \tag{15}$$

Some well-known Pythagorean triples are $(3, 4, 5)$ and $(5, 12, 13)$. We denote the set of Pyhtagorean triples by $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + y^2 = z^2\}$. Note that Equation (15) is a Diophantine equation, since it is a polynomial equation and we consider (positive) integer solutions. This implies that $S$ is a Diophantine set, because

$$(x, y, z) \in S \iff x^2 + y^2 - z^2 = 0. \tag{16}$$

The main goal of this section was to familiarize ourselves with the concepts of Diophantine equations and sets. We learned exactly what Hilbert means in the statement of his tenth problem when he mentions Diophantine equations. We expanded this to Diophantine sets to be able to talk about this problem in a slightly different fashion. The original statement of Hilbert's Tenth Problem is to find an algorithm that checks whether or not a Diophantine equation has a solution. This is equivalent to asking whether we can definitively determine whether or not something is an element of the Diophantine set that our Diophantine equation represents. The step from equations to sets proves to be useful when we want to build the bridge from this number theoretical notion of Diophantine equations to the field of computability theory. We elaborate more on this in Section 2.3. Before that, let us look at a specific Diophantine equation.

## 2.2 Pell's equation

Recall that in Diophantine equations we are only allowed to use addition and multiplication, and that exponentiation is forbidden (Remark 2). It turns out that this lack of exponentiation is problematic for solving Hilbert's Tenth Problem. We see later on, in Section 2.5, why exponentiation is so crucial. For now, just keep in mind that in our search to find some connection between algorithms and Diophantine equations, exponentiation is bound to arise somewhere along the way. What we wish to accomplish is to describe exponentiation using only Diophantine equations. Julia Robinson made a step in this direction in 1950 by conjecturing that there exists a Diophantine set that models controlled exponential growth [14].

**Theorem 2.2** ([1] Julia Robinson Hypothesis)**.** *There exists a Diophantine set $S \subset \mathbb{N}^2$ such that:*

*(i)* $(u, v) \in S \implies v \leq u^u$,

*(ii) For each positive integer $k$, there is $(u, v) \in S$ such that $v > u^k$.*

This hypothesis elegantly captures exponential behavior of the form where $v$ grows exponentially with respect to $u$. The first statement ensures that the growth is not too fast, namely that $v$ is bounded from above by $u^u$. The second statement, on the other hand, forces the growth to be fast enough: *at least* exponential for some positive integer $k$.
When Julia Robinson stated this conjecture, it would still take twenty years to prove it. In the late 1960s, she lost faith in the hypothesis herself, and even briefly worked towards a positive solution of Hilbert's Tenth Problem [3]. In 1970 however, the Julia Robinson Hypothesis was finally proven to be true by Yuri Matiyasevich, who was only twenty-two, and found a Diophantine set satisfying the above properties using Fibonacci numbers and a Diophantine equation called Pell's equation. When Robinson heard of Matiyasevich' proof, she wrote him a letter, and famously said [15]: "Now I know it is true, it is beautiful, it is wonderful. If you really are twenty-two, I am especially pleased to think that when I first made the conjecture you were a baby and I just had to wait for you to grow up!"

Pell's equation plays an important role in the proof of Hilbert's Tenth Problem. It is a Diophantine equation with solutions that can model exponential growth. Originally, Matiyasevich showed that there is a Diophantine set that describes exponentiation using the unit group of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and the Fibonacci numbers. Matiyasevich' approach did the trick, but later some more approachable methods were discovered. One of them uses the unit group of $\mathbb{Z}[\sqrt{d}]$ for some nonsquare positive integer $d$, and this is the approach we consider in this section. We do not discuss a full proof, but rather the intuition behind how something purely Diophantine can behave exponentially after all [16].

**Definition 2.6** ([12] Pell's equation)**.** The equation

$$x^2 - dy^2 = 1 \tag{17}$$

is called Pell's equation. We typically look at solutions $(x, y) \in \mathbb{N}^2$, and we take $d$ to be a positive integer that is *not* a perfect square.

We take $d$ to be nonsquare because of the following reasoning: suppose that $d = b^2$ for some $b \in \mathbb{Z}$, and suppose that $(x, y) \in \mathbb{N}^2$ satisfies Pell's equation. In this case,

$$1 = x^2 - dy^2 = x^2 - (by)^2 = (x - by)(x + by) \tag{18}$$

$$\implies x - by = x + by = \pm 1 \tag{19}$$

$$\implies y = 0 \quad \text{and} \quad x = \pm 1. \tag{20}$$

This means that if $d$ were a square, the only solution would be $(x, y) = (\pm 1, 0) \notin \mathbb{N}^2$. We call this the trivial solution. To avoid this, we take $d$ to be nonsquare. We call the solution with the least positive $y$ the fundamental solution [12].

*Remark* 4. Pell's equation is actually misnamed! There is no record that John Pell, who worked for the University of Amsterdam, ever worked on finding nontrivial solutions to such equations. Instead, a better name might be Fermat's equation or Brouckner's equation. This misconception is due to Euler, who misread a book in which the work on such equations is discussed [11], [17].

The solutions to Pell's equation have an interesting connection to the ring

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}, \tag{21}$$

and in particular to its unit group

$$\left(\mathbb{Z}[\sqrt{d}]\right)^\times = \{x \in \mathbb{Z}[\sqrt{d}] : \exists y \in \mathbb{Z}[\sqrt{d}] \text{ s.t. } xy = 1\}. \tag{22}$$

This is a group with multiplication as its group law [18].

To see the connection to Pell's equation, let us look at the norm map. The norm map of $\mathbb{Z}[\sqrt{d}]$ is defined as

$$\mathrm{N} : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}, \quad N(x + y\sqrt{d}) = (x - y\sqrt{d})(x + y\sqrt{d}) = x^2 - dy^2 \text{ [18]}. \tag{23}$$

This is precisely where the connection between Pell's equation and $\mathbb{Z}[\sqrt{d}]$ comes from: the definition of the norm looks suspiciously similar to Equation (17). The following proposition is vital to this connection.

**Proposition 2.1.** *Let $\left(\mathbb{Z}[\sqrt{d}]\right)^\times$ be the unit group of $\mathbb{Z}[\sqrt{d}]$ and let $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ be the norm map. We have*

$$\alpha \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times \iff N(\alpha) = \pm 1. \tag{24}$$

*Proof.* $\Longleftarrow$ : Take $\alpha = x + y\sqrt{d}$ and suppose $N(\alpha) = \pm 1$. This means that $(x + y\sqrt{d})(x - y\sqrt{d}) = \pm 1$. This implies that either $(x - y\sqrt{d})$ or $-(x - y\sqrt{d})$ is the inverse of $\alpha$, so $\alpha$ is a unit: $\alpha \in \mathbb{Z}[\sqrt{d}]^\times$.
$\Longrightarrow$ : Let $\alpha \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times$. This means there is some $\beta \in \mathbb{Z}[\sqrt{d}]$ such that $\alpha\beta = 1$. By the multiplicative property of the norm map, $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$. Since $N(\alpha), N(\beta) \in \mathbb{Z}$, we must conclude that $N(\alpha) = N(\beta) = \pm 1$. □

The above proposition shows that $(x, y) \in \mathbb{N}^2$ is a solution to Pell's equation in (17) if, and only if, $N(x + y\sqrt{d}) = 1$, and that this directly implies that that $x + y\sqrt{d} =: \alpha$ is a unit in $\mathbb{Z}[\sqrt{d}]$ [18]. Since the group law of the unit group is multiplication, we have that $\alpha^n \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times \subseteq \mathbb{Z}[\sqrt{d}]$ for any $n \in \mathbb{N}$. Hence, there are $x_n, y_n \in \mathbb{Z}$ such that $x_n + y_n\sqrt{d} = \alpha^n$. Because of the multiplicative property of the norm map, we have

$$N(x_n + y_n\sqrt{d}) = N(\alpha^n) = (N(\alpha))^n = 1. \tag{25}$$

This means that $x_n + y_n\sqrt{d}$ also has norm 1, and hence $(x_n, y_n)$ is also a solution of Pell's equation. This way, we can obtain all solution to Pell's equation from just one: the fundamental solution.
The set of numbers of the form $x \pm y\sqrt{d}$ such that $(x, y)$ is a (possibly trivial) solution of Pell's equation in fact forms a subgroup of $\mathbb{Z}[\sqrt{d}]$ [8, Lemma 3.3].

It is important for us to be able to find the fundamental solution of a given Pell equation. However, in some cases this is not straightforward; for instance, the fundamental solution of $x^2 - 61y^2 = 1$ is $(x, y) = (1766319049, 226153980)$ [11]. We can simplify this task by choosing $d$ wisely. From now on, let $d := a^2 - 1$, for some positive integer $a > 1$. In this case, we claim that $(x, y) = (a, 1)$ is the fundamental solution. If it is a solution, it is certainly the fundamental solution, because $y = 1$ is the smallest possible positive integer. Note that

$$x^2 - (a^2 - 1)y^2 = a^2 - (a^2 - 1) \cdot 1 = 1, \tag{26}$$

so $(a, 1)$ is indeed a solution to Pell's equation [16].

Moreover, we have that

$$x_n + y_n\sqrt{d} = (a + \sqrt{d})^n, \tag{27}$$

where $(a, 1)$ is our fundamental solution, so we can generate all solutions to Pell's equation from the fundamental one [12], [11]. In some cases, we also denote the trivial solution by $(x_0, y_0)$, and the fundamental solution by $(x_1, y_1)$. This allows us to denote all solutions to Pell's equation in one go, as $(x_n, y_n)$, for $n = 0, 1, 2, \ldots$.

*Remark* 5. Indian mathematicians were already familiar with Pell equations. As early as the 7th century CE, Bragmagupta had the insight we mentioned above, namely that other solutions to Pell's equation can be generated from a nontrivial solution.
The ancient Greeks were also already tinkering with this equation. They knew that $\sqrt{2}$ is not constructible with compass and straightedge. Instead, they used solutions to Pell's equation approximate $\sqrt{2}$. Such approximations were also discovered in Indian mathematics. They work as follows:

$$x^2 - dy^2 = 1 \tag{28}$$
$$\implies x^2 = dy^2 + 1 \tag{29}$$
$$\implies \frac{x^2}{y^2} - d = \frac{1}{y^2} \tag{30}$$
$$\implies \left(\frac{x}{y} - \sqrt{d}\right)\left(\frac{x}{y} + \sqrt{d}\right) = \frac{1}{y^2} \tag{31}$$
$$\implies \left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2}. \tag{32}$$

Hence, for $(x, y)$ a solution to Pell's equation, the fraction $\frac{x}{y}$ is a relatively good approximation of $\sqrt{d}$ [11], [17], [8].

In the part that follows, we aim to do the following. Consider the graph of an exponential function: $S = \{(x, y) \in \mathbb{N}^2 : x = 2^y\}$. We want to check if $S$ is Diophantine, so by Definition 2.5, we want to find a Diophantine equation $h(z_1, \ldots, z_n, x, y)$ such that

$$(x, y) \in S \iff \exists z_1 \ldots \exists z_n (h(z_1, \ldots, z_n, x, y) = 0). \tag{33}$$

We cannot simply take $h(x, y) = x - 2^y$, because exponentiation is not allowed in Diophantine equations. Instead, we have to somehow express this exponentiation using only addition and multiplication, and this is where Pell's equation comes in.

This part of the proof of Hilbert's Tenth Problem is the part that took the longest. It was already proven in the 1960s in the work of Putnam, Davis, and Robinson that once exponentiation could be expressed purely with Diophantine equations, Hilbert's Tenth Problem would be proven to be undecidable. The last piece of the puzzle – expressing this exponentiation – was eventually found by Matiyasevich in 1970. This proof is quite complicated and extensive, and we do not dive into it in this thesis. A comprehensible account is part of the 2017 Bachelor's Thesis by S. Groen: "Matijasevic's Theorem: Diophantine descriptions of recursively enumerable sets" [16]. In this section, we discuss some key lemmas that give an indication that the solutions to Pell's equation indeed model exponential growth.

Consider Pell's equation as before:

$$x^2 - (a^2 - 1)y^2 = 1, \quad \text{with } a > 1. \tag{34}$$

We denote by $(x_1, y_1)$ our fundamental solution $(a, 1)$, and by $(x_0, y_0)$ our trivial solution $(1, 0)$. We denote by $(x_n, y_n)$, with $\mathbb{N} \ni n > 1$, the other solutions to Pell's equation, as obtained in Equation (25).

The following lemma shows that $x_n, y_n$ indeed increase as $n$ increases and that both $x_n$ and $y_n$ have $n$ as a strict and a nonstrict lower bound, respectively.

**Lemma 2.3** ([16]). *For every $n \in \mathbb{N}$, we have that $x_{n+1} > x_n > n$, and $y_{n+1} > y_n \geq n$.*

*Proof.* This proof uses induction.
**Base case:** We have $x_1 > x_0 > 0$ and $y_1 > y_0 > 0$, since $a > 1 > 0$ and $1 > 0 \geq 0$, respectively.
**Inductive hypothesis:** Suppose the statement holds for some positive integer $k$, so $x_{k+1} > x_k > k$. Lemma 2.10 in [16] states that

$$x_{n+1} = 2ax_n - x_{n-1} \quad \text{and} \quad y_{n+1} = 2ay_n - y_{n-1}. \tag{35}$$

**Inductive step:**

$$\begin{aligned} x_{k+2} = \quad & 2ax_{k+1} - x_k > ax_{k+1} + x_{k+1} - x_k > ax_{k+1} > x_{k+1} && (36)\\ \implies & x_{k+2} > x_{k+1}. && (37) \end{aligned}$$

Combining this with the induction hypothesis, we get

$$\begin{aligned} & x_{k+1} > x_k > k && (38)\\ \implies & x_{k+1} > k + 1 && (39)\\ \implies & x_{k+2} > x_{k+1} > k + 1. && (40) \end{aligned}$$

The case for $y_{k+1}$ is very similar. Hence, $x_{k+2} > x_{k+1} > k + 1$ and $y_{k+2} > y_{k+1} > k + 1$. This concludes our proof. □

The next lemma tells us that $x_n$ shows rough exponential growth. It grows sufficiently fast (at least exponentially with base $a$), but not too fast (at most exponentially with base $2a$).

**Lemma 2.4** ([16]). *For every $n \in \mathbb{N}$, $a^n \leq x_n \leq (2a)^n$.*

*Proof.* Once more, we use induction.
**Base case:** Note that $a^0 \leq x_0 \leq (2a)^0$ and $a^1 \leq x_1 \leq (2a)^1$, since $1 \leq 1 \leq 1$ and $a \leq a \leq 2a$, respectively.
**Inductive hypothesis:** Suppose $a^k \leq x_k \leq (2a)^k$ for some positive integer $k$.
**Inductive step:** We have that

$$x_{k+1} = 2ax_k - x_{k-1} \leq 2ax_k \leq 2a(2a)^k = (2a)^{k+1} \tag{41}$$

and

$$x_{k+1} = 2ax_k - x_{k-1} \geq 2ax_k - x_k = ax_k + (a-1)x_k \geq ax_k \geq a \cdot a^k = a^{k+1}. \tag{42}$$

Therefore, $a^{k+1} \leq x_{k+1} \leq (2a)^{k+1}$, which concludes our proof. □

The next step is to connect the above properties to the properties mentioned in the Julia Robinson Hypothesis (2.2) to show that the solutions $(x_n, y_n)$ to Pell's equation grow roughly exponentially in $n$. What is left to be done is to translate this behavior so that it is in the form of a Diophantine set, like in the statement of the Julia Robinson Hypothesis. That is to say, we explicitly construct Diophantine equations such that the corresponding Diophantine set is the graph of the exponential function. We omit the details of the rest of the proof, but the interested reader can find them in [16, Section 2]. The outline is as follows. We have to find the positive integer $n$ corresponding to a given solution of Pell's equation, i.e. when we have a solution $(x, y)$, we want to find $n$ such that

$(x, y) = (x_n, y_n)$. This allows us to express $x_n$ and $y_n$ with a system of eight Diophantine equations. This system is key to take the leap to describe a general exponential expression $m = p^n$ using a system of twelve Diophantine equations. These specific systems are the subject of Theorems 2.30 and 2.32 of [16].

As mentioned at the beginning of this section, this is not the exact approach that Matiyasevich took. Instead, he took advantage of the properties of the Fibonacci sequence:

$$a_1 = a_2 = 1, \quad a_{n+1} = a_n + a_{n-1}. \tag{43}$$

Matiyasevich's breakthrough was that he showed that the function $a_{2n}$ of even-indexed Fibonacci numbers is Diophantine. This implies that the set

$$S = \{(u, v) | v = a_{2u} \wedge u \geq 2\} \tag{44}$$

satisfies the Julia Robinson Hypothesis (Theorem 2.2), which follows from the fact that, for $n \geq 3$, the following inequalities hold [1]:

$$\left(\frac{5}{4}\right)^n < a_n < 2^{n-1}. \tag{45}$$

The importance of these inequalities is that they signify two things: the Fibonacci numbers grow at least exponentially fast, so they grow faster than any polynomial. Moreover, they do not grow faster than exponentially fast. This means that they show constrained exponential behavior, and this is exactly what is needed to satisfy the Julia Robinson Hypothesis.

*Remark* 6. The Fibonacci sequence, and the sequences $\{x_n\}$ and $\{y_n\}$ for $(x_n, y_n)$ a solution to Pell's equation, are special cases of so-called *Lucas sequences*, named after 19th century number theorist Edouard Lucas. Readers who are familiar with recursion in programming might be familiar with Lucas's invention of the game: the Towers of Hanoi. This is a game involving a wooden board with three rods and a number of wooden discs of different sizes. The objective of the game is to move all discs from one rod to another without putting a larger disc on top of a smaller disc, and only moving one disc at a time [8].

The fact that the exponential function is Diophantine leads to the following conclusion: a set is Diophantine if, and only if, it is exponential Diophantine. The fact that every Diophantine set is exponential Diophantine is immediate; a Diophantine set is simply a special case of an exponential Diophantine set. Namely, in an exponential Diophantine set, exponentiation is allowed, but not required. The purpose of this section was to show the other inclusion: every exponential Diophantine set is Diophantine. Let us see how this follows.
Let $S$ be an exponential Diophantine set, so, slightly tweaking Definition 2.5 of Diophantine sets, this means there exists a polynomial $e(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ in which we allow exponentiation, such that

$$(x_1, \ldots, x_n) \in S \iff \exists y_1 \ldots \exists y_m (e(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0). \tag{46}$$

Recall that exponentiation can be described using Diophantine equations, so there is a Diophantine equation $h(x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that $e$ is equivalent to $h$. So

$$(x_1, \ldots, x_n) \in S \iff \exists y_1 \ldots \exists y_m (h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0), \tag{47}$$

which means that $S$ is a Diophantine set.

## 2.3 Turing machines

We want a way to connect the concept of sets to the concept of algorithms. For this purpose, we introduce the strong notion of a Turing machine. This concept helps us determine whether something

is an element of a certain set or not. It turns out that whether this is possible depends on the type of set with which one is dealing. Let us consider some concepts of such kinds of sets intuitively for now. Once we have some understanding of their ideas, we formally define Turing machines. This is important to be able to rigorously define such sets (see Definition 2.7).

Let $n \in \mathbb{N}$. A subset $S \subset \mathbb{N}^n$ is called a *recursively enumerable* set if there exists an algorithm that takes an element $x \in \mathbb{N}^n$ as input, and returns *YES* after a finite number of steps if, and only if, $x \in S$. If $x \notin S$, then the algorithm returns anything but *YES*, or it runs for an infinite amount of time. A recursively enumerable set can be listed (enumerated) by some program. However, the program has no way to determine when an element is *not* in the set.
For some sets, we do have a way to determine definitively if an element is or is not in the set. A subset $S \subset \mathbb{N}^n$ is called a *recursive* set if there exists an algorithm that takes an element $x \in \mathbb{N}^n$ as input, runs for a finite number of steps, and returns whether or not $x \in S$. A recursive set is a set for which you can write a program that always halts, and tells you whether or not something is in the set [12]. Let us look at some examples.

**Example 2.7** (Recursive set: even numbers)**.** Consider the set of even numbers:

$$E = \{n \in \mathbb{N} : \exists y \in \mathbb{N} \text{ s.t. } n = 2y\}. \tag{48}$$

The set $E$ is a recursive set, because the program that computes ($x$ mod 2) for some input $x \in \mathbb{N}$ always determines whether or not $x$ is even, and it always halts.

**Example 2.8** (Recursively enumerable set: even numbers)**.** The set $E$ of even numbers is also a recursively enumerable set, because its elements can be listed: 2, 4, 6,....

This is no coincidence. We can see from the definitions that every recursive set is a recursively enumerable set. Indeed, if there is an algorithm that can determine in a finite number of steps whether something is or is not in the set, then it can certainly determine whether something is in the set. However, the other way around the inclusion does not hold: there are recursively enumerable sets that are not recursive. To investigate this, we have to dive into the world of Turing machines and decidability.

*Remark* 7. For a moment let us suppose that Diophantine sets are equivalent to *recursive* sets. In this case, Hilbert's Tenth Problem is decidable: there is an algorithm to determine whether something is or is not in a Diophantine set, meaning that we can definitively determine whether or not any Diophantine equation has an integer solution. Unfortunately, Diophantine sets are not equivalent to recursive sets [12], but it turns out they are equivalent to recursively enumerable sets. It was already proven in 1936 by mathematician Alonzo Church that there is no algorithm that can determine whether or not something is an element of a given recursively enumerable set. Therefore, the equivalence of Diophantine and recursively enumerable sets is the crucial insight why Hilbert's Tenth Problem is undecidable [19], [16].

In the early 20th century, David Hilbert was a leading mathematician in the formalist movement, a philosophy that believes that mathematics is based on a finite set of axioms and a formal system of rules of inference. He believed that with this formal system, mathematics could be proven complete, consistent, and decidable, meaning that everything that is true has a proof, there are no contradictions, and every true statement can be derived in a finite number of steps from the axioms. This came to be known as Hilbert's Program [20].
In 1930, Hilbert famously said the words [21]:

> We must know.
>
> We will know.

However, when Gödel published his famous incompleteness theorems in the 1930s, Hilbert's Program received a serious blow. Completeness and consistency were off the table. What was left: decidability

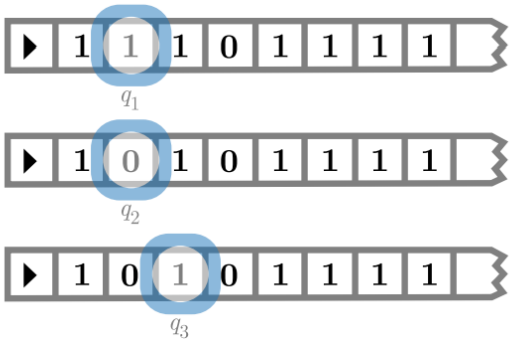


**Figure 1:** *A Turing machine executing a program* [2]

[20].
Interestingly enough, decidability is closely linked to the concept of an algorithm, and even Hilbert's Tenth Problem, already stated in 1900, is actually a decidability problem. However, the concept of an algorithm was not rigorous until 1936, when Alan Turing defined the notion of a Turing machine: a machine with infinite memory and a strict set of computational rules, that can carry out any conceivable computation. Turing showed that there is no general way to tell whether a Turing machine halts on a given input. This became known as the Halting problem; it shows the inherent undecidability of both computer programs and formal systems in general [22]. Let us look at a more formal, yet still intuitive definition of a Turing machine.

The following part is based on Part III of the book "Logic, Sets, Computation: An Open Introduction to Metalogic", which is a rigorous and accessible book that is freely available online [2]. The aim of this part is to give an intuitive idea of what a Turing machine is.
Even though in principle a Turing machine is not a physical machine, but rather a pure abstraction of a computational procedure, let us imagine it to have some physical attributes. Imagine a tape, divided into squares, that runs infinitely to the right. Each square contains a "letter" of a pre-defined alphabet. Moreover, imagine a read-write head, that can either read something off a square of the tape, or write something on it from the alphabet. In our case, we consider an alphabet consisting of three letters:

$$\triangleright, \quad \sqcup, \quad I. \tag{49}$$

Here, $\triangleright$ signifies the leftmost endpoint of the tape, and the symbol $\sqcup$ denotes a square on the tape being empty. At the beginning, before we run a program, our tape consists of the symbol $\triangleright$ at the leftmost square of the tape, followed by some finite input(s) $I$, which are in turn followed by infinitely many empty squares ($\sqcup$) all the way to the right. The input $I$ is a finite string that the Turing machine receives at the start of a run. At any step, the machine is in a certain state, which we denote by $q_1, q_2, q_3, \ldots$. The Turing machine program itself is then given by a function $\delta$, which takes a state $q$ and a letter of the alphabet, and returns what happens next: the state to which the machine should go, whatever the machine has to write on the square it is at, and whether it has to move to a different square: left ($L$), right ($R$), or neither ($N$).

Let us clarify this with an example.

**Example 2.9** (Moving right)**.** Let us consider a Turing machine with two states: $q_0$ and $q_1$. We want to write a program that if it reads some input on the first square, deletes it and then moves to the right. We denote this as follows:

$$\delta(q_0, I) = \langle q_1, \sqcup, R \rangle. \tag{50}$$

What this function signifies, is that if the machine reads some input $I$ in state $q_0$, it first overwrites the $I$ with the empty symbol $\sqcup$, and then moves one square to the right. The new state in which it is then is $q_1$.

Note that in the above example, there is only a command for when the machine reads $I$ in the first square. What if the first square is empty, i.e. it contains the symbol $\sqcup$? In this case, we define that the program *halts*. So if there is no explicit execution mentioned for some instance, we implicitly mean that the program stops running entirely. A Turing machine can either halt or run indefinitely given some input, and if it halts we say that it accepts the input. This *halting* is an important notion that will come back later on, so keep it in mind!

At the beginning of Section 2.3 about recursive and recursively enumerable sets, we used the term "algorithm" quite loosely when defining these concepts. Your intuitive notion of an algorithm is probably good, but we would still like to alter the definitions slightly to make them more rigorous and to include the strong notion of the Turing machine.

**Definition 2.7** ([23])**.** A subset $S \subset \mathbb{N}^n$ is called *recursively enumerable* if there exists a Turing machine that halts given an input $I$ if, and only if, $I \in S$.
The set $S$ is called *recursive* if there exists a Turing machine that halts on all inputs of $S$. In this case, $S$ is decidable: the Turing machine can determine whether or not an input is an element of $S$.

Let us use our newfound tool of the Turing machine to show again that the set of even numbers is recursively enumerable.

**Example 2.10.** In order to show that the set of even numbers is recursively enumerable, we have to show that there exists a Turing machine that can determine correctly whether a number is even. Note that our Turing machine need not halt when the input is an odd number!
For this purpose, we again consider a Turing machine with two states: $q_0$ and $q_1$. The way we determine whether a number is even is to make sure the machine halts if, and only if, there are an even number of inputs $I$ on the tape. Consider

$$\delta(q_0, I) = \langle q_1, I, R\rangle, \tag{51}$$
$$\delta(q_1, I) = \langle q_0, I, R\rangle, \tag{52}$$
$$\delta(q_1, \sqcup) = \langle q_1, \sqcup, R\rangle. \tag{53}$$

Note that every time an $I$ is read, the head moves one square to the right and switches to the opposite state. Since we start in state $q_0$, every time we have scanned an even number of $I$'s we are back in state $q_0$, and every time we have scanned an odd number of $I$'s we are in state $q_1$. When our input ends, so we encounter a $\sqcup$ instead of an $I$, and we are in state $q_1$, we continue going right on the tape indefinitely. However, if we are in state $q_0$ when our input ends, there is no command and our program halts. Hence, the Turing machine halts if, and only if, it receives an even number of $I$'s as input, and hence the even numbers are recursively enumerable.

We defined that a program *halts* if there is no command available, but one could do it differently: we could introduce a specific *halting state* $h$. We would simply add a command to go to the halting state whenever there is no command. Additionally, we could add a *reject state* $r$, that we could turn to whenever we have something like a infinite loop. If we add these concepts to our Turing machine, we can show that the set of even numbers is not only recursively enumerable, but recursive as well.

**Example 2.11.** We have two states $q_0$ and $q_1$, and the following rules:

$$\delta(q_0, I) = \langle q_1, I, R\rangle, \tag{54}$$
$$\delta(q_1, I) = \langle q_0, I, R\rangle, \tag{55}$$
$$\delta(q_1, \sqcup) = \langle q_1, \sqcup, R\rangle, \tag{56}$$

just like in our previous example. Let us add the following halting and reject states:

$$\delta(q_0, \sqcup) = \langle h, \sqcup, N \rangle, \tag{57}$$
$$\delta(q_1, \sqcup) = \langle r, \sqcup, N \rangle. \tag{58}$$

This way, whenever we end up in state $q_0$ when our input runs out, the program halts: we have an even number of $I$'s. On the other hand, when we end up in state $q_1$, our input is rejected: the number of $I$'s is odd. So, there exists a Turing machine which determines precisely whether or not something is even or odd, and never runs indefinitely. Therefore, the set of even numbers is a recursive set.

## 2.4 The Halting problem

We are now ready to move on to the Halting problem, which captures the essence of undecidability.

**Definition 2.8** (The Halting problem)**.** The *halting problem* is the problem of determining whether a certain Turing machine halts for a given input, or runs forever.

The question whether a program halts is of interested to us, because we want to know whether or not some input we give the machine is accepted − is the program going to run forever, and are we waiting in vain, or is it just a few more minutes until we get an answer? We want to know! Unfortunately, this is too much to ask. It was proven by Alan Turing in 1936 that the Halting problem is undecidable: there is no general way to tell whether a program is going to halt or not [22]. The formal proof of this statement involves a lot of technicalities, but we disregard these and instead outline the general idea of the proof, which is a proof by contradiction.

Let us assume that we *can* solve the Halting problem. Suppose there is some magical Turing machine that can always correctly determine whether another Turing machine halts given some input. Let us call this magical machine $H$. We can feed $H$ some Turing machine with input, and if this program halts, $H$ outputs 1, and if it does not halt, $H$ outputs 0. So far so good.
Let us go a step further. We create another Turing machine, $H'$, that encompasses $H$, but flips the output of $H$. So if $H$ outputs 1 (halts), then $H'$ outputs 0 (runs forever), and vice versa. Now we do something peculiar: we feed $H'$ *itself* as input! Let us see what happens:

1. Suppose $H'$ halts. In this case, $H$ outputs 1. Note that $H'$ flips this value, so $H'$ outputs 0, meaning it does not halt and runs forever.

2. Suppose $H'$ runs forever. Then, $H$ outputs 0, but again $H'$ flips this value to 1, meaning that $H'$ halts.

In both cases, we arrive at a contradiction. We cannot have that $H'$ both halts and runs forever. We conclude that our assumption is wrong: there cannot exist a magical Turing machine $H$ that always determines whether a program halts or not. See Figure 2 for a visualization.
Let us take our new understanding of the Halting problem and apply it to recursively enumerable sets. These concepts are inherently linked.

**Example 2.12.** The Halting problem set is denoted by

$$S = \{(P, I) : \text{ the program } P \text{ halts given input } I\}. \tag{59}$$

The set $S$ is recursively enumerable, because we can simply design a Turing machine that halts precisely when $P$ halts. If $P$ does not halt, the Turing machine and $P$ both run forever. Note that $S$ cannot be recursive, since if it were, the Halting problem would be decidable.

*Remark* 8 (The barber's paradox). According to the Cambridge Dictionary [24], a *paradox* is "a situation or statement that seems impossible or is difficult to understand because it contains two

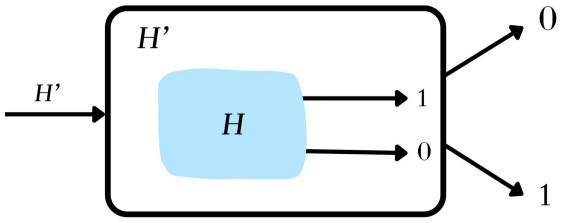


**Figure 2:** *Turing machine $H'$ receiving its own program as input: contradiction*

opposite facts or characteristics". Paraphrased, a paradox is something that contradicts itself. A famous example is the barber's paradox, credited to Bertrand Russell [25]. It goes as follows: imagine a small town, and in this town there is a barbershop. It is owned by the barber, and the barber has one very strict rule: he only shaves town residents who do not shave themselves. At first sight, this seems like a good rule; if a town resident does not shave themselves, then the barber does it for them. On the other hand, if a resident does shave themselves, the barber does not have to shave them, and his rule is obeyed. There is one snag in this story, though, that makes the entire situation a paradox: who shaves the barber? The barber certainly does not shave himself, because in that case the barber would not shave him. However, if the barber does not shave himself, then the barber has to shave himself!
This might remind you of the argument we used in proving the Halting problem. Indeed, this proof has a paradoxical flavor. It is important to note, though, that the Halting problem itself is no paradox! The paradox we encounter in the argument forces us to conclude that such a Turing machine cannot exist: a definitive answer that follows from our proof by contradiction.

## 2.5 A negative solution to Hilbert's Tenth Problem

If we think of the previous sections as baking a cake, this section is the cherry on top. So far, we saw how Diophantine sets capture whether a Diophantine equation can be solved. Moreover, we saw that Diophantine sets are actually equivalent to exponential Diophantine sets. On a seemingly unrelated note, we also acquainted ourselves with the concept of Turing machines and recursively enumerable sets. This section is meant to connect these topics, and this connection is at the core of the undecidability of Hilbert's Tenth Problem. Once we obtain the results below, all the hard work of the previous sections pays off − we can conclude that Diophantine sets are equivalent to recursively enumerable sets, and hence that Hilbert's Tenth Problem is undecidable.

*Remark* 9. Let us pay some attention to an important insight: every Diophantine set is a recursively enumerable set, which is one way of the equivalence we aim to show. This follows from the definition of recursively enumerable sets (Definition 2.7) in the following way. Let us take a Diophantine set $S$, and recall Definition 2.5 of Diophantine sets. This definition tells us that the set $S$ consists of all $n$-tuples $(x_1, \ldots, x_n) \in \mathbb{N}^n$ such that the corresponding Diophantine equation $h \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ has an integer solution, which is an $m$-tuple $(y_1, \ldots, y_m) \in \mathbb{N}^m$. We want to show that the set $S$ is also a recursively enumerable set, which by Definition 2.7 means that we have to find a Turing machine that can enumerate the elements of $S$. We define such a Turing machine program in the following way: when given an $n$-tuple $(x_1, \ldots, x_n)$ as input, go over all $m$-tuples $(y_1, \ldots, y_m)$ and check whether plugging it in $h$ yields $h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$. If we find $h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$, halt.
This program checks if $(x_1, \ldots, x_n) \in S$; in other words, the program enumerates $S$. However, if $(x_1, \ldots, x_n) \notin S$, the program runs forever, because it will try every possible $(y_1, \ldots, y_m) \in \mathbb{N}^m$ and none will work. This is exactly the definition of a recursively enumerable set. The heart of the undecidability here is that you cannot know in advance whether the program will halt or not − it is

equivalent to the halting problem. Therefore, every Diophantine set is recursively enumerable. Note that if we take exponential Diophantine sets instead of Diophantine sets, so allowing exponentiation as well, the exact same proof structure shows that every exponential Diophantine set is recursively enumerable.

Recall our thoughts from Remark 7: if Diophantine sets are equivalent to recursively enumerable sets, then it immediately follows that Hilbert's Tenth Problem is undecidable. In the above remark, we see that one way around the inclusion already holds: every (exponential) Diophantine set is recursively enumerable. To obtain our desired result, we only have to show the other inclusion. Historically, it was first shown that every recursively enumerable set is exponential Diophantine. This important result is known as the DPR Theorem, named after its contributors Davis, Putnam, and Robinson. This result is exactly why we were so concerned with expressing exponentiation in a Diophantine fashion in Section 2.2. Namely, upon succeeding, we show that Diophantine and exponential Diophantine sets coincide, from which immediately follows that every Diophantine set is recursively enumerable!

The remainder of this section is used to touch upon the steps to prove that all recursively enumerable sets are exponential Diophantine: the DPR Theorem. The original proof is the subject of the 1961 paper of Robinson, Davis, and Putnam [26]. A more accessible read of the same proof can be found in Section II.2 of "Logical Number Theory" by C. Smorynski [8]. The following part is based on both of these sources.

**Theorem 2.5** (DPR Theorem)**.** *A set is recursively enumerable if and only if it is exponential Diophantine, i.e. if we allow exponentiation as well as addition and multiplication.*

This theorem states that

$$\{\text{exponential Diophantine sets}\} = \{\text{recursively enumerable sets}\}. \tag{60}$$

The argument for the inclusion $\subseteq$ is given in Remark 9.
To show the other inclusion $\supseteq$, we take a recursively enumerable set $S$ and show that it is exponential Diophantine, i.e. that there exists an exponential Diophantine equation $e \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m]$ such that

$$(x_1, \dots, x_n) \in S \iff \exists y_1 \dots \exists y_m (e(x_1, \dots, x_n, y_1, \dots, y_m) = 0). \tag{61}$$

The first step towards proving this was made by Martin Davis in the early 1950s. He showed that every recursively enumerable set has a representation that is *almost* Diophantine. Namely, for every recursively enumerable set $S$, there is a Diophantine equation $h$ such that [8, Theorem 2.5]

$$(x_1, \dots, x_n) \in S \iff \exists z_1 \forall z_2 \leq z_1 \exists y_1 \leq z_1 \dots \exists y_m \leq z_1 (h(x_1, \dots, x_n, y_1, \dots, y_m, z_1, z_2) = 0). \tag{62}$$

This became known as Davis normal form. It is a considerable step in the desired direction, because this expression is very similar to the one we want to obtain. There is just one issue: the bounded universal quantifier. In the 1961 paper by Robinson, Davis, and Putnam [26], the authors proved that one can eliminate this bounded universal quantifier at the cost of allowing exponentiation in the polynomial $h$. This result is stated and proven in [26, Lemma 3] and [8, Theorem 2.11]. These results provide explicit exponential Diophantine equations that are equivalent to an expression in Davis normal form. We repeat, but do not prove, [8, Theorem 2.11] here to give the interested reader a general idea of the form of such exponential Diophantine equations.

**Theorem 2.6** (Bounded Quantifier Theorem)**.** *Let $h \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m, z_1, z_2]$. In this case, there is a polynomial $f \in \mathbb{Z}[x_1, \dots, x_n, z_1]$ such that, for any $(x_1, \dots, x_n) \in \mathbb{N}^m$ we have*

*(i)* $\forall z_1 (f(x_1, \dots, x_n, z_1) \geq z_1)$

*(ii)* $\forall z_1 \forall z_2 \forall y_1 \leq z_1 \dots \forall y_m \leq z_1 (|h(x_1, \dots, x_n, y_1 \dots, y_m, z_1, z_2)| \leq f(x_1, \dots, x_n, z_1))$

*(iii) For any $z_1$, the following are equivalent:*

*(a)*

$$\forall z_2 \leq z_1 \exists y_1 \leq z_1 \ldots \exists y_m \leq z_1 (h(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, z_2) = 0)$$

*(b)*

$$\begin{aligned} \exists c \exists t \exists v_1 \ldots \exists v_m \Big( & t = f(x_1, \ldots, x_n, z_1)! \quad \wedge \quad 1 + (c+1)t = \prod_{n=0}^{x} (1 + (m+1)t) \quad \wedge \\ & \wedge \quad 1 + (c+1)t \Big| \prod_{j=0}^{z_1} (v_1 - j) \wedge \cdots \wedge 1 + (c+1)t \Big| \prod_{j=0}^{z_1} (v_m - j) \quad \wedge \\ & \wedge \quad 1 + (c+1)t | h(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, c) \Big) \end{aligned}$$

Note that in $(iii)$, $(a)$ is Davis normal form, and $(b)$ contains an exponential Diophantine expression. The conclusion is that, since any recursively enumerable set $S$ can be represented in Davis normal form, and in turn Davis normal form can be represented by exponential Diophantine equations, we know that every recursively enumerable set is exponential Diophantine.

Historically, the above was the first result on the equivalence between recursively enumerable sets and exponential Diophantine sets. It was a serious breakthrough, though, at the time, it did not lead directly to the undecidability of Hilbert's Tenth Problem. That specific result is due to Matiyasevich roughly ten years later. However, Matiyasevich also found another approach to proving the DPR Theorem. This proof omits the starting point of the Davis normal form, and instead directly proves the desired equivalence using Turing machines. Recall from the definition of recursively enumerable sets that there is a Turing machine that can enumerate that set. Matiyasevich's ingenious idea is to encode this Turing machine program into an expression containing only addition, multiplication, exponentiation, and existential quantifiers. They directly give the link to the recursively enumerable set having an exponential Diophantine representation [27].

With the above result, we have all the necessary tools in our toolbox to prove the MRDP Theorem, which is named after Matiyasevich, Davis, Putnam, and Robinson.

**Theorem 2.7** ([28],[23] MRDP Theorem)**.** *A set is recursively enumerable if and only if it is Diophantine.*

This theorem claims the stronger notion that

$$\{\text{Diophantine sets}\} = \{\text{recursively enumerable sets}\}. \tag{63}$$

The argument for the inclusion $\subseteq$ is likewise given in Remark 9.
For the statement that every recursively enumerable set is Diophantine ($\supseteq$), we built the foundation for the proof throughout all previous sections.
By the DPR Theorem (2.5), we know that every recursively enumerable set is exponential Diophantine. Moreover, at the end of Section 2.2, we remarked that every exponential Diophantine set is Diophantine (see Equation (47)). This allows us to conclude that that every recursively enumerable set is Diophantine.

We have proven the fact that recursively enumerable sets and Diophantine sets coincide. As surmised in Remark 7, this leads to the conclusion that Hilbert's Tenth Problem is undecidable: there does not exist a general algorithm that can determine whether a given Diophantine equation has an integer solution.

# 3 The MRDP Theorem versus $\mathbb{Z}[\sqrt{2}]$

The aim of this thesis is to not only give the proof of the undecidability of Hilbert's Tenth Problem over several rings, but also to show the reader the historical timeline of the happenings, and from time to time give some additional remarks. We want to encourage questions such as "who?", "why?", "when?", and "how?", and this section is dedicated to precisely such a question. Namely: what happens if we try to apply the undecidability proof of Hilbert's Tenth Problem over $\mathbb{Z}$ to the ring $\mathbb{Z}[\sqrt{2}]$? The purpose of this section is to provide some insight to this question, and it is of an investigatory nature. We continue with extensive, formal results on the matter in Section 4.

Without a strict wish to be mathematically rigorous, let us simply brainstorm together about some facets of our proof over $\mathbb{Z}$ and whether they are compatible with the structure of $\mathbb{Z}[\sqrt{2}]$. The first thing that comes to mind are Diophantine equations and sets. We ascertained the following: a Diophantine equation is a representation of a Diophantine set. This was illustrated in Example 2.5: the Diophantine equation $x = y^2$ is a representation of the set of perfect squares. Crucial is that we agreed here that we consider only positive integers, in both the coefficients of Diophantine equations and the solutions we allow. However, what if we consider elements of $\mathbb{Z}[\sqrt{2}]$ instead of $\mathbb{N}$? In this case, the representation changes. Note that, among others, the pair $(x, y) = (2, \sqrt{2})$ is a new solution to $x = y^2$. This means that this equation no longer represents the set of perfect squares in $\mathbb{N}$ [4].
The next thing to notice is Pell's equation: $x^2 - dy^2 = 1$. Recall that we considered solutions in $\mathbb{N}^2$, and that we discovered that these solutions have a connection to the unit group of $\mathbb{Z}[\sqrt{d}]$. This connection is a vital component in proving that exponentiation is Diophantine. Though, if we consider solutions in $\mathbb{Z}[\sqrt{2}]^2$ instead of $\mathbb{N}^2$, there is no guarantee that there is still such a connection.
Another subject of attention is the fact that Matiyasevich used the Fibonacci sequence to prove that exponentiation is Diophantine. The Fibonacci numbers are defined to be (positive) integers. Since $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}]$, the Fibonacci sequence is also a sequence in $\mathbb{Z}[\sqrt{2}]$, but the exponential growth that is shown in $\mathbb{Z}$ might not directly transfer to $\mathbb{Z}[\sqrt{2}]$.
It is clear that the proof as it is cannot be directly applied to Hilbert's Tenth Problem over $\mathbb{Z}[\sqrt{2}]$; we encounter problems. Is there a way around these problems? There may be, but we do not go into these. Instead, we view this section as a perfect opportunity to introduce some new concepts. We are here to learn as much as we can, after all. In the remainder of this section we introduce two concepts that do play a role in the proof of Hilbert's Tenth Problem over $\mathbb{Z}$, but we have not explicitly considered yet. We first take a look at why they are important in the original proof, and then we try to adapt them to see how they behave over $\mathbb{Z}[\sqrt{2}]$.

The first new concept we introduce is Gödel numbering. This part is based on an article of the Stanford Encyclopedia of Philosophy [29]. In Section 2.3, we mentioned Gödel's incompleteness theorems. Even though these theorems were, and still are, groundbreaking results, in this thesis we do not concern ourselves with their exact statements, but rather with the proof that Gödel gave. For some background, we do explain their statements informally. Gödel's first incompleteness theorem states that any consistent formal language in which we can do some amount of arithmetic contains statements that cannot be proved or disproved in the system. The second theorem says that such a system cannot prove of itself that it is consistent. These theorems shook the foundation of mathematics in the 1930s; it was formally proven for the first time that the arithmetic most of mathematics is built on contains statements that inherently do not have a proof. As we said, we do not go into these theorems in full rigor, but instead we are interested in a proof technique that Gödel used for the first theorem: Gödel numbering. The goal of Gödel numbering is to assign to every symbol, formula and even theorem and proof in a formal system a unique natural number. This way, we can do arithmetic on formulas!

To illustrate how Gödel numbering works, we apply it to the language of rings that we defined at the

beginning of Section 2. Recall that it consists of variables $x_1, x_2, \ldots$, constants $0, 1$, binary predicates $=, +, \cdot$, connectives $\wedge, \vee, \neg$, quantifiers $\forall, \exists$, and parentheses $(,)$. This is our language, and we can build any formula we wish from it. The next step is to give all of these symbols a natural number. It is not important in which order we do this, but it is very important to keep the ordering fixed once it is determined. For example, let us choose the following numbering:

| | | | |
|---|---|---|---|
| #(‘0’)= 1 | #(‘ =’)= 5 | #(‘∨’)= 9 | #(‘$x_i$’)= $13 + i$ |
| #(‘1’)= 2 | #(‘(’)= 6 | #(‘¬’)= 10 | |
| #(‘+’)= 3 | #(‘)’)= 7 | #(‘∀’)= 11 | |
| #(‘·’)= 4 | #(‘∧’)= 8 | #(‘∃’)= 12 | |

At this point, we have assigned to every element of our vocabulary a natural number. We are not done yet: we want to combine these symbols to construct formulas! An important aspect is that we have to ensure that every formula can be *uniquely* described. This can be done in multiple ways, one of which is pairing functions [30], but we use the method Gödel used: exploiting unique prime factorization. Let us see how this works using a familiar example (Example 2.4):

$$\exists y(x = y^2). \tag{64}$$

Let us start by rewriting this formula such that it is consistent with our language. We rename $x$ and $y$ as follows: $x_1 := x$ and $x_2 := y$. We obtain

$$\exists x_2(x_1 = x_2 \cdot x_2). \tag{65}$$

Using the numbering we fixed in the above table, we can translate this formula into the following string of numbers:

$$[12, 13 + 2, 6, 13 + 1, 5, 13 + 2, 4, 13 + 2, 7] \tag{66}$$

$$= \quad [12, 25, 6, 14, 5, 15, 4, 15, 7]. \tag{67}$$

This string has length nine. To take the leap to unique prime factorization, we take the first nine prime numbers, and raise them to the power of the numbers in our string, as such:

$$g = 2^{12} \cdot 3^{15} \cdot 5^6 \cdot 7^{14} \cdot 11^5 \cdot 13^{15} \cdot 17^4 \cdot 19^{15} \cdot 23^7. \tag{68}$$

We can rely on unique prime factorization that $g$ is the unique representation of Equation (65) in our fixed method. A vital property of this method is that we can not only encode formulas, but we can also decode them. Let us clarify this with an example. Suppose we receive the number 2430. Its prime factorization is:

$$2430 = 2 \cdot 1215 = 2 \cdot 243 \cdot 5 = 2^1 \cdot 3^5 \cdot 5^1. \tag{69}$$

We decode:

$$[1, 5, 1] \implies 0 = 0. \tag{70}$$

Gödel numbering is merely a step in the rigorous proof of Gödel's incompleteness theorems. The interested reader who is fluent in German can read the proof in Gödel's original article [31]; English-speaking readers can find an account in [30].

Of course, Gödel numbering is a very ingenious method in itself, but we want to apply it to something else: Turing machines. Turing machines are countable [2], so they can be indexed. Gödel numbering provides a method to uniquely number Turing machines. We assign natural numbers to the movements of the read-write head, the input and output, and the states [32]. Being able to encode Turing

machine programs this way allows us to encode into a natural number if a certain Turing machine halts given some input, so halting is translated to a property of a natural number. This, in turn, can be represented in a Diophantine way, which means that we can represent the Halting problem set as a Diophantine set. Since the Halting problem is undecidable, undecidability of Hilbert's Tenth Problem follows. This is in essence what Matiyasevich does in his alternative proof of the DPR Theorem [27].

Recall the aim of this section: applying the original undecidability proof to $\mathbb{Z}[\sqrt{2}]$. At this point, we know how Gödel numbering plays a part in the proof over $\mathbb{Z}$, so let us try to adapt Gödel numbering to work in $\mathbb{Z}[\sqrt{2}]$. To do this, we have to take a step back. What exactly is this encoding? Well, the assigning of numbers to objects in our language is in fact an injective mapping from elements of our language to $\mathbb{N}$. Injectivity is required because we do not want two objects to be assigned the same number [33].
Let us think of a way to get such a mapping for $\mathbb{Z}[\sqrt{2}]$. We could in principle directly assign members of $\mathbb{Z}[\sqrt{2}]$ to our objects, but we can also take a different approach: using the units of $\mathbb{Z}[\sqrt{2}]$. We do this hand in hand with learning a new concept: well-orderings.

A subset $S$ of the real numbers is well-ordered if every non-empty subset of $S$ has a least element according to this ordering [34].

**Example 3.1.** The set $\mathbb{N}$ is well-ordered with its usual ordering $<$.
The set $\mathbb{Z}$ is not well-ordered with the usual $<$. Indeed, the set $\mathbb{Z}$ itself does not have a least element. The same holds for the set $\mathbb{R}$.

The well-ordering on $\mathbb{N}$ ensures for example that natural induction is a sound proof method. Moreover, we can use it to show that certain computer programs terminate, and do not have an infinite loop. We run into problems when we turn to $\mathbb{Z}[\sqrt{2}]$. It is not well-ordered with the usual ordering, because for any element $a+b\sqrt{2}$, the element $a+b\sqrt{2}-1$ is smaller. Is there another way to define a well-ordering on $\mathbb{Z}[\sqrt{2}]$? In fact, we can define a well-ordering on any set. However, for $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{2}]$, this is not the usual ordering, so it is not compatible with usual addition and multiplication, and these are precisely the arithmetic operations that we want to preserve. The way to proceed is this: we try to mimic $\mathbb{N}$ inside $\mathbb{Z}[\sqrt{2}]$. Interestingly, in order to do this we can use knowledge we obtained before: properties of the solutions of Pell's equation (Section 2.2).

Recall that the solutions to Pell's equation with $d = 2$ ($x^2 - 2y^2 = 1$) are connected to the units of $\mathbb{Z}[\sqrt{2}]$. We defined the unit group of $\mathbb{Z}[\sqrt{2}]$ as in Equation 22, but it turns out that the unit group is generated by a single element. In the case of $\mathbb{Z}[\sqrt{2}]$, this element is $1+\sqrt{2}$. Hence, we can write the unit group of $\mathbb{Z}[\sqrt{2}]$ as

$$\left(\mathbb{Z}[\sqrt{2}]\right)^\times = \{\pm\left(1+\sqrt{2}\right)^n : n \in \mathbb{Z}\} \quad [18, \text{Example I.2.5}]. \tag{71}$$

There is a connection between this unit group and the solutions to Pell's equation. In Section 2.2, we considered $d = a^2-1$, and in this case the fundamental solution is $(x,y) = (a,1)$. However, $d = 2$ does not satisfy $d = a^2 - 1$ for any positive integer $a$. Instead, we have to find the fundamental solution ourselves. In the case of $d = 2$, this is not so hard. We claim that $(x,y) = (3,2)$ is the fundamental solution. Indeed, it is a solution, since

$$3^2 - 2 \cdot 2^2 = 9 - 8 = 1. \tag{72}$$

Also note that

$$1^2 - 2 \cdot 1^2 = -1, \tag{73}$$

so that $(1,1)$ is not a solution. However, $1+\sqrt{2}$ is a unit of $\mathbb{Z}[\sqrt{2}]$, and it is called the fundamental unit. In the case of $\mathbb{Z}[\sqrt{2}]$, its unit group is of the form in Equation (71). Also note that

$$\left(1+\sqrt{2}\right)^2 = 3 + 2\sqrt{2}. \tag{74}$$

Let us note that the map

$$n \mapsto \left(1+\sqrt{2}\right)^n \tag{75}$$

is injective for $n \geq 0$. Moreover, it is strictly increasing. We have that the sequence of $(1+\sqrt{2})^n$ for $n \in \mathbb{N}$ mimics behavior of $\mathbb{N}$ inside $\mathbb{Z}[\sqrt{2}]$. Let us if this extends to the operations addition and multiplication.

- Multiplication in $\mathbb{Z}[\sqrt{2}]$ models addition in $\mathbb{N}$:

$$\left(1+\sqrt{2}\right)^n \left(1+\sqrt{2}\right)^m = \left(1+\sqrt{2}\right)^{m+n}. \tag{76}$$

- Exponentiation in $\mathbb{Z}[\sqrt{2}]$ models multiplication in $\mathbb{N}$:

$$\left((1+\sqrt{2})^n\right)^m = \left(1+\sqrt{2}\right)^{n \cdot m}. \tag{77}$$

To summarize, what we did is to extend the encoding from $\mathbb{N}$ to (the units of) $\mathbb{Z}[\sqrt{2}]$; we found elements of $\mathbb{Z}[\sqrt{2}]$ that behave similarly to the positive integers. This way, we can easily extend our existing Gödel numbering scheme to $\mathbb{Z}[\sqrt{2}]$. In fact, we are not limited to Gödel numbering. Since we "define" $\mathbb{N}$ in $\mathbb{Z}[\sqrt{2}]$, we can, with a detour, inherit all the properties of $\mathbb{N}$. If we do this rigorously, we can even inherit the undecidability of Hilbert's Tenth Problem. This is the notion of *Diophantine definition*.

This section was a way for us to openly brainstorm and test the extent of our knowledge, and we noticed, that while we cannot directly apply the undecidability proof of Hilbert's Tenth Probelm over $\mathbb{Z}$ to $\mathbb{Z}[\sqrt{2}]$, we did form an idea for a new proof. We build a rigorous mathematical foundation for this new proof in the next section, where we formally define Hilbert's Tenth Problem over more general rings, extend our definition of Diophantine equations and sets, and rigorously define Diophantine definitions. We even explicitly find a Diophantine definition for rings such as $\mathbb{Z}[\sqrt{2}]$, from which we can conclude that Hilbert's Tenth Problem is indeed undecidable over $\mathbb{Z}[\sqrt{2}]$.

# 4 Extending to more general rings

In the previous section, we learned about the aspects that are important in Hilbert's Tenth Problem over $\mathbb{Z}$, and saw how these aspects combine to prove the negative solution. The crown jewel is the MRDP Theorem (Theorem 2.7), which states that Diophantine sets and recursively enumerable sets coincide. Unfortunately, this theorem and its proof cannot simply be extended to rings different from $\mathbb{Z}$. One reason for this is that we only defined our tools, like Diophantine sets and recursively enumerable sets, over $\mathbb{Z}$, and even more specifically over $\mathbb{N}$. Another is that, for more general rings, Pell's equation does not suffice to show that exponentiation is Diophantine. One of the main difficulties of adapting the proof to work on larger rings is to find a good substitute for it. It is discovered that elliptic curves, and their more general counterpart, abelian varieties, can fulfill such a role [35]. To fully understand what these are and how they contribute to a more general proof, we have to start with a clean slate. We do not only have to find a proof for Hilbert's Tenth Problem over more general rings, but first and foremost we have to adapt our problem statement and the definitions we use to fit its new world.

*Remark* 10. Throughout this section, any time we consider a ring $R$, it is a commutative, unitary ring.

Let us give the statement of Hilbert's Tenth Problem over a general ring $R$.

**Definition 4.1** ([9] Generalized Hilbert's Tenth Problem)**.** Consider a ring $R$. Hilbert's Tenth Problem over $R$ asks if there exists a general algorithm that takes as input a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and produces as output *YES* if there exist $y_1 \ldots, y_n \in R$ such that $f(y_1, \ldots, y_n) = 0$.
Alternatively, we can take a subset $S \subseteq R$ and consider Hilbert's Tenth Problem over $R$ with coefficients in $S$. In this case, we take $f \in S[x_1, \ldots, x_n]$. The rest of the problem statement stays the same.

*Remark* 11. In this section, we consider Hilbert's Tenth Problem over $R$ with coefficients in $R$. In what follows, this is what we mean when we talk about Hilbert's Tenth Problem over $R$.

The generalized Hilbert's Tenth Problem is once again a decision problem; we either have to show that there is no such algorithm (the problem is undecidable), or there *is* such an algorithm (it is decidable). We want to find something to which this problem is equivalent which we can use to define more concretely in which cases it is decidable or undecidable. It would be useful if this includes Turing machines, just like recursively enumerable sets. Unfortunately, recursively enumerable sets are only defined over $\mathbb{N}$, see Definition 2.7. However, we can try to carry this concept over to general rings, using some handy tools. We arrive at positive existential theory. This concept helps us to generalize Diophantine equations and sets to a general ring $R$, with the aid of some tools from logic. Let us dive into the definitions.

## 4.1 Positive existential theory

This section is based on E. Bod's Master's thesis "Hilbert's Tenth Problem and some generalizations" [23, Sections 1.2, 1.3] and on B. Poonen's notes "Hilbert's Tenth Problem over rings of number-theoretic interest" [9, Section 4].

In this section we want to define Diophantine sets over a general ring $R$. We do not do this directly (though we technically could: simply replace $\mathbb{Z}$ by $R$ in Definition 2.5), but we find it important to also define the notion of positive existential sets. The reason for this is that over some rings, these concepts are the same, and over other rings, they are different! This sparks our interest, and we want to find out which rings entice one result, and which the other.
As stated in Section 2, Diophantine equations are polynomial equations for which we determine the ring or field of which the coefficients are elements. Moreover, we state in which ring or field we look for solutions. Since we extend to more general rings than $\mathbb{Z}$, from now on we specify what kind of

Diophantine equations we mean. Namely, in what follows, we consider Diophantine equations over $R$: polynomial equations with coefficients in $R$ for which we are interested in solutions in $R$.
In order to build a proper mathematical basis for the concepts we are about to encounter, we turn to our first-order logic preliminaries, from the beginning of Section 2. It is important to note that, in this section, we are working in the language of rings. Let us denote the language of rings by $\mathcal{L}$. Recall that we already defined first-order formulas in the language of rings in Definition 2.3. We go a step further and consider special cases of these: positive existential formulas and Diophantine formulas. We use these concepts to extend the definitions to sentences and theory, which pave the way to understanding undecidability in a more general context.

**Definition 4.2** (Positive existential formula)**.** A *positive existential formula* in $\mathcal{L}$ is a first-order formula in $\mathcal{L}$ of the form

$$\exists x_1 \dots \exists x_n A, \tag{78}$$

where $A$ is built from $+, \cdot, 0, 1, =, \wedge, \vee$, parentheses, and variables. Quantifiers and negation $(\forall, \exists, \neg)$ are not allowed in $S$.

**Definition 4.3** (Diophantine formula)**.** A *Diophantine formula* in $\mathcal{L}$ is a first-order formula in $\mathcal{L}$ of the form

$$\exists x_1 \dots \exists x_n A, \tag{79}$$

where $A$ is built from $+, \cdot, 0, 1, =$, parentheses, and variables. Quantifiers, and, or, and negation $(\forall, \exists, \wedge, \vee, \neg)$ are not allowed in $S$.

*Remark* 12. From the above definitions one can see that a Diophantine formula is a special case of a positive existential formula.

Let us consider some examples.

**Example 4.1.** An example of a positive existential formula in $\mathcal{L}$ is

$$\exists x \exists y((x + 1 = y) \vee (x^2 + z^2 = 2)). \tag{80}$$

A Diophantine formula in $\mathcal{L}$ is, for instance,

$$\exists x(x = y^2). \tag{81}$$

Note that in the above example, some variables appear behind a quantifier at the beginning of the formula, and some do not. We say that a variable that does appear next to such a quantifier is *bound* by that quantifier. Variables that are not bound are called *free* [7]. For example, in Equation (80), the variables $x$ and $y$ are bound, while the variable $z$ is free. This brings us to the following definition. In the remainder of this section, we are always working in the language of rings, so we omit stating it explicitly.

**Definition 4.4** ([9] Sentences)**.** A first-order (respectively positive existential, Diophantine) formula in which all variables are bound by quantifiers is called a first-order (respectively positive existential, Diophantine) *sentence*.

In logic, we can evaluate the truth value of a sentence. In our case, we are specifically working with rings, so the way we do this is by plugging in the elements of our ring $R$ for the bound variables and checking if the sentence is satisfied, i.e. if the polynomial equations hold. If we have a formula instead of a sentence, we additionally have free variables. Before we can check the truth value of a formula in the above way, we have to substitute values $x_1, \dots, x_n \in R$ for all free variables $z_1, \dots, z_n$ of the formula. If $A$ is a formula with $n$ free variables, then the elements $x_i$ that we can substitute in $A$ such that $A$ can be satisfied forms a subset of $R^n$, in the form of $\{(x_1, \dots, x_n) \in R^n : A(x_1, \dots, x_n)\}$. The attentive reader might already see some similarity with the definition of Diophantine sets! Let us formalize this in a definition.

**Definition 4.5** ([9] Subsets)**.** Let $A$ be a positive existential formula over $R$. A subset of $R^n$ of the form $\{(x_1, \ldots, x_n) \in R^n : A(x_1, \ldots, x_n)\} \subseteq R^n$ is called a positive existential subset over $R$.
Similarly, if $A$ is a Diophantine formula, then such a subset is called a Diophantine subset over $R$.

Let us apply this definition in our natural habitat: $\mathbb{Z}$.

**Example 4.2.** If we consider Hilbert's Tenth Problem over the integers, then the above definition reduces to our original definition of Diophantine sets (Definition 2.5, especially Remark 3). Indeed, let us take $R = \mathbb{Z}$. According to the definition above, a Diophantine subset $S \subseteq \mathbb{Z}^n$ is of the form

$$S = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : A(x_1, \ldots, x_n)\}, \tag{82}$$

where $A$ is a Diophantine formula with $n$ free variables $x_1, \ldots, x_n$, and $m$ bound variables. Let us call the bound variables $y_1, \ldots, y_m \in \mathbb{Z}$. Since $A$ is Diophantine formula, it is of the form

$$A(x_1, \ldots, x_n) = \exists y_1 \ldots \exists y_m (h(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0). \tag{83}$$

for some polynomial $h \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$.
This is very similar to how we defined Diophantine sets in Definition 2.5, but here we used solutions in $\mathbb{N}^n$ instead of $\mathbb{Z}^n$. We did this to simplify the original proof, since we know that Hilbert's Tenth Problem over $\mathbb{Z}$ and over $\mathbb{N}$ are equivalent. However, if we wanted to be truly rigorous, we would have to extend our initial definition to $\mathbb{Z}$ instead of $\mathbb{N}$, since $\mathbb{Z}$ is a ring and $\mathbb{N}$ is not.

This is wonderful, our generalized definition of Diophantine sets works for the integers! This encourages us to continue to the next step, which is of importance. In the previous section, we devoted an entire subsection to it: the concept of a Turing machine, and in particular of a recursively enumerable set. Recursively enumerable sets are crucial, because they build the bridge between a set and the concept of computability. However, unfortunately for us, recursively enumerable sets are defined only for (positive) integers. This means that for our generalized problem, we need something else to give us a lift to the field of computability theory. This something is a theory. It encapsulates whether a positive existential formula is satisfiable, i.e. whether we can plug elements of our ring into the formula to make it hold.

**Definition 4.6** ([9] Theories)**.** Let $R$ be a ring. The *first order theory* (respectively *positive existential theory*) of $R$ in the language of rings is the set of first order (respectively positive existential) sentences that are true when we plug in elements of $R$ for the variables in the sentence. A theory is called *decidable* if there is a Turing machine with input a sentence and output whether or not the sentence is in the theory, i.e. whether or not the sentence is true.

*Remark* 13. You might think, why go to all this trouble to define positive existential formulas, sets, and theories? Can we not just directly define Diophantine sets over a general ring $R$? The answer to that question is that, in general, this is not enough. The reason that we did not define positive existential sets in Section 2, but only Diophantine sets, is that over $\mathbb{Z}$, these are exactly the same. So, for certain rings, these concepts are equivalent, bringing us to the topic of Lemma 1.12 and Theorem 1.13 in Bod's thesis [23], and the topic of Proposition 8.5 and Corollary 8.6 of Poonen's notes [9]. What are the conditions so that positive existential sets are equivalent to Diophantine sets? Let us find out!

**Lemma 4.1** ([23])**.** *Let $R$ be a ring, and let $S \subseteq R$ be a subset. Let $S'$ be the ring generated by the elements of $S$.*
*Suppose there exist polynomials $f, g \in S'[x, y]$ such that for all $a, b \in R$,*

$$f(a, b) = 0 \iff a = 0 \wedge b = 0, \tag{84}$$
$$g(a, b) = 0 \iff a = 0 \vee b = 0. \tag{85}$$

*In this case, a subset of $R^n$ is Diophantine over $R$ if, and only if, the subset is positive existential over $R$.*

*Proof.* Let us prove both implications.
$\Longrightarrow$ : By Remark 12, every Diophantine formula is a positive existential formula. By Definition 4.5, it immediately follows that every Diophantine subset is positive existential.
The backward implication is trickier.
$\Longleftarrow$ : Suppose a subset $R'$ of $R^n$ is positive existential over $R$. Let $\exists y_1 \dots \exists y_m(A(x_1, \dots, x_n))$ be the corresponding positive existential formula, so $R'$ is of the form $\{(a_1, \dots, a_n) \in R^n : A(a_1, \dots, a_n)\}$. From the definition of positive existential formulas, $A$ consists of polynomial equations that are concatenated using the logical operators $\wedge$ and $\vee$. Our aim is to translate $A$ in such a way that we get rid of the logical operators so that we end up with a single equation in $A$. Namely, in this case our positive existential formula is a Diophantine formula by definition. To obtain this, we apply the following steps repeatedly until we have the desired result.

1. Convert every equation of the form $a = b$ to $c = a - b = 0$ (as we did in Remark 1);
2. Convert any expression of the form $c = 0 \wedge d = 0$ to $f(c, d) = 0$. We can do this because they are equivalent by Equation (84);
3. Convert any expression of the form $c = 0 \vee d = 0$ to $f(c, d) = 0$. These are equivalent by Equation (85).

Repeating these steps, we can translate $A$ to an equivalent Diophantine equation. We conclude that our positive existential formula $\exists y_1 \dots \exists y_m(A(x_1, \dots, x_n))$ is also Diophantine. It follows that every positive existential subset is Diophantine. □

This lemma is already a useful result in itself, but we can use it to show an even stronger result.

**Theorem 4.2** ([23])**.** *Let $R$ be an integral domain (a commutative ring without zero divisors), and let $K$ be its field of fractions. Let $S \subseteq R$ be a subset. Let $S'$ be the ring generated by the elements of $S$, and let $K'$ be the field of fractions of $S'$. Suppose that $K$ is not algebraically closed and that $K$ has an extension $K(\alpha)/K$ for which the norm map $N : K(\alpha)/K \to K$ is given by a polynomial over $K'$. In this case, a subset of $R^n$ is Diophantine over $R$ if, and only if, the subset is positive existential over $R$.*

*Proof.* We want to apply Lemma 4.1. Keeping the same notation, this means that we need to find polynomials $f, g \in S'[x, y]$ such that Equations (84) and (85) hold.
We assume that $R$ is an integral domain, so for all elements $a, b \in R$, we have

$$ab = 0 \Longleftrightarrow a = 0 \vee b = 0. \tag{86}$$

This allows us to take $g(x, y) = xy \in S'[x, y]$ to satisfy Equation (85).
What remains to be done is to find a polynomial $f \in S'[x, y]$ satisfying Equation (84). We use our assumption that the norm map is a polynomial in $K'[x, y]$. Namely, for an element $x + \alpha y \in K(\alpha)/K$, we know that $N(x + \alpha y)$ is given by a polynomial with coefficients in $K'$. Since $K'$ is the field of fractions of $S'$, there exists an element $r \in S' \setminus \{0\}$ such that $rN(x + \alpha y)$ is given by a polynomial in $S'[x, y]$. Indeed, this is the case for $r$ the common denominator of the coefficients of $N(x + \alpha y)$. This way, we ensure that the coefficients of $rN(x + \alpha y)$ are in $S'$. Note

$$rN(x + \alpha y) = 0 \Longleftrightarrow N(x + \alpha y) = 0 \Longleftrightarrow x + \alpha y = 0 \Longleftrightarrow x = 0 \wedge y = 0. \tag{87}$$

The first equivalence follows from the fact that $S' \subseteq R$, which means that $S'$ is an integral domain, and from the fact that $r \neq 0$. We see that the polynomial $f(x, y) = rN(x + \alpha y) \in S'[x, y]$ satisfies Equation (84).
We satisfy the conditions for Lemma 4.1, and when we apply it we can conclude that indeed a subset of $R^n$ is Diophantine over $R$ if, and only if, it is positive existential over $R$. □

Let us try to make sense of this theorem over our familiar integers.

**Example 4.3.** Consider $R = \mathbb{Z}$. In this example, we use Theorem 4.2 to show that in $\mathbb{Z}^n$, a positive existential subset is equivalent to a Diophantine subset.
We know that $\mathbb{Z}$ is an integral domain. Its field of fractions is the field of rational numbers $\mathbb{Q}$. In this case, we take $S = \mathbb{Z} \subseteq \mathbb{Z}$. Hence $S' = \mathbb{Z}$, and the field of fractions of $S'$ is $K' = \mathbb{Q}$ again. We know that $\mathbb{Q}$ is not algebraically closed. For instance, the roots of $x^2 - 2 \in \mathbb{Q}[x]$, $\pm\sqrt{2}$, are not elements of $\mathbb{Q}$.
Let us take $\sqrt{2} \notin \mathbb{Q}$ as our algebraic element. We consider the field extension $\mathbb{Q}(\sqrt{2})$. The elements of $\mathbb{Q}(\sqrt{2})$ are of the form $a + b\sqrt{2}$, with $a, b \in \mathbb{Q}$. Define the norm map $N : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}$ as $N(x + y\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2 \in \mathbb{Q}[x, y]$.
We satisfy all conditions of Theorem 4.2, so we can conclude that a subset $S \subseteq \mathbb{Z}^n$ is Diophantine if, and only if, it is positive existential.
We have our result, but let us investigate a little more closely why. Recall from Lemma 4.1 that we need, for $R = \mathbb{Z}$, polynomials $f, g \in \mathbb{Z}[x, y]$ with some conditions on $f$ and $g$, namely those in Equation (84) and (85). The existence of $g$ follows from the fact that $\mathbb{Z}$ is an integral domain. Let us explicitly find $f$. Note that $N(x + \sqrt{2}y) = x^2 - 2y^2$ is not only a polynomial with coefficients in $\mathbb{Q}$, but more specifically it is a polynomial with coefficients in $\mathbb{Z}$. Hence, for $r = 1 \in \mathbb{Z}$, we have that

$$1 \cdot N(x + y\sqrt{2}) = 0 \iff x + y\sqrt{2} = 0 \iff x = 0 \wedge y = 0. \tag{88}$$

This means that $f(x, y) = x^2 - 2y^2 \in \mathbb{Z}[x, y]$ satisfies Equation (84).

Note that, since positive existential and Diophantine sets over $\mathbb{Z}$ are the same, stating that Hilbert's Tenth Problem is undecidable is the same as stating that the positive existential theory of $\mathbb{Z}$ is undecidable. More generally, for any ring $R$ for which Theorem 4.2 holds, the undecidability of Hilbert's Tenth Problem over $R$ is equivalent to the undecidability of the positive existential theory of $R$ [9].

We developed a notion of Hilbert's Tenth Problem in a more general setting: we familiarized ourselves with Diophantine sets over a general ring $R$, and we learned about theories and how we can determine their (un)decidability, but we want more! We know that the positive existential theory over $\mathbb{Z}$ is undecidable. We worked very hard to obtain this result, so we want to use it. What if there is some way that we can use the undecidability over $\mathbb{Z}$ to show undecidability over $R$? Fortunately, there is, and it is called a positive existential or Diophantine definition, based on whether you are working with positive existential or Diophantine sets. Though, in what follows, we take $R$ to satisfy the conditions of Theorem 4.2, so we can use these terms interchangeably. Our aim is to, in a way, embed the positive existential theory of $\mathbb{Z}$ into the positive existential theory of another ring $R$. If we do this, we can translate positive existential formulas over $\mathbb{Z}$ to positive existential formulas over $R$. After doing this correctly, the undecidability carries over [23].

Let us dive into the definition.

**Definition 4.7** ([36] Diophantine definition)**.** Let $R$ be a ring and let $S \subseteq R$ be a subset. We say that $S$ has a *Diophantine definition over* $R$, or that $S$ is *Diophantine over* $R$, if there exists a finite system of polynomials with coefficients in $R$,

$$\Sigma : f_i(t, x_1, \ldots, x_n) \in R[t, x_1, \ldots, x_n] \quad \text{for } i = 1, 2, \ldots, m, \tag{89}$$

such that for any $\tau \in R$ we have that

$$\tau \in S \iff \exists a_1 \ldots \exists a_n (f_i(\tau, a_1, \ldots, a_n) = 0) \tag{90}$$

where $a_1, \ldots, a_n \in R$ and $i = 1, 2, \ldots, m$.

*Remark* 14. Let us give some attention to the fact that this definition is in some sense remarkably similar to the definition of Diophantine subsets (Definition 4.5). Indeed, the above definition is actually

an algebraic instead of logical version of the previous logical definition, and it focuses specifically on $R$ instead of $R^n$. Why do we bother mentioning the latter definition? Well, what we did was translate the form to one that we can more easily apply to the rings we are going to look at, namely (spoiler alert) rings of integers. Moreover, this form lends itself to a short and elegant proof why this Diophantine definition is so important! This is the subject of the proposition below. This proposition shows exactly why we can use Diophantine definitions to extend our undecidability result for $\mathbb{Z}$ to more general rings.

**Proposition 4.1** ([36])**.** *Suppose $R$ is a ring containing $\mathbb{Z}$, and $\mathbb{Z}$ has a Diophantine definition over $R$. In this case, there is no algorithm to determine whether or not an arbitrary finite system of polynomial equations with coefficients in $R$ has solutions in $R$. In other words, Hilbert's Tenth Problem over $R$ is undecidable.*

*Proof.* Take a polynomial $h(t_1, \ldots, t_r) \in \mathbb{Z}[t_1, \ldots, t_r]$. By assumption, $\mathbb{Z}$ has a Diophantine definition over $R$. Let $\Sigma : f_i(t, x_1, \ldots, x_n) \in R[t, x_1, \ldots, x_n]$ for $i = 1, 2 \ldots, m$ be the system of equations satisfying this definition. Consider the system of equations

$$h(t_1, \ldots, t_r) = 0, \quad f_i(t_j, x_{j,1}, \ldots, x_{j,n}) = 0, \quad 1 \leq i \leq m, 1 \leq j \leq r. \tag{91}$$

From the definition of Diophantine definition, we have $t_j \in \mathbb{Z} \Leftrightarrow \exists a_{j,1} \ldots \exists a_{j,n}(f_i(t_j, x_{j,1}, \ldots, x_{j,n}) = 0)$ for $a_{j,i} \in R$. Hence, the system of equations (91) has solutions in $R$ if, and only if, $h$ has solutions in $\mathbb{Z}$. Therefore, if there exists an algorithm to determine whether or not the system of equations (91) has solutions in $R$, then there exists an algorithm to determine whether or not $h$ has solutions in $\mathbb{Z}$. However, since we know there is no such algorithm for $\mathbb{Z}$, there can be no such algorithm for $R$. □

To paraphrase, we found an explicit way and explicit conditions to transfer the undecidability result from $\mathbb{Z}$ to a different ring. The time has come to get our hands dirty and to use these results for some specific rings. The question remains, which rings do we choose? There are many options. Well, we stay a little bit in our comfort zone, and consider a general class of rings of which $\mathbb{Z}$ is simply a specific instance: rings of integers.

## 4.2 Undecidability over quadratic rings of integers

In the sections that follow, we focus on Hilbert's Tenth Problem over rings of integers of a number field $K$, denoted by $\mathcal{O}_K$. These concepts are formally defined in Definition 4.8 and Definition 4.9. However, to ease ourselves into this segue, we start slow and consider quadratic rings of integers in the current section. We use the specific case of rings of integers over quadratic number fields to better understand the nature of the formal definition of general rings of integers. This functions as a stepping stone to the next section, Section 4.3, in which we broaden our horizon to rings of integers over any number field $K$.

Historically, after the publishing of the MRDP Theorem (Theorem 2.7), mathematicians solved Hilbert's Tenth Problem for several special cases of more general rings, one of which is quadratic rings of integers. This result was already shown quite soon after the proof of the original problem, in 1975, by J. Denef [37]. This section serves to give an outline of the proof of this result. It is particularly interesting, because it makes explicit use of the definition of Diophantine definition (Definition 4.7) and illustrates the strength of carrying over the undecidability result from $\mathbb{Z}$ via Proposition 4.1.

Before we continue, it is necessary to consider the formal definition of a number field and its ring of integers.

**Definition 4.8** ([38] Number field)**.** A number field $K$ is a finite field extension of $\mathbb{Q}$, i.e.

$$[K : \mathbb{Q}] < \infty. \tag{92}$$

**Example 4.4.** An extension of degree one is certainly finite, so $\mathbb{Q}$ itself is a number field.

*Remark* 15. If $K$ is a number field, and we take $\alpha \in K$, then there exists a monic polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. We can see this as follows. Note that Definition 4.8 is equivalent to saying that a number field $K$ is a finite-dimensional vector space over $\mathbb{Q}$. Therefore, $\{1, \alpha, \alpha^2, \dots\}$ must be linearly dependent, which means there exist coefficients such that

$$c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0, \text{ with } c_i \in \mathbb{Q} \tag{93}$$

such that the $c_i$ are not all zero. Hence, $\alpha$ is a root of a polynomial with coefficients in $\mathbb{Q}$. We can make this polynomial monic by dividing every term by $c_n$ [38].

We use Definition 4.8 to define rings of integers.

**Definition 4.9** ([38] Ring of integers)**.** Let $K$ be a number field. Its ring of integers $\mathcal{O}_K \subseteq K$ is the set of all elements $\alpha \in K$ such that there is a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$, i.e.

$$\mathcal{O}_K = \{\alpha \in K : f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[X]\}. \tag{94}$$

It can be proven that $\mathcal{O}_K$ is a subring of $K$.

**Example 4.5.** The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

This definition is all well and good, but why are monic polynomials with integer coefficients so special? Is there a reason we chose to define rings of integers this way? Well, there certainly is. Let us see how we get to this definition in the specific case of rings of integers of quadratic number fields. The following part is based on Keith Conrad's notes "Factoring in Quadratic Fields" [39].

Let $K$ be a quadratic number field. It is of the following form:

$$K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}, \tag{95}$$

where we take $d \in \mathbb{Z}$ to be nonsquare and nonzero. The aim of the ring of integers $\mathcal{O}_K$ of $K$ is to "mimic" integer behavior inside $K$: we want to find a subring of $K$ that has the same properties as $\mathbb{Z}$ does in $\mathbb{Q}$. From Section 2.2, we are familiar with the following ring:

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}. \tag{96}$$

In what follows, we learn that the ring of integers of $K$ is sometimes $\mathbb{Z}[\sqrt{d}]$, but sometimes it is larger! To see exactly how this works, we define the following operation: conjugation.

**Definition 4.10** (Conjugates)**.** Let $\alpha \in K = \mathbb{Q}(\sqrt{d})$, so $\alpha$ is of the form $\alpha = x + y\sqrt{d}$ for some $x, y \in \mathbb{Q}$. The conjugate $\overline{\alpha}$ of $\alpha$ is defined as

$$\overline{\alpha} = x - y\sqrt{d}. \tag{97}$$

*Remark* 16. With these conjugates in our toolbox we can highlight some interesting facts. First of all, we have the following equalities for any $\alpha, \beta \in K$:

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}, \quad \overline{\overline{\alpha}} = \alpha. \tag{98}$$

Moreover, some expressions including conjugates are known to always lie in $\mathbb{Q}$; in such cases, the square-root term of the element disappears. For instance, let $\alpha \in K$. We have that

$$\alpha = \overline{\alpha} \tag{99}$$
$$\iff \quad x + y\sqrt{d} = x - y\sqrt{d} \tag{100}$$
$$\iff \quad y = 0 \tag{101}$$
$$\iff \quad \alpha \in \mathbb{Q}. \tag{102}$$

Moreover, we have that

$$\alpha + \overline{\alpha} = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x \in \mathbb{Q} \tag{103}$$
$$\text{and} \quad \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 \in \mathbb{Q}. \tag{104}$$

The elements $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are special to us and deserve a name.

**Definition 4.11.** For $\alpha \in K$, we define the *trace* and the *norm* of $\alpha$. These are defined respectively as

$$\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}, \tag{105}$$
$$N(\alpha) = \alpha\overline{\alpha}. \tag{106}$$

*Remark* 17. Indeed, the above norm is the very same norm map that we are already familiar with, but in this case we are working with $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$.

By Remark 16, the trace and the norm are rational numbers. This helps us to prove that Remark 15 holds in the quadratic case: every $\alpha \in K$ is a root of a monic polynomial with coefficients in $\mathbb{Q}$ of degree two. Indeed, the polynomial

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - \mathrm{Tr}(\alpha)x + N(\alpha) \tag{107}$$

has as its two roots precisely $\alpha$ and $\overline{\alpha}$, and has coefficients in $\mathbb{Q}$.

This forms our bridge to rings of integers: if we consider the polynomial in Equation (107), and add the requirement that its coefficients are in $\mathbb{Z}$, then the roots of such polynomials are precisely the elements of the ring of integers, by Definition 4.9. This means that our search of the elements of the ring of integers starts with the question: when exactly are both the trace and the norm of an element of $K$ integers?
Let us start with the trace. Recall that we have $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2x$. This means that we at least need $x \in \mathbb{Z}$, or $x = \pm\frac{1}{2}$. The norm is a bit trickier, so let us start from the other side. We take an educated guess and see if it is exactly the ring of integers of $K$. Our educated guess is $\mathbb{Z}[\sqrt{d}]$. It has elements of the form $x + y\sqrt{d}$ with $x, y \in \mathbb{Z}$, so for an element of this ring, its trace is certainly an integer. What about its norm? Take $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. We obtain

$$N(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2, \tag{108}$$

which is most certainly an integer, since $x, y, d$ are integers by assumption. At this point we are sure that elements of $\mathbb{Z}[\sqrt{d}]$ are roots of a monic polynomial with integer coefficients of degree two. Indeed, the polynomial of Equation (107) has integer coefficients, since we ensured that the trace and norm are integers. The question remains: are we done now? Do we have $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_K$? For one thing, we know that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, but do we always have the other inclusion? The big reveal is that in many cases, this is so, but most certainly not in all cases.

**Example 4.6.** Take $d \equiv 1 \mod 4$. Note that the element $\frac{1+\sqrt{d}}{2} \in \mathbb{Q}(\sqrt{d})$ is not an element of $\mathbb{Z}[\sqrt{d}]$, since $\frac{1}{2} \notin \mathbb{Z}$, but it is a root of a monic polynomial of degree two with integer coefficients! Consider:

$$x^2 - x + \frac{1 - d}{4}. \tag{109}$$

This polynomial has integer coefficients since $d \equiv 1 \mod 4$, and it has $\frac{1+\sqrt{d}}{2}$ and its conjugate as its two roots.

This is very insightful and leads us to the following result.

**Theorem 4.3.** *Consider the quadratic number field $K = \mathbb{Q}(\sqrt{d})$. Its ring of integers $\mathcal{O}_K$ is*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \mod 4. \end{cases} \tag{110}$$

**Example 4.7.**

- For $K = \mathbb{Q}(\sqrt{2})$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$,
- For $K = \mathbb{Q}(\sqrt{5})$ we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$,
- For $K = \mathbb{Q}(i)$ we have $\mathcal{O}_K = \mathbb{Z}[i]$ (Gaussian integers).

*Remark* 18. Recall that we took $d$ to be a nonsquare and nonzero integer. This means that we allow $d$ to be negative, in which case the corresponding ring of integers of $\mathbb{Q}(\sqrt{d})$ is a complex ring. We can simplify our lives a little bit by considering the following scenario: we take $d > 1$ a positive integer. We claim that we can denote the two the two possible rings of integers of the number field $\mathbb{Q}(\sqrt{d})$ by $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}[\sqrt{-d}]$. Let us see why this holds.
If we have $d \equiv 2, 3 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and we are already in on of our two mentioned cases. However, if $d \equiv 1 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. We can avoid this, though, by noting that $d \equiv 1 \mod 4 \implies -d \equiv 3 \mod 4$. Hence, we obtain $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$.

The above remark allows us to continue this section with only using the ring $\mathbb{Z}[\sqrt{d}]$ for a ring of integers of a quadratic number field. We simply distinguish between $d > 1$ and $d < 0$. Keep in mind that for $d > 1$, the ring $\mathbb{Z}[\sqrt{d}]$ is a real ring. On the other hand, for $d < 0$, it is a complex ring. The remainder of this section consists of an explicit proof of the undecidability of Hilbert's Tenth Problem over real rings of integers of a quadratic number field, i.e. we take $d > 1$. We follow the original proof of J. Denef [37], sometimes using the version in [23] for some additional clarification on the proof steps.

*Remark* 19. Let us take a break and consider our current position. So far, we learned about rings of integers of quadratic number fields, and we know where their definition comes from. At this point, we are ready for the following theorem. Its statement ensures that $\mathbb{Z}$ has a Diophantine definition in $\mathbb{Z}[\sqrt{d}]$. As proven in Proposition 4.1, this means that undecidability of Hilbert's Tenth Problem transfers from $\mathbb{Z}$ to $\mathbb{Z}[\sqrt{d}]$!

**Theorem 4.4** ([37]). *Let $\mathbb{Z}[\sqrt{d}]$ be a quadratic ring of integers where $d > 1$. There exists a (finite) system $\Sigma$ of Diophantine equations in the variables $t, x, \ldots, s$ such that the following two statements hold:*

*(i) If $\Sigma$ has a solution $(t, x, \ldots, s) \in \mathbb{Z}[\sqrt{d}]$, then $t \in \mathbb{Z}$.*

*(ii) If $k \in \mathbb{N}$, then $\Sigma$ has a solution $(t, x, \ldots, s) \in \mathbb{Z}[\sqrt{d}]$ with $t = k^2$.*

Our main goal is to construct such a system of equations as in Theorem 4.4 explicitly. Indeed, the following theorem proposes a candidate for such a system of equations.

**Theorem 4.5** ([37], [23]). *We consider a real quadratic ring of integers $\mathbb{Z}[\sqrt{d}]$, i.e. $d \equiv 2, 3 \mod 4$. Let $(u, v)$ be a nontrivial solution of Pell's equation, so $u^2 - dv^2 = 1$ and $(u, v) \neq (1, 0)$. Define $e := u^2 - 1$. Let $\Sigma$ be the following system of equations in variables $t, x, y, l, m, z, w, h, q, r, s$.*

*(a)* $x^2 - ey^2 = 1$

*(b)* $l^2 - em^2 = 1$

*(c)* $m^2 - y^2 t = zy^4$

*(d)* $t = w^2$

*(e)* $y^2 - t = 1 + h^2 + q^2 + r^2 + s^2$.

*This system of equations has the properties mentioned in Theorem 4.4, i.e. the following statements hold:*

*(i) If $\Sigma$ has a solution in $\mathbb{Z}[\sqrt{d}]$, then $t \in \mathbb{Z}$,*

*(ii) For every $k \in \mathbb{N}$, there is a solution for $\Sigma$ in $\mathbb{Z}[\sqrt{d}]$ with $t = k^2$.*

The proof of this statement is quite tricky, so we need the help of three lemmas. We state and prove these lemmas first, and after this we consider the proof of Theorem 4.5.

Pell's equation plays a fundamental role in the following lemmas. For a quick refresher, the reader can take a look at Section 2.2. As in that section, we take $d$ to be a nonsquare integer, and we take $a = d^2 - 1$. In Section 2.2, we found that Pell's equation has infinitely many solutions, and that they are of the form $(x_n + y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^n$, with $(x_1, y_1)$ the fundamental solution. Moreover, we discussed some lemmas that were useful to see how these solutions model exponential behavior. There is one additional general result about the behavior of the solutions to Pell's equation that is important to mention for this section.

**Lemma 4.6** ([37])**.** *Let $d, n, k \in \mathbb{N}$, and $d > 1$. Consider Pell's equation: $x^2 - dy^2 = 1$. Denote by $(x_n, y_n)$ the solutions to Pell's equation. We have*

$$y_{nk}^2 \equiv y_n^2 k^2 \mod y_n^4. \tag{111}$$

Since this is a technical statement that is merely used for the proof of the main result, we omit its proof. The interested reader can find it in [23, Lemma 6.5] or [37, Lemma 3].

Let us move on to the remaining two lemmas. The following lemma puts some restrictions on the solutions of a Pell equation that considers solutions in $\mathbb{Z}[\sqrt{d}]^2$ (like Equation $(a)$). Namely, in a specific case, we can conclude that for a solution $(x, y)$ of such an equation, $y^2$ is a positive integer − it loses its square-root term!

**Lemma 4.7** ([37] Real)**.** *We consider a real quadratic ring of integers $\mathbb{Z}[\sqrt{d}]$. Let $(u, v)$ be a nontrivial solution of Pell's equation, so $u^2 - dv^2 = 1$ and $(u, v) \neq (1, 0)$. Define $e := u^2 - 1$. If we moreover have $x^2 - ey^2 = 1$ for some $x, y \in \mathbb{Z}[\sqrt{d}]$, then $y^2 \in \mathbb{N}$.*

*Proof.* Rewriting $u^2 - dv^2 = 1$ and substituting $e$, we obtain $e = dv^2$. Note that this gives

$$1 = x^2 - ey^2 = x^2 - dv^2y^2 = (x - vy\sqrt{d})(x + vy\sqrt{d}). \tag{112}$$

This means that $(x+vy\sqrt{d}) =: w$ is a unit in $\mathbb{Z}[\sqrt{d}]$, and its multiplicative inverse is $x-vy\sqrt{d} =: w^{-1}$. At this point we want to find an expression containing $y^2$, but no square roots. To obtain this, we subtract $(x + vy\sqrt{d})$ and its inverse and square them. This gives

$$w - w^{-1} = 2vy\sqrt{d} \tag{113}$$
$$\implies (w - w^{-1})^2 = 4v^2y^2d \tag{114}$$
$$\implies w^2 - 2ww^{-1} + (w^{-1})^2 = 4v^2y^2d \tag{115}$$
$$\implies w^2 + (w^{-1})^2 = 4v^2y^2d + 2. \tag{116}$$

We know that $w$ is a unit, so $N(w) = \pm 1$. Since the norm is defined by multiplying $w$ with its conjugate $\overline{w} \in \mathbb{Q}(\sqrt{d})$, we know that $w^{-1} = \pm\overline{w}$, since $ww^{-1} = 1$. From this we can infer $4v^2y^2d+2 = w^2 + \overline{w}^2 \in \mathbb{Q}$, because of the following reasoning: under the Galois map, an element is sent to its conjugate. Moreover, if an element is mapped to itself, this implies that it is an element in the base field, which is in our case $\mathbb{Q}$. Since $w^2 + \overline{w}^2$ is mapped to itself, we have that it is in $\mathbb{Q}$. Therefore, $4v^2y^2d + 2 \in \mathbb{Q}$, which implies that $y^2 \in \mathbb{Q}$, since $v, d \in \mathbb{Q}$ by assumption. Since $y \in \mathbb{Z}[\sqrt{d}]$, we must conclude that $y^2 \in \mathbb{Z}$. Moreover, $\mathbb{Z}[\sqrt{d}]$ is a real ring, so all squares are nonnegative; this implies that $y^2 \in \mathbb{N}$. □

In the preceding lemma, we introduced the conjugate of an element of $\mathbb{Z}[\sqrt{d}]$. It is defined analogously to Definition 4.10. Moreover, we have to define congruence in a general ring $R$. For this purpose, let us consider the definition of a factor ring.

**Definition 4.12** (Factor ring [18])**.** Let $R$ be a ring and $I \subseteq R$ and ideal. The set of residue classes

$$R/I := \{x + I \subseteq R : x \in R\} \tag{117}$$

is a ring, and it is called the factor ring of $R$ with respect to $I$.

Note that for elements $x, y \in R$, and $I$ and ideal in $R$, the following holds:

$$x + I = y + I \iff x \equiv y \mod I \iff x - y \in I. \tag{118}$$

Let $R = \mathbb{Z}[\sqrt{d}]$, and let $I$ be the principal ideal generated by $z$, for some $z \in \mathbb{Z}[\sqrt{d}]$. This means that $I$ is of the form $I = (z) = \{wz : w \in \mathbb{Z}[\sqrt{d}]\}$. Combining this with our notion of a factor ring, we obtain that for $x, y, z \in \mathbb{Z}[\sqrt{d}]$:

$$x \equiv y \mod (z) \iff x - y \in (z) \iff x - y = wz \quad \text{for some } w \in \mathbb{Z}[\sqrt{d}]. \tag{119}$$

If the reader is unfamiliar with, or needs a refresher on ideals or factor rings, this can be found in [18, Section 2].

The following lemma uses congruence and conjugates explicitly. We claim that certain congruence conditions on elements of $\mathbb{Z}[\sqrt{d}]$ and their conjugates force these two elements to be equal.

**Lemma 4.8** ([23])**.** *Suppose $x, y, z \in \mathbb{Z}[\sqrt{d}]$, and $x \equiv y \mod (z)$. Let $\overline{x}, \overline{y}, \overline{z}$ denote the conjugates of $x, y, z$ respectively, and suppose $0 \leq x, y < z$ and $0 \leq \overline{x}, \overline{y} < \overline{z}$. In this case, we have that $x = y$.*

*Proof.* For a contradiction, let us suppose that $x \neq y$, so $x - y \neq 0$. Since $x \equiv y \mod (z)$, we have that there exists $w \in \mathbb{Z}[\sqrt{d}]$ with $w \neq 0$ such that $x - y = wz$. In the next step, we take (real) absolute values of $x - y$ and $\overline{x} - \overline{y}$ and multiply them to obtain the following inequality:

$$|x - y| \cdot |\overline{x} - \overline{y}| = |wz| \cdot |\overline{wz}| = |w\overline{w}| \cdot |z\overline{z}| = |N(w)| \cdot |z\overline{z}| \geq |z\overline{z}|. \tag{120}$$

The inequality follows from the fact that $N(w)$ is an integer by Equation (23), and it is nonzero since $w \neq 0$. However, this contradicts our assumptions that $0 \leq x, y < z$ and $0 \leq \overline{x}, \overline{y} < \overline{z}$. Indeed,

$$0 \leq x, y < z \implies |x - y| < z \tag{121}$$

$$\text{and} \quad 0 \leq \overline{x}, \overline{y} < \overline{z} \implies |\overline{x} - \overline{y}| < \overline{z}, \tag{122}$$

from which

$$|x - y| \cdot |\overline{x} - \overline{y}| < z\overline{z} \tag{123}$$

directly follows. However, Equation (120) states that $|x - y| \cdot |\overline{x} - \overline{y}| \geq z\overline{z}$. From this contradiction we conclude that $x = y$. □

Do you recall the purpose of the above lemmas? Their aim is to aid in the proof of Theorem 4.5. With these results in our toolbox, we are ready for the proof of this main result. For clarity, we repeat the system of equations $\Sigma$ here:

(a) $x^2 - ey^2 = 1$

(b) $l^2 - em^2 = 1$

(c) $m^2 - y^2 t = zy^4$

(d) $t = w^2$

(e) $y^2 - t = 1 + h^2 + q^2 + r^2 + s^2$.

*Proof of Theorem 4.5.* (i) Suppose $\Sigma$ has a solution with $t, x, y, l, m, z, w, h, q, r, s$ in $\mathbb{Z}[\sqrt{d}]$. We want to show that $t \in \mathbb{Z}$. By Lemma 4.7 we have that $y^2, m^2 \in \mathbb{N}$, so in particular $y^2 > 0$. Equation $(c)$ gives

$$m^2 - y^2 t = zy^4 \implies \frac{m^2}{y^2} - t = zy^2 \implies \frac{m^2}{y^2} \equiv t \mod y^2. \tag{124}$$

This implies that also $\frac{m^2}{y^2} \equiv \bar{t} \mod y^2$, since $y^2, m^2 \in \mathbb{N}$ so they are their own conjugates. Hence $t \equiv \bar{t} \mod y^2$.
Since we are working in a real ring, all squares are nonnegative. From Equation $(d)$, we can see that $t \geq 0$. Moreover, $\bar{t} \geq 0$, since Equation $(d)$ also implies $\bar{t} = \overline{w}^2$. Equation $(e)$ signifies that $t, \bar{t} < y^2 = \overline{y}^2$. This means that $0 \leq t, \bar{t} < y^2$, and since $y^2 \in \mathbb{N}$ it is its own conjugate so we satisfy the requirements for Lemma 4.8. From this lemma we can conclude that $t = \bar{t}$, which directly implies that $t \in \mathbb{N}$.

(ii) We want to show that for every $k \in \mathbb{N}$, there is a solution for $\Sigma$ in $\mathbb{Z}[\sqrt{d}]$ with $t = k^2$. Let us take some $k \in \mathbb{N}$. We make use of the fact that all solutions to Pell's equation are $(x_n, y_n)$ for $n = 0, 1, 2, \ldots$. We denote by $(x_n(u), y_n(u)) \in (\mathbb{Z}[\sqrt{d}])^2$ solutions to $x^2 - ey^2 = 1$. Pick $n \in \mathbb{N}$ such that $y_n(u) > k$. Set $x = x_n(u), y = y_n(u), l = x_{nk}(u)$, and $m = y_{nk}(u)$. It follows that Equations $(a)$ and $(b)$ are satisfied.
By Lemma 4.6, there exists a $z$ that satisfies Equation $(c)$.
Moreover, set $w = k$ so we obtain $t = k^2$. This means that Equation $(d)$ is satisfied.
Lastly, we know that $y^2, k^2 \in \mathbb{N}$. Since $y^2 > t = k^2$ from Equation $(e)$, we know that $y^2 - t \in \mathbb{N}$. By Lagrange's theorem (Theorem 2.1), we know that integers $h, q, r, s$ exist such that Equation $(e)$ is satisfied. Hence, $\Sigma$ indeed has a solution in $\mathbb{Z}[\sqrt{d}]$.

□

As we determined in Remark 19, this proves that Hilbert's Tenth Problem is undecidable for rings of the form $\mathbb{Z}[\sqrt{d}]$ for an integer $d > 1$! We did so by constructing a Diophantine definition of $\mathbb{Z}$ in $\mathbb{Z}[\sqrt{d}]$, so that undecidability over the integers transfers to $\mathbb{Z}[\sqrt{d}]$. One can also construct such a Diophantine definition for $\mathbb{Z}[\sqrt{-d}]$, but the proof of this result is slightly trickier than the real case. The interested reader can find it in [37] or [23, Section 6.3].

*Remark* 20. Theorem 4.5 elegantly shows a Diophantine definition of $\mathbb{Z}$ in $\mathbb{Z}[\sqrt{d}]$ with $d > 1$. A very crucial role is fulfilled by Pell's equation. The solutions to Pell's equation give a natural connection between $\mathbb{Z}$ and the unit group of $\mathbb{Z}[\sqrt{d}]$. Namely, the exponents of the solutions behave as $\mathbb{Z}$. However, a simple way to see that this connection does not extend to general rings of integers is to consider complex rings of integers. The units of the Gaussian integers are $\{\pm 1, \pm i\}$, and the units of $\mathbb{Z}[\sqrt{d}]$ for $d < 1$ are $\{\pm 1\}$. The connection between the units and the solutions to Pell's equation is lost.

## 4.3 Undecidability over rings of integers of a general number field $K$

In the previous section we considered Hilbert's Tenth Problem over quadratic rings of integers. This possible generalization was already discovered quite soon after Matiyasevich's proof in 1970. However, mathematicians would not be mathematicians if they did not investigate whether this result could be generalized even further. Quadratic rings of integers are a rather specific case, and the natural sequent question is to consider general rings of integers. That is to say, rings of integers over any number field $K$, not just those of degree two. Interestingly enough, this question showed itself to be easier to ask than to answer. Only extremely recently, the proof that confirms the undecidability of Hilbert's Tenth Problem over general rings of integers was published. Even more interesting is that this result was obtained independently, yet very close together in time, via two slightly different ways: one published by Koymans and Pagano in December 2024 [35], and the other by Alpöge, Bhargava, Ho, and Shnidman in January 2025 [40], both in preprint. Meanwhile, Koymans and Pagano published

their second version in April 2025. Unfortunately, the full proof of this result is outside of the scope of this thesis. Therefore, we dedicate this section instead to understanding the theorem statements from which undecidability follows. Along the way, we give an account of the contributions that helped accomplish this breakthrough, and the chronological order in which they happened. Moreover, we aim to intuitively explain the proof methods used in the proofs of the main result.
In order to understand the theorem statements, we need some additional background knowledge. Namely, both of these statements rely on abelian varieties; one in full generality, and one in their one-dimensional case: elliptic curves. Let us find out what these concepts entail.

The definition of abelian varieties itself relies on another definition: that of an algebraic variety. Namely, an abelian variety is a special case of an algebraic variety. In turn, an algebraic variety is the zero locus − or solution set − of a set of polynomials over some field $K$. For example, if you take $\mathbb{R}^2$, and you take the polynomials $y - x^2 = 0$ and $x - y = 0$, then their intersection points form an algebraic variety.
An abelian variety over $K$ is an algebraic variety over $K$ for which you define addition and inverse using maps. That is to say, you define a group structure on the algebraic variety. We usually denote an abelian variety over a field $K$ by $A$. In this case, the points on $A$ that form a group are called the $K$-rational points on $A$, and we denote them by $A(K)$. Note how an algebraic variety is a geometric object, and by defining a group structure on it we build a bridge from geometry to algebra. As the name abelian variety suggests, the group structure is commutative. Moreover, abelian varieties are projective; they include points at infinity [41].

The most famous examples of an abelian varieties are elliptic curves: they are one-dimensional abelian varieties. Since elliptic curves are very interesting to study in themselves, a bit easier to understand than general abelian varieties, and useful later on in this section, we take some time to take a look at their properties. The following part is based on the lecture notes for the course Security and Coding, by J. Top [42].

An *elliptic curve* over a field $K$ is given by an equation of the form

$$y^2 = x^3 + ax + b, \tag{125}$$

where we additionally require $\text{char}(K) \neq 2, 3$. As mentioned, we add a point at infinity: $\mathcal{O}$. Why this is required becomes clear later on. The points on an elliptic curve $E$ form a set of the form

$$E(K) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}. \tag{126}$$

The next step is to define a group structure on $E(K)$. Interestingly, we take a geometric approach to this! We illustrate this using figures from [42], illustrated with additional explanation. The important part is that we have to define a way to add two points, $P$ and $Q$, on the elliptic curve, such that their sum is again a point on the elliptic curve. Moreover, a group structure requires inverses and an identity element.

1. Figure 3: In this picture you see an elliptic curve $E$. On it, two points are specified, named $P$ and $Q$. We want to add $P$ and $Q$. Note that in order to define such a group law, the new point has to be on $E$ as well. How we do this is shown in the next step.

2. Figure 4: Draw a line $L$ through $P$ and $Q$. Since $E$ is defined by a cubic equation, $L$ always has a third intersection point with the curve.

3. Figure 5: Let us call this third intersection point $R$. You might think this is our new point, but we are not quite there yet. Instead, our new point $P \oplus Q$ (or simply $P + Q$) is the *reflection* of $R$ in the $x$-axis.

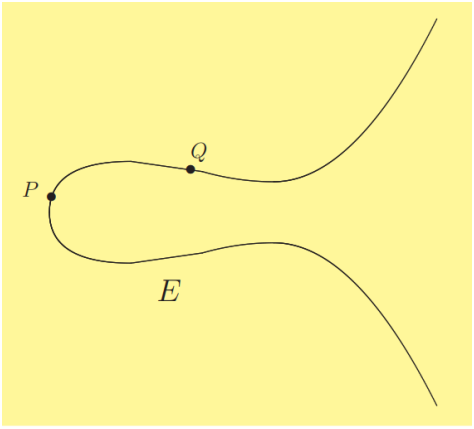


**Figure 3:** *Two points $P$ and $Q$ on an elliptic curve $E$.*

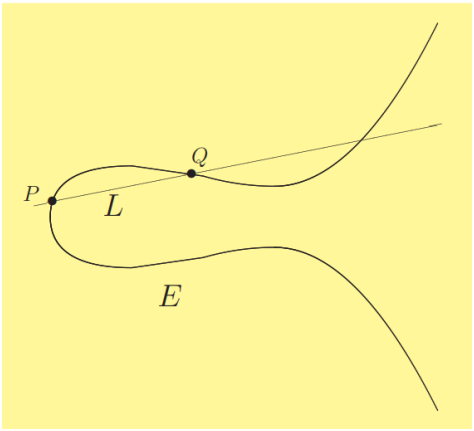


**Figure 4:** *The line $L$ through $P$ and $Q$ always has a third intersection point.*

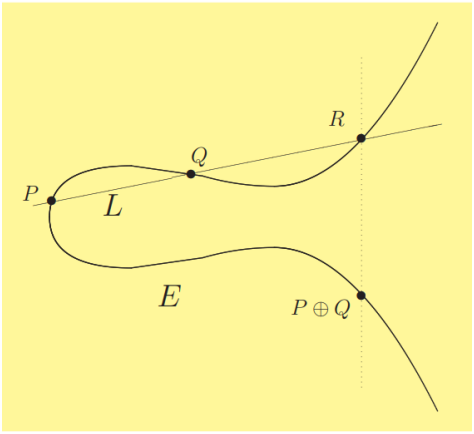


**Figure 5:** *To add $P$ and $Q$, reflect the intersection point in the $x$-axis.*

There are some other situations that we could encounter. For example, what if we want to add the point $P$ to itself? In this case, we take $L$ to be the tangent line to the curve at the point $P$. The point $P+P$ is then the reflection of the intersection of $L$. One other interesting situation arises when we want to add the point $P$ to its reflection in the $x$-axis: the point $-P$. In this case, the line $L$ is the vertical line through $P$ and $-P$, but where is its third intersection point? This is where the point $\mathcal{O}$ comes in. We say that the line $L$ intersects the curve $E$ at infinity. Reflecting infinity yields infinity, so adding $P$ and $-P$ gives the point at infinity. We notice that $\mathcal{O}$ is the identity element, and that $-P$ is the inverse of $P$. The following theorem shows that the rules we defined above indeed put a group structure on the points of $E$.

**Theorem 4.9** ([42])**.** *Addition* $(+)$ *on* $E(K)$ *forms a group law. Indeed,*

*(i)* $P+\mathcal{O}=\mathcal{O}+P=P$ *for all* $P\in E$*,*

*(ii)* $P+(-P)=\mathcal{O}$ *for all* $P\in E$*,*

*(iii)* $P+(Q+R)=(P+Q)+R$ *for all* $P,Q,R\in E$*,*

*(iv)* $P+Q=Q+P$ *for all* $P,Q\in E$*.*

Note that the last line means that the points of $E$ even form a *commutative* group.

Let us revert back to the general case: abelian varieties. A known result, by the name of the Mordell-Weil Theorem, states that for a number field $K$, and an abelian variety $A(K)$, the group structure actually constitutes a finitely generated abelian group [43]. This comes in handy, because we can use the structure theorem for finitely generated abelian groups. Recall that its statement is as follows.

**Theorem 4.10** ([44] Structure theorem for finitely generated abelian groups)**.** *For any finitely generated abelian group* $A$*, there exist a unique nonnegative integer* $r$ *and a unique (possibly empty) finite sequence* $(d_1,\dots,d_m)$ *of positive integers satisfying* $d_m|d_{m-1}|\dots|d_1$*, such that*

$$A\cong\mathbb{Z}^r\times\mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_m\mathbb{Z}. \tag{127}$$

This nonnegative integer $r$ is of great interest to us, so we give it a name.

**Definition 4.13** (Rank)**.** Given a finitely generated abelian group $A$, the nonnegative integer $r$ mentioned in Theorem 4.10 is called the *rank* of $A$.

What this rank signifies is how many *copies* of $\mathbb{Z}$ can be found in $A$. It shows the structure of the elements of infinite order of $A$. The part of Equation (127) that does not include $r$ (which is $\mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_m\mathbb{Z}$) is called the *torsion* part of $A$. This torsion part contains the elements of finite order.

When we talk about the rank in terms of *copies* of $\mathbb{Z}$, this might ring a bell. Namely, to transfer Hilbert's Tenth Problem to more general rings, our approach is to simulate, or find behavior similar to that of $\mathbb{Z}$ inside this more general ring. A copy should have something to do with this! Indeed, this is in extremely rough terms the idea of the main result, and the reason why rank is so important to it. In particular, we want to have *rank stability*: the property that the rank of an abelian variety over some field does not change when we view it over a larger field. With this in mind, let us move on to the main results.

The key step in the proof of the MRDP Theorem (Theorem 2.7) for Hilbert's Tenth Problem over $\mathbb{Z}$ is showing that exponentiation can be expressed in a Diophantine fashion. This relies heavily on the solutions of Pell's equation. However, this method does not extend to more general rings. Historically, an idea to solve this problem is to instead use elliptic curves. We discuss the first result on this topic, which is once again shown independently: by B. Poonen in 2002 [45], and by G. Cornelissen, T. Pheidas, and K. Zahidi in 2005 [46].

**Theorem 4.11.** *Let $F \subseteq K$ be number fields, and let $\mathcal{O}_F$ and $\mathcal{O}_K$ be their respective rings of integers. If there exists an elliptic curve $E$ over $F$ such that*

$$\text{rank}(E(F)) = \text{rank}(E(K)) = 1, \tag{128}$$

*then there exists a Diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$.*

Paraphrased, this result states the following: we are looking for an elliptic curve which is defined over some field $F$. We want this curve to have a certain property: if you look at it in a different setting, namely extend the field over which it is defined, then its general structure remains the same. Let us elaborate on this. What the equation says is that if you extend this base field, then the rank of the group of the elliptic curve remains the same: the infinite part does not grow. Note that the entire group might grow, in which case specifically the torsion part grows. Another option is that it simply stays the same. The question is, what is so special about this infinite part? Well, this infinite part determines the arithmetic structure of the group. Hence, what the theorem actually says is: if we can carry over the important structure from $E(F)$ to $E(K)$, then we can also carry over properties from $F$ to $K$. This, in turn, enables us to give a Diophantine definition of $\mathcal{O}_F$ in $\mathcal{O}_K$!

*Remark* 21. Note that if we take $F = \mathbb{Q}$, then its ring of integers is $\mathcal{O}_F = \mathbb{Z}$. According to this result, if we show that there exists an elliptic curve $E$ such that $\text{rank}(E(\mathbb{Q})) = \text{rank}(E(K)) = 1$, then $\mathbb{Z}$ has a Diophantine definition over $\mathcal{O}_K$. By Proposition 4.1, this means that Hilbert's Tenth Problem over $\mathcal{O}_K$ is undecidable! Hence, after the development of this result, the search for such an elliptic curve took off.

At this point there is good news and bad news. As usual, the bad news first: such an elliptic curve is quite hard to find. Good news: mathematician Alexandra Shlapentokh proved that the same result can be reached with looser assumptions [47]. Namely, she showed that Equation (128) can be replaced by the following condition:

$$\text{rank}(E(\mathbb{Q})) = \text{rank}(E(K)) > 0. \tag{129}$$

This is a less restrictive assumption that gives the same result. Indeed, we do not strictly need that the rank is 1, but any positive rank suffices to carry over arithmetical properties. It is still crucial, though, to require $\text{rank}(E(\mathbb{Q})) = \text{rank}(E(K))$. To summarize, if we can find an elliptic curve with this property, then Hilbert's Tenth Problem over $\mathcal{O}_K$ is undecidable.

### Koymans and Pagano

Mathematicians P. Koymans and C. Pagano spent the years after this result trying to construct an elliptic curve that satisfies Equation (129). More than a decade later, they succeeded! Their full proof can be found in their paper "Hilbert's Tenth Problem via additive combinatorics" [35]. Their methods are very advanced, so we do not dive into them in this thesis. However, we do aim to give an intuitive idea of the methods they used and where they stem from.

The authors begin with a simple equation for an elliptic curve $E$ over some field $F$. They let $E$ be defined by the equation

$$y^2 = (x - a_1)(x - a_2)(x - a_3). \tag{130}$$

This elliptic curve does not yet satisfy the desired properties; some things need to be adapted. The first thing the authors do to tweak this curve is apply something called a *twist*. They multiply the equation by $t := d(c - a_1 d)(c - a_2 d)(c - a_3 d)$. This gives the elliptic curve $E^t$, given by

$$ty^2 = (x - a_1)(x - a_2)(x - a_3). \tag{131}$$

The advantage of this is that this curve is known to have positive rank. The authors argue that indeed, the point $(x, y) = (\frac{c}{d}, \frac{1}{d^2})$ is nontorsion, i.e. of infinite order.

The trickiest part is the following: the authors need to control the rank growth when they consider $E$ over a field extension $K/F$. For a general twist $t$, this is extremely difficult. To overcome this hurdle, the authors use a key insight: the use of additive combinatorics. They notice that for specific choices of $d, c - a_1 d, c - a_2 d$, and $c - a_3 d$, namely choosing them all to be specific prime numbers, the rank growth control is acquired. From the existence of an elliptic curve with the property that $\text{rank}(E(F)) = \text{rank}(E(K)) > 0$, the undecidability of Hilbert's Tenth Problem over any ring of integers is a fact by Remark 21!

*Remark* 22. What is additive combinatorics? In the lecture notes for the course "Introduction to additive combinatorics" for ETH Zürich [48], E. Kowalski gives an almost philosophical remark on what this field of mathematics entails. His exact words are: "Like many mathematical terminology, "additive combinatorics" is both perfectly accurate and deeply misleading. It is accurate because its meaning is clear to the mathematical community, and reflects well the early history of the subject; it is misleading because it hides the breadth and importance this topic has acquired in recent years."
Though, if one feels that the meaning of the term is not clear, how does one learn what is considered additive combinatorics and what is not? One way is to dive into the history of additive combinatorics. Interestingly, the term "additive combinatorics" is not very old: it was coined in 2006 with the publishing of a book of the same name by T.C. Tao and V.H. Vu [49], [50]. The authors explain: "Additive combinatorics is the theory of counting additive structures in sets". Additive gives the sense of working in abelian groups, and combinatorics makes one think of counting. However, even though the name is relatively new, results from almost 200 years prior are deemed important results in the field. For example:

*Theorem* 4.12 (Cauchy, 1813 [48]). *Let $p$ be a prime number. If $A \subset \mathbb{Z}/p\mathbb{Z}$ and $B \subset \mathbb{Z}/p\mathbb{Z}$ are arbitrary nonempty sets, then we have*

$$|A + B| \geq \min(p, |A| + |B| - 1), \tag{132}$$

*where $|\cdot|$ denotes the cardinality of a set, and $A + B$ is the set of all elements of the form $a + b$ with $(a, b) \in A \times B$.*

This theorem sets a lower bound on the size of the sumset of $A$ and $B$: it is either bigger than or equal to $p$, or bigger than the sum of the sizes of $A$ and $B$. This already gives a feel for additive combinatorics: we have abelian groups ($\mathbb{Z}/p\mathbb{Z}$ is even a field), and counting (cardinality of a set). Other important theorems in the subject are Van der Waerden's Theorem (1928) and the Erdós-Szemerédi Theorem (1983) [48].
As mentioned, though, there have been and still are many recent developments in additive combinatorics that have made the field more complex than its name can capture. For one, some interesting results are about non-abelian groups. Moreover, it turns out that there are connections between additive combinatorics and other fields of mathematics that were previously unthought of. For example, additive combinatorics has applications in ergodic theory, analysis, and research on prime numbers [48].

*Remark* 23. Peter Koymans from Utrecht University, and Carlo Pagano from Concordia University met each other in graduate school, and have worked together ever since. Koymans says that Hilbert's Tenth Problem already sparked his interest in undergraduate school. Throughout his time working with Pagano, this interest only grew. In an interview with Quanta Magazine [4], Koymans said: "I spent a few days every year thinking about it and getting horribly stuck. I'd try three things and they'd all blow up in my face."
After a conference in 2022, Koymans and Pagano decided to fully focus on finding an elliptic curve that satisfies the desired properties to solve Hilbert's Tenth Problem over general rings of integers. In only a few years, they prevailed. This just goes to show that even though a problem feels impossible to solve, and your attempts seem fruitless, collaboration and resilience bring you a very long way.

*Remark* 24. Both Koymans and Pagano have posted video lectures on their result online. The interested reader is encouraged to add them to their watch list. Koymans's web seminar from May 15th

2025 can be found in [51]. The video lecture from Pagano from February 14th 2025 can be found in [52].

### Alpöge, Bhargava, Ho, and Shnidman

Merely a month after Koymans and Pagano published their result, Hilbert's Tenth Problem over rings of integers was proven to be undecidable via a slightly different approach. In their paper "Rank stability in quadratic extensions and Hilbert's Tenth Problem for the ring of integers of a number field" [40], authors Alpöge, Bhargava, Ho, and Shnidman divert from trying to find an elliptic curve satisfying Equation (129), but instead use a different result from Shlapentokh, together with B. Mazur and K. Rubin. This different result is:

**Theorem 4.13** ([36])**.** *Let $K/F$ be a quadratic extension of number fields. Suppose there exists an abelian variety $A(F)$ such that*

$$\operatorname{rank}(A(F)) = \operatorname{rank}(A(K)) > 0. \tag{133}$$

*In this case, Hilbert's Tenth Problem is undecidable over the ring of integers of any number field.*

This is a different statement from the elliptic curve result. In a way, it is more restrictive, since we require a *quadratic* extension of number fields. However, it is also less restrictive in the sense that we consider general abelian varieties instead of elliptic curves.
Alpöge, Bhargava, Ho, and Shnidman focused on this result: their aim was to find an abelian variety that satisfies the conditions of Theorem 4.13, and they did so! Interestingly, the authors use additive combinatorics for their proof as well, just like Koymans and Pagano.

The idea behind their proof is the following: let $K$ be a quadratic extension of the number field $F$; it is of the form $K = F(\sqrt{d})$ for some nonsquare and nonzero integer $d$. It is important to note that one can construct an abelian variety by taking the Jacobian of a curve in one's base field. For example, the authors consider the family of curves

$$C_n : y^2 = x^\ell + n, \tag{134}$$

where $n \in F$ and $\ell$ is some prime that is chosen is a smart way. The authors proceed by taking the abelian variety $A := J_n$, where $J_n$ denote the Jacobian of $C_n$. This approach is taken because for this specific case, one can determine the rank of this abelian variety, where in general the rank of abelian varieties is very hard to determine. Namely, for a smart choice of $n$ involving $d$ and $\ell$, it is known that $A = J_n$ has rank zero. Recall, however, that we want positive rank! This problem is solved once again using a twist $t$ to produce another abelian variety $A^d$. This $A^d$ is constructed in such a way that it has a nontorsion point, to ensure positive rank. The authors note that $A^d$ has exactly the same structure over $K$ both and $F$, so it must have stable rank. We have

$$\operatorname{rank}(A^d(K)) = \operatorname{rank}(A(F)) + \operatorname{rank}(A^d(F)) = \operatorname{rank}(A^d(F)) > 0, \tag{135}$$

where we make use of the fact that $\operatorname{rank}(A(F)) = 0$. In conclusion, the abelian variety $A^d$ satisfies the requirements for Theorem 4.13, from which the undecidability of Hilbert's Tenth Problem over general rings of integers follows.

# 5 Conclusion

The aim of this thesis was to study Hilbert's Tenth Problem and its connections to number theory and mathematical logic. We began with the original problem over the integers, and showed that Diophantine sets are equivalent to recursively enumerable sets. This remarkable equivalence connects number-theoretic and logical concepts, and leads to the conclusion that Hilbert's Tenth Problem is undecidable over $\mathbb{Z}$. A key step in the proof involves Pell's equation; we used the properties of its solutions to show that exponentiation is Diophantine.
We then extended our focus to rings of integers in quadratic number fields. In this setting, we introduced the concept of Diophantine definition, and we used it to show that we can translate the undecidability of Hilbert's Tenth Problem over $\mathbb{Z}$ to the case of certain more general rings. We considered the case of real quadratic rings of integers by explicitly constructing a Diophantine definition. From this, undecidability of Hilbert's Tenth Problem over real quadratic rings of integers follows.
Lastly, we considered the even more general case of rings of integers of general number fields. We saw that the tools we used for its quadratic equivalent are no longer sufficient, and we examined abelian varieties and elliptic curves, and how they are used to prove that Hilbert's Tenth Problem over general rings of integers is undecidable.

Research on Hilbert's Tenth Problem is far from finished. There are several rings and fields over which it is still an open problem, the most famous of which is the field of rational numbers. There are promising partial results, such as those related to Mazur's conjecture and reductions to the homogeneous Diophantine problem, but a definitive proof is yet to be found [45], [8].

More than a century after Hilbert stated his famous 23 problems, their influence is still felt. His tenth problem, in particular, has sparked developments that connect fields of mathematics from logic and computation to number theory. The fact that new results are still being published − including undecidability results for general rings of integers mere months ago − emphasizes its impact. Even though the original question has been answered, its generalizations continue to be a subject of research. I, for one, look forward to what the future holds. To answer the question stated in the introduction: are there limits to what mathematics can do? Maybe there are, but keep in mind: knowing that we cannot know is knowledge all the same. That is the elegance of undecidability.

# References


[1] M. Davis, "Hilbert's tenth problem is unsolvable," *The American Mathematical Monthly*, vol. 80, 1973.

[2] R. Zach, *Sets, Logic, Computation: An Open Introduction to Metalogic*. Independently Published, 2021, accessed April 10, 2025. [Online]. Available: https://slc.openlogicproject.org/

[3] M. Davis, "Foreword to hilbert's tenth problem," https://logic.pdmi.ras.ru/~yumat/H10Pbook/foreword.htm, 1993, accessed: 2025-04-25.

[4] J. Howlett, "New proof probe the limits of mathematical trurh," 2025, quanta Magazine article. [Online]. Available: https://www.quantamagazine.org/new-proofs-probe-the-limits-of-mathematical-truth-20250203/

[5] Y. Watase, "Lagrange's four-square theorem," *Formalized Mathematics*, vol. 22, no. 2, pp. 141–145, 2014. [Online]. Available: https://fm.mizar.org/2014-22/pdf22-2/lagra4sq.pdf

[6] G. Priest, *An Introduction to Non-Classical Logic: From If to Is*, 2nd ed., ser. Cambridge Introductions to Philosophy. Cambridge University Press, 2008.

[7] J. Barwise and J. Etchemendy, *Language, Proof and Logic*. CSLI Publications, 1999.

[8] C. Smorynski, *Logical Number Theory I, An Introduction*. Springer-Verlag, 1991.

[9] B. Poonen, "Hilbert's tenth problem over rings of number-theoretic interest," https://math.mit.edu/~poonen/papers/aws2003.pdf, 2003, lecture notes from the Arizona Winter School, March 15–19, 2003.

[10] J. Koenigsmann, "Defining $\mathbb{Z}$ in $\mathbb{Q}$," 2013. [Online]. Available: https://arxiv.org/abs/1011.3424

[11] T. Andreescu, D. Andrica, and I. Cucurezeanu, *An Introduction to Diophantine Equations: A Problem-Based Approach*. Birkhäuser, 2010. [Online]. Available: https://link.springer.com/book/10.1007/978-0-8176-4549-6

[12] E. Massop, "Hilbert's tenth problem," Bachelor's Thesis, University of Leiden, 2012.

[13] D. Hart, "An exploration of diophantine equations," Bachelor's Thesis, Washington and Lee University, 2024, accessed April 10, 2025. [Online]. Available: https://digitalarchive.wlu.edu/_flysystem/fedora/2025-02/wlu_ir_hart_math_2024.pdf

[14] J. Robinson, "Definability and decision problems in arithmetic," *The Journal of Symbolic Logic*, vol. 14, no. 2, pp. 98–114, 1950. [Online]. Available: https://www.jstor.org/stable/2266514

[15] D. Fitzpatrick, J. Connor, and E. Robertson, "Julia robinson and hilbert's 10th problem," https://mathshistory.st-andrews.ac.uk/Extras/Robinson_Hilbert_10th/, 2008, interview with Julia Robinson, MacTutor History of Mathematics Archive, University of St Andrews.

[16] S. Groen, "Matijasevic's theorem: Diophantine descriptions of recursively enumerable sets," Bachelor's Thesis, University of Groningen, 2017, accessed April 22, 2025. [Online]. Available: https://fse.studenttheses.ub.rug.nl/15275/

[17] D. C. Marshall, E. Odell, and M. Starbird, *Number Theory Through Inquiry*. Washington, DC: Mathematical Association of America, 2007.

[18] J. Top, "Algebraic structures," http://www.math.rug.nl/~top/dic.pdf, 2017, based on Dutch lecture notes by L.N.M. van Geemen, H.W. Lenstra, F. Oort, and J. Top. University of Groningen, 2nd year Bachelor Mathematics.

[19] A. Church, "A note on the entscheidungsproblem," *Journal of Symbolic Logic*, vol. 1, no. 1, p. 40–41, 1936.

[20] R. Zach, "Hilbert's program," *The Stanford Encyclopedia of Philosophy*, 2023, first published July 31, 2003; substantive revision September 29, 2023. [Online]. Available: https://plato.stanford.edu/entries/hilbert-program/

[21] D. Hilbert, "David hilbert's radio address - english translation," https://old.maa.org/press/periodicals/convergence/david-hilberts-radio-address-english-translation, published by the Mathematical Association of America. Accessed: 2025-04-23.

[22] A. M. Turing, "On computable numbers, with an application to the entscheidungsproblem," *Proceedings of the London Mathematical Society*, vol. s2-42, no. 1, pp. 230–265, 1936. [Online]. Available: https://www.cs.ox.ac.uk/activities/ieg/e-library/sources/tp2-ie.pdf

[23] E. Bod, "Hilbert's tenth problem and some generalizations," Master's thesis, University of Utrecht, 2009.

[24] Cambridge Dictionary definition of "paradox". [Online]. Available: https://dictionary.cambridge.org/dictionary/english/paradox

[25] Philosophy Terms, "Barber paradox," accessed 2025-06-09. [Online]. Available: https://philosophyterms.com/barber-paradox/

[26] M. Davis, H. Putnam, and J. Robinson, "The decision problem for exponential diophantine equations," *Annals of Mathematics*, vol. 74, no. 3, pp. 425–436, 1961. [Online]. Available: https://www.jstor.org/stable/1970289

[27] Y. V. Matiyasevich, "A new proof of the theorem on exponential diophantine representation of enumerable sets," *Zapiski Nauchnykh Seminarov LOMI*, vol. 60, pp. 75–92, 1976, translated in Math. Notes, Vol. 29, No. 5, pp. 355–364, 1981. Translated by J. P. Jones and L. Guy.

[28] Y. I. Manin, *A Course in Mathematical Logic for Mathematicians*, 2nd ed., ser. Graduate Texts in Mathematics. Springer, 2010, vol. 53.

[29] P. Raatikainen, "Gödel's Incompleteness Theorems," in *The Stanford Encyclopedia of Philosophy*, Summer 2025 ed., E. N. Zalta and U. Nodelman, Eds. Metaphysics Research Lab, Stanford University, 2025.

[30] G. Boolos, *The Logic of Provability*. Cambridge University Press, 1993.

[31] K. Gödel, "Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i," *Monatshefte für Mathematik und Physik*, vol. 38, pp. 173–198, 1931.

[32] E. Acar, "Models of hypercomputation," Master's thesis, Technical University of Vienna, 2012.

[33] "Applied logic: Lecture 23 – unsolvable problems in logic," Lecture notes, CS4860, Cornell University, April 2009, accessed June 13, 2025. [Online]. Available: https://www.cs.cornell.edu/courses/cs4860/2009sp/lec-23.pdf

[34] H. Kwong, "The well-ordering principle," libretexts Mathematics. [Online]. Available: https://math.libretexts.org/Courses/Monroe_Community_College/MTH_220_Discrete_Math/3%3A_Proof_Techniques/3.7%3A_The_Well-Ordering_Principle

[35] P. Koymans and C. Pagano, "Hilbert's tenth problem via additive combinatorics," 2024. [Online]. Available: https://arxiv.org/abs/2412.01768

[36] B. Mazur, K. Rubin, and A. Shlapentokh, "Existential definability and diophantine stability," *Duke Mathematical Journal*, vol. 172, no. 10, pp. 1963–2026, 2023.

[37] J. Denef, "Hilbert's tenth problem for quadratic rings," *Proceedings of the American Mathematical Society*, vol. 48, no. 1, pp. 214–220, 1975. [Online]. Available: https://doi.org/10.2307/2040720

[38] M. Kisin, "Math 129: Number fields," https://web.evanchen.cc/notes/Harvard-129.pdf, 2015, lecture notes taken by Evan Chen, Spring 2015.

[39] K. Conrad, "Factoring in quadratic fields," 2021. [Online]. Available: https://kconrad.math.uconn.edu/blurbs/

[40] L. Alpöge, M. Bhargava, W. Ho, and A. Shnidman, "Rank stability in quadratic extensions and hilbert's tenth problem for the ring of integers of a number field," *arXiv preprint arXiv:2501.18774*, 2025, accessed April 10, 2025. [Online]. Available: https://arxiv.org/abs/2501.18774

[41] J. S. Milne, "Abelian varieties (v2.00)," pp. 166+vi, 2008, available at www.jmilne.org/math/.

[42] J. Top, "Security and coding," pp. 54–76, lecture notes.

[43] T. Ooe and J. Top, "On the mordell-weil rank of an abelian variety over a number field," *Journal of Pure and Applied Algebra*, vol. 58, pp. 261–265, 1989.

[44] J. Top and J. Müller, "Group theory," 2018, lecture notes, Groningen, 2nd year bachelor mathematics.

[45] B. Poonen, "Using elliptic curves of rank one towards the undecidability of hilbert's tenth problem over rings of algebraic integers," *Algorithmic Number Theory*, vol. 5, pp. 33–42, 2002.

[46] G. Cornelissen, T. Pheidas, and K. Zahidi, "Division-ample sets and the diophantine problem for rings of integers," *Journal de Théorie des Nombres de Bordeaux*, vol. 17, pp. 727–735, 2005.

[47] A. Shlapentokh, "Elliptic curves retaining their rank in finite extensions and hilbert's tenth problem for rings of algebraic numbers," *Transactions of the American Mathematical Society*, vol. 360, no. 7, pp. 3541–3555, 2008. [Online]. Available: http://www.jstor.org/stable/20161389

[48] E. Kowalski, "Introduction to additive combinatorics," 2024, lecture notes ETH Zurich. [Online]. Available: https://people.math.ethz.ch/~kowalski/lecture-notes.html

[49] T. Tao and V. H. Vu, *Additive Combinatorics*, ser. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[50] B. Green, "Book review," *Bulletin of the American Mathematical Society (New Series)*, vol. 46, no. 3, pp. 489–497, 2009, article electronically published on January 15, 2009.

[51] P. Koymans, "Peter koymans: Hilbert 10 via additive combinatorics i (ntws 251)," 2025, youtube video. [Online]. Available: https://youtu.be/Cc7TmXeOSpA?si=YtyQDJmFRKmCOHsJ

[52] C. Pagano, "Carlo pagano: Hilbert 10 via additive combinatorics," 2025, youtube video. [Online]. Available: https://youtu.be/LdkLcDU9l_8?si=FwrOnZAajn8gh1Ac