UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
PROGRAMA DE MAGÍSTER EN MATEMÁTICA - ACADÉMICO

Análogos del Décimo Problema de Hilbert

Profesor Guía: Xavier Vidaux Negre
Departamento de Matemática
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Tesis para ser presentada a la Dirección de Postgrado de la Universidad de Concepción

JAVIER ANTONIO UTRERAS ALARCÓN
CONCEPCIÓN-CHILE
2010

Análogos del Décimo Problema de Hilbert
Analogues of Hilbert's Tenth Problem

Javier Utreras Alarcón
Universidad de Concepción

Quiero agradecer muy especialmente a mi profesor guía, X. Vidaux, por todos los consejos que me dio, toda la paciencia que me tuvo, todo el tiempo que me dedicó y todos los libros que me hizo leer. Alguna vez se debe aprender a trabajar duro, y en mi caso fue con él.

Agradezco también a todo el Departamento de Matemática de la Universidad: gracias a ellos, y a todo lo que hicieron por mí, descubrí la Matemática.

Agradezco a T. Pheidas y J. Demeyer, por las muy útiles sugerencias que me dieron al momento de redactar la tesis.

Agradezco a mis amigos. Porque son quienes hacen más interesante y divertida mi vida, y nunca han dejado de estar conmigo.

Agradezco finalmente a mi familia. Por todo, la verdad. Por ser quienes son y hacerme ser quien soy. Y por siempre estar apoyándome.

Contents

Introducción **4**

Introduction **7**

1 Logical background **10**
1.1 Turing Machines and computable functions 10
1.2 Recursive and listable sets 12
1.3 Interpretations and theories 13

2 Hilbert's Tenth Problem **15**
2.1 Matiyasevich's theorem 15
2.2 Decidability of theories 16
2.3 Reducing to Hilbert's Tenth Problem 18

3 Representation by diagonal forms **20**
3.1 Büchi's Problem 21
3.2 Higher-degree diagonal forms 22
3.3 The n k-th powers problem 24

4 A variation on the square relation **27**
4.1 The consecutive right triangles problem 27
4.2 Relation to Büchi's Problem 29

5 Languages that include divisibility **33**
5.1 A general result of Kosovskii for languages with addition and divisibility 33
5.2 Some consequences of Kosovskii's Theorem 36
5.2.1 The language of k-th powers and divisibility 36
5.2.2 The language of an exponential function and divisibility 38
5.3 Weakening the divisibility relation 39

6 Diophantine problem over $\mathbb{Q}$ versus Diophantine homogeneous problem over $\mathbb{Z}$ 42

Bibliography 46

Introducción

El décimo problema en la famosa lista de problemas propuestos por D. Hilbert pide lo siguiente:

> Diseñar un algoritmo que decida si una ecuación polinomial a coeficientes enteros tiene alguna solución entera o no.

(Estas ecuaciones son llamadas *ecuaciones Diofantinas*). Setenta años después de su formulación, en el año 1970, Y. Matiyasevich (basándose en trabajos de M. Davis, J. Robinson y H. Putnam) mostró que no existe ningún algoritmo que realice lo pedido [10].

Como se mostró que no existen algoritmos para determinar la existencia de soluciones enteras a ecuaciones Diofantinas, surgió el problema de determinar la existencia de dichos algoritmos para algunos subconjuntos del conjunto de todas las ecuaciones Diofantinas. Por ejemplo, del resultado de Matiyasevich se desprende que no existe ningún algoritmo para determinar si un sistema de ecuaciones Diofantinas de segundo grado tiene soluciones enteras. Por otro lado, M. Presburger mostró en 1929 que sí existe el algoritmo correspondiente para sistemas de ecuaciones Diofantinas lineales [15].

Consideremos ahora los sistemas de ecuaciones Diofantinas de segundo grado con la siguiente propiedad: ninguna incógnita aparece sin estar elevada al cuadrado. El conjunto de todos estos sistemas es un subconjunto del conjunto de todos los sistemas de ecuaciones Diofantinas de segundo grado, y contiene al conjunto de todas las ecuaciones Diofantinas lineales, ya que toda ecuación Diofantina lineal puede ser escrita de la forma pedida (puesto que todo entero puede ser escrito de la forma $x^2 + y^2 - z^2$, para algunos enteros x, y y z). Debido a estas inclusiones, el problema de determinar la existencia de un algoritmo que decida la existencia de soluciones enteras para estos sistemas está de alguna forma "en medio" de los problemas ya resueltos mencionados en el párrafo anterior. Este problema está abierto, y se conoce como el Problema de representación por formas diagonales cuadráticas.

Para estudiar este problema, sea S el conjunto de todos los cuadrados en $\mathbb{Z}$. El Problema de representación por formas diagonales cuadráticas es equivalente (cf. Proposición 3.3) al problema siguiente:

> Determinar si existe un algoritmo que decida si un sistema formado por ecuaciones Diofantinas lineales y relaciones de la forma $x_i \in S$ tiene alguna solución entera.

Este es el problema central de este trabajo, y así nos referiremos a él en lo que sigue.

Esta tesis está estructurada de la forma siguiente: en el Capítulo 1 se hace un breve repaso de lógica, el necesario para fijar un vocabulario para estudiar los problemas presentados. Los resultados presentados se pueden encontrar en cualquier libro básico de lógica, como [1]. Los lectores que ya conozcan los conceptos de *función computable*, *conjunto recursivo* y *lenguaje de primer orden* pueden omitir este Capítulo.

En el Capítulo 2 no se presentan resultados originales. En cambio, se muestran algunas ideas generales usadas en demostraciones como las que se presentarán más adelante en este trabajo.

En el Capítulo 3 se estudian los métodos que siguió J. R. Büchi para enfrentar el problema central. Su idea fue conjeturar un resultado aritmético, conocido actualmente como el *problema de los n cuadrados de Büchi* (aún abierto; P. Vojta [21] lo resolvió asumiendo la Conjetura de Bombieri). Mostró que si este problema tiene una respuesta positiva entonces el problema central tiene respuesta negativa. Posteriormente, T. Pheidas y X. Vidaux generalizaron las ideas de Büchi a potencias más altas. En este trabajo, daremos una nueva demostración de su resultado.

En el Capítulo 4 se presenta una variante del problema central, donde se incluyen relaciones del tipo $x_i x_j \in S$ (se agradece a J. Demeyer por sugerirla). Se sigue un enfoque similar al de Büchi: formulamos un problema aritmético que, de ser cierto, responde al problema de decisión para esta variante. Luego mostramos la conexión que hay entre nuestro problema aritmético y la conjetura de Büchi.

En el Capítulo 5, a partir de un teorema de Kosovskii para sistemas de ecuaciones Diofantinas lineales y relaciones de divisibilidad, obtenemos el siguiente resultado:

Teorema. *Para todo $k \geq 2$, no existen algoritmos que decidan si existen soluciones enteras a sistemas que consisten en ecuaciones Diofantinas lineales, relaciones de la forma $x|y$, y uno de los siguientes tipos de relación:*

i) "x es una potencia k-ésima", o

ii) $x = k^y$.

Posteriormente obtenemos un resultado general de inexistencia de algoritmos para sistemas de ecuaciones como el del problema central, pero que además incluyen otros tipos de relaciones:

Teorema. *Para todo* $k \geq 1$*, no existen algoritmos que decidan si existen soluciones enteras a sistemas que consisten en ecuaciones Diofantinas lineales, y relaciones de los siguiente tipos:*

i) "x es un cuadrado", y

ii) los pares (x, y) *que satisfacen: existe* t *tal que* $y = tx$ *y, para cada primo* p *que divide a* t*, se cumple* $p^k \leq x$.

Las relaciones de tipo *ii)* son más débiles que la divisibilidad. Además, la intersección de todas ellas (variando k) es la relación de igualdad. En ese sentido, este resultado es una mejora del resultado de Kosovskii.

En el Capítulo 6, generalizamos un resultado conocido que relaciona el Décimo Problema de Hilbert para $\mathbb{Q}$ con un problema de decisión para formas homogéneas en los enteros. Mostramos:

Teorema. *Sea* K *un campo de números formalmente real. El problema de decidir si una ecuación Diofantina en* K *tiene solución es algorítmicamente equivalente al problema de decidir si una forma homogénea en el anillo de enteros de* K *tiene solución no trivial.*

En todo este trabajo consideraremos a 0 como un número natural.

Introduction

The tenth problem in D. Hilbert's famous list asked the following:

> Devise an algorithm to decide whether a polynomial equation with integer coefficients has an integer solution.

(These equations are called *Diophantine equations*.) In the year 1970, 70 years after Hilbert posed it, Y. Matiyasevich (based on work of M. Davis, J. Robinson and H. Putnam) proved that such an algorithm does not exist [10].

Knowing that the decision problem for integer solutions of Diophantine equations had a negative answer, the problem shifted to smaller classes of equations. For example, it follows from Matiyasevich's negative answer that there exists no algorithm to decide whether a system of second-degree Diophantine equations has integral solutions; while, on the other hand, a result of M. Presburger (1929) implies that an analogous algorithm for systems of linear Diophantine equations exists [15].

Consider all systems of second degree Diophantine equations in where every unknown appears squared in all of its ocurrences. These systems form a subset of all systems of second degree Diophantine equations, and it can be shown that every linear Diophantine equation can be written as such (just because any integer can be written as $x^2+y^2-z^2$ for some integers x, y and z). Thus, the decision problem for integer solutions to this kind of systems of equations is "in between" the two already known results mentioned in the previous paragraph. This problem is known as the Problem of representation by diagonal quadratic forms, and is currently open.

To study this last problem, let $S \subset \mathbb{Z}$ be the set of all perfect squares. The Problem of representation by diagonal quadratic forms is now equivalent (cf. Proposition 3.3) to

> Determine if there exists an algorithm to decide whether a system of linear Diophantine equations, together with relations of

the form $x_i \in S$, has a solution in $\mathbb{Z}$.

This is the main problem that inspires most of this work, and will be referred to as such in the following.

This thesis is structured as follows: Chapter 1 presents a brief collection of definitions and results from logic needed to correctly state Hilbert's Tenth Problem and its related problems. The results given there can be found in logic textbooks such as [1]. Readers already acquainted with the concepts of *computable function*, *recursive set* and *first order language* may skip this Chapter.

Chapter 2 does not present any original result; it contains instead the general well-known ideas that we might use in our proofs without mentioning them.

In Chapter 3, J. R. Büchi's approach to the main problem is shown. What he did was to conjecture an arithmetical result, today known as *Büchi's n squares problem* (still open; P. Vojta [21] solved it, assuming Bombieri's Conjecture for surfaces). If this problem had a positive answer, he showed that an undecidability answer to the main problem would follow. Afterwards, T. Pheidas and X. Vidaux generalized Büchi's approach to powers other than squares. We will give a new proof of this *reduction* result.

Chapter 4 presents a small variation on the main problem, including relations of the form $x_i x_j \in S$ to the systems (thanks to J. Demeyer for proposing this problem). To approach this new problem, we do a work similar to Büchi's: we formulate an arithmetical problem that, if positively answered, implies an undecidability result to this *a priori* weaker problem. Afterwards, we show the relation between this new arithmetical problem and Büchi's original conjecture.

In Chapter 5, starting from a theorem by Kosovskii for studying systems that include linear Diophantine equations and divisibility relations, we get the following result :

Theorem. *For any $k \geq 2$, there exists no algorithm to decide whether there exists a solution in the integers to a system that consists of linear Diophantine equations, relations of the form $x|y$, and one of the following kinds of relations :*

i) "x is a k-th power", or

ii) $x = k^y$.

Later in the same Chapter we obtain a general undecidability result for systems of equations like the one in the main problem, but that include some other kinds of relations. We show

Theorem. *For any $k \geq 1$, there exists no algorithm to decide whether there exists a solution in the integers to a system that consists of linear Diophantine equations, and two types of relations:*

i) "x is a square", and

ii) the set of pairs (x, y) satisfying: there exists t such that $y = tx$ and, for every prime p, if p divides t then $p^k \leq x$.

Note that relations of type *ii)* are weaker than divisibility, and that the intersection of all of them (as k varies) is the equality. In that sense, this result is an improvement of Kosovskii's result.

In Chapter 6, we generalize a known result relating the analogues of Hilbert's Tenth Problem for $\mathbb{Q}$ and for homogeneous forms over $\mathbb{Z}$. We prove

Theorem. *Let K be a formally real number field. The decision problem for solutions of Diophantine equations in K is algorithmically equivalent to the decision problem for nonzero solutions of forms in the ring of integers of K.*

Throughout this work, we consider 0 as a natural number.

Chapter 1

Logical background

1.1 Turing Machines and computable functions

In Hilbert's time, the notion of "algorithm" was not formally defined. During the subsequent decades, a set-theoretical construction was developed to formalize it. Intuitively, an algorithm is a machine which, after receiving an input (consisting of natural numbers), follows a finite set of instructions; then it can either a) produce an output (a natural number) after a finite number of steps, or b) never stop computing. We say a function $f : \mathbb{N}^k \supseteq A \to \mathbb{N}$ is *computable* if there exists such a machine that

i) when given $(x_1, \ldots, x_m) \in A$ as input, gives the output $f(x_1, \ldots, x_m)$, and

ii) when given $(x_1, \ldots, x_m) \notin A$ as input, never stops computing.

A natural question arises : is this definition of computable functions equivalent to the intuitive notion of "function computable by an algorithm"? That is what *Church's thesis* states :

Church's thesis. *Every function $f : \mathbb{N}^k \supseteq A \to \mathbb{N}$ whose values can be calculated using an algorithm (in the intuitive sense) is computable.*

As the intuitive idea of algorithm is not formalized, this result cannot be proven. However, in formal mathematics, asking for an algorithm to compute something means asking for a computable function to perform the desired job.

There are several (equivalent) ways of constructing a theoretical machine that fulfills the conditions we want. In the rest of this section, we will detail

the construction of such a machine, the *Turing Machine*.

First of all, let

$$S = \{d, b, |\}.$$

Definition. *A* Turing Machine T *is an ordered 3-uple* $(n, \mathcal{E}, M)$*, where*

- n *is a positive integer called the* number of bands*;*
- $\mathcal{E}$ *is a finite set with two distinct distinguished elements* e_i *and* e_f*, respectively called the* initial state *and the* final state*; and*
- $M : S^n \times \mathcal{E} \to S^n \times \mathcal{E} \times \{-1, 0, 1\}$ *is a function called the* transition map*.*

Definition. *A* configuration $\mathcal{C}$ *of a machine* $T = (n, \mathcal{E}, M)$ *is a triple* (f, m, e)*, where*

- $f : \mathbb{N} \to S^n$ *is a function satisfying* $f(0) = (d, \ldots, d)$*;*
- m *is a nonnegative integer called the* position of the reading head*; and*
- $\mathrm{e} \in \mathcal{E}$*.*

Definition. *Given a function* $f_0 : \mathbb{N} \to S^n$ *satisfying* $f_0(0) = (d, \ldots, d)$*, we can define the* configuration $\mathcal{C}_t$ of the machine T at a time t *recursively as*

$$\mathcal{C}_0 = (f_0, 0, \mathrm{e}_i),$$

$$\mathcal{C}_{t+1} = (f_{t+1}, m_{t+1}, \mathrm{e}_{t+1}),$$

where

$$f_{t+1}(i) = \begin{cases} \pi_1(M(f_t(m_t), \mathrm{e}_t)) & \text{for } i = m_t \\ f_t(i) & \text{otherwise,} \end{cases}$$

$$m_{t+1} = m_t + \pi_3(M(f_t(m_t), \mathrm{e}_t)),$$

$$\mathrm{e}_{t+1} = \pi_2(M(f_t(m_t), \mathrm{e}_t)),$$

where π_1*,* π_2 *and* π_3 *are the projections from* $S^n \times \mathcal{E} \times \{-1, 0, 1\}$*.*

The function f_0 *is called the* input function *for these configurations. If there exists a least* t *such that* $\mathrm{e}_t = \mathrm{e}_f$*, we say that the machine* halts *at time* t *with* output function f_t*. Otherwise, we say that the machine doesn't halt.*

Note that both the halting of the machine an the output function depend on the input function.

After these definitions, we can now use Turing Machines to simulate the behavior of certain functions. First of all, we show how to represent a nonnegative integer using a Turing Machine:

Definition. *Given a machine $T = (n, \mathcal{E}, M)$ in a configuration $\mathcal{C} = (f, m, \mathrm{e})$ and two nonnegative integers i, k with $i \leq n$, we say that the* i-th row of f represents k *if*

$$\pi_i(f(j)) = \begin{cases} d & \text{for } j = 0 \\ | & \text{for } 1 \leq j \leq k \\ b & \text{for } k < j \end{cases}$$

where $\pi_i : S^n \to S$ is the i-th projection.

We formalize the idea of "computable function" given before:

Definition. *Given a Turing Machine $T = (n, \mathcal{E}, M)$ and a function $\phi : \mathbb{N}^k \supseteq A \to \mathbb{N}$, we say that T* computes *ϕ if $n \geq k + 1$, and*

- *for every $(x_1, \ldots, x_k) \in A$, if we consider the function f_0 that represents x_i in its i-th row, for $1 \leq i \leq k$, and represents 0 in every other row as the input function for T, the machine will halt, and the output function will represent $\phi(x_1, \ldots, x_k)$ in its $(k+1)$-th row; and*
- *for every $(x_1, \ldots, x_k) \notin A$, if we consider the function f_0 that represents x_i in its i-th row, for $1 \leq i \leq k$, and represents 0 in every other row as the input function for T, the machine will not halt.*

Definition. *A function $f : A \subseteq \mathbb{N}^k \to \mathbb{N}$ is said to be* computable *if there exists some Turing Machine T that computes it.*

1.2 Recursive and listable sets

Related to the notion of computability, we define two kinds of subsets of $\mathbb{N}$:

Definition. *A set $A \subseteq \mathbb{N}$ is* recursive *if its characteristic function is computable.*

Definition. *A set $A \subseteq \mathbb{N}$ is* listable *if it is empty or if there exists a surjective computable function $f : \mathbb{N} \to A$.*

Recursive sets are precisely the subsets of $\mathbb{N}$ for which the following decision problem has a positive answer :

> Does there exist an algorithm to decide whether a given $x \in \mathbb{N}$ belongs to A?

The relation between these two kinds of sets is given by the next theorem :

Theorem 1.1. *All recursive sets are listable. However, there exist listable sets which are not recursive.*

1.3 Interpretations and theories

Definition. *A* first order language *is a set of symbols, each of which is labeled as exactly one of the following :*

- *a constant symbol,*
- *an n-place relation symbol, for one $n \geq 1$, or*
- *an n-place function symbol, for one $n \geq 1$.*

Definition. *If $\mathcal{L}$ is a first order language, an* $\mathcal{L}$-formula *is a well-formed sentence made up of*

- *the equality symbol $=$,*
- *variables x_i, with $i \in \mathbb{N}$,*
- *logical connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ and $\leftrightarrow$,*
- *quantifiers $\forall$ and $\exists$,*
- *the constant symbols of $\mathcal{L}$,*
- *for every $k \geq 1$, the k-place relation symbols of $\mathcal{L}$ as if they were k-ary relations over the set of variables and constant symbols, and*
- *for every $k \geq 1$, the k-place function symbols of $\mathcal{L}$ as if they were functions from the set of variables and constant symbols (to the k-th power) to the set of variables and constant symbols.*

An $\mathcal{L}$-formula is an $\mathcal{L}$-sentence *if all variables appear under the scope of a quantifier.*

An $\mathcal{L}$-formula is positive existential *if the only quantifiers and logical connectives that appear in it are $\exists$, $\wedge$ and $\vee$, and all quantifiers $\exists$ appear at the beginning of the formula (before any connective appears).*

We are only using relation and function symbols *as if they were* relations and functions. They become actual relations and functions through an *interpretation*:

Definition. *Given a set A, an* interpretation $\mathcal{I}$ *of a first order language $\mathcal{L}$ is a rule that assigns to each constant symbol of $\mathcal{L}$ an element of A; to each n-place relation symbol of $\mathcal{L}$ a n-ary relation over A; and to each n-place function symbol of $\mathcal{L}$ a function $f : A^n \to A$.*

Through an interpretation $\mathcal{I}$ we give meaning, inside a set A, to $\mathcal{L}$-sentences. When interpreted, a sentence F may state either a true or a false fact about A. If it states a true fact, we say that A *models* (or *satisfies*) F through $\mathcal{I}$, and we write

$$A_{\mathcal{I}} \models F.$$

Definition. *Given a language $\mathcal{L}$, a set A and an interpretation $\mathcal{I}$ of $\mathcal{L}$ over A, the* theory *of A in the language is the set of all $\mathcal{L}$-sentences F in the language such that*

$$A_{\mathcal{I}} \models F.$$

Definition. *Given a language $\mathcal{L}$, a set A and an interpretation $\mathcal{I}$ of $\mathcal{L}$ over A, the* positive existential theory *of A in the language is the set of all positive existential $\mathcal{L}$-sentences F in the language such that*

$$A_{\mathcal{I}} \models F.$$

Throughout this work, all first order languages will be interpreted over $\mathbb{N}$ or over $\mathbb{Z}$, and all interpretations of symbols used in arithmetic will be in accord with their original meanings. This means that, for example, the constant symbol 0 in a language will be interpreted in $\mathbb{N}$ and in $\mathbb{Z}$ as the number 0, and the same with usual functions and relations like $+$ (the addition function) or $|$ (the divisibility relation).

Chapter 2

Hilbert's Tenth Problem

2.1 Matiyasevich's theorem

Definition. *A set $A \subseteq \mathbb{N}$ is called a* Diophantine set *if there exists a polynomial $F(x_0, \ldots, x_n)$ with integer coefficients such that*

$$A = \{x \in \mathbb{N} : \text{ there exists } (z_1, \ldots, z_n) \in \mathbb{N}^n \text{ such that } F(x, z_1, \ldots, z_n) = 0\}.$$

The study of these sets is connected to the answer to Hilbert's Tenth Problem. In fact, the result proven by Matiyasevich in 1970 [10] is the following:

Theorem 2.1 (Matiyasevich)**.** *Listable sets are Diophantine.*

From this result follows the impossibility answer to Hilbert's Tenth Problem:

Theorem 2.2. *There exists no algorithm to decide whether a Diophantine equation has solutions in $\mathbb{N}$.*

Proof. Suppose such an algorithm exists. Let A be a listable nonrecursive set. By Matiyasevich's Theorem, there exists a polynomial F such that, for each $x \in \mathbb{N}$, x belongs to A if and only if the Diophantine equation

$$F(x, z_1, \ldots, z_n) = 0$$

has solutions in $\mathbb{N}$. Using the mentioned algorithm we would be able to decide, given $x \in \mathbb{N}$, whether it belongs to A or not. But A is nonrecursive. □

Corollary 2.3. *There exists no algorithm to decide whether a Diophantine equation has a solution in $\mathbb{Z}$.*

Proof. Suppose that such an algorithm exists. Given a Diophantine equation

$$F(x_1, \ldots, x_n) = 0,$$

we would be able to decide whether

$$F(x_{1_1}^2 + x_{1_2}^2 + x_{1_3}^2 + x_{1_4}^2, \ldots, x_{n_1}^2 + x_{n_2}^2 + x_{n_3}^2 + x_{n_4}^2) = 0$$

has integer solutions, but that would decide whether the original equation had solutions in $\mathbb{N}$ (by Lagrange's four squares Theorem). □

By using the method of this last proof, many of the results that will be obtained in this work for solutions in $\mathbb{N}$ can be generalized to $\mathbb{Z}$.

2.2 Decidability of theories

Consider the first order language

$$\mathcal{L} = \{0, 1, +, \cdot\},$$

where each symbol is interpreted in $\mathbb{Z}$ as usual ($\mathcal{L}$ is called the "language of rings"). Given a Diophantine equation $P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)$, with both P and Q polynomial with positive coefficients, we can construct a positive existential $\mathcal{L}$-sentence

$$F : \exists x_1 \ldots \exists x_n (P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)),$$

as every monomial with positive coefficient can be expressed using the symbols $\cdot$ and 1. Moreover, this Diophantine equation has integer solutions if and only if $\mathbb{Z}$ models F. On the other hand, every positive existential $\mathcal{L}$-sentence is interpreted in $\mathbb{Z}$ as the assertion of existence of integer solutions to a disjunction of systems of Diophantine equations. For any Diophantine equations $F = 0$ and $G = 0$ we have

$$(F = 0 \text{ and } G = 0) \text{ if and only if } F^2 + G^2 = 0,$$

$$(F = 0 \text{ or } G = 0) \text{ if and only if } FG = 0.$$

This disjunction of systems of Diophantine equations has a solution over the integers if and only if a particular Diophantine equation (built by iterating

the methods shown above, to collapse the system to a single equation) has a solution.

From the previous paragraph it follows that Hilbert's Tenth Problem is equivalent to

Problem 2.4. *Devise an algorithm to decide whether a given positive existential $\mathcal{L}$-sentence belongs to the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}$.*

And its impossibility answer becomes

Theorem 2.5. *The positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}$ is undecidable, i.e., there is no algorithm to decide whether a positive existential $\mathcal{L}$-sentence belongs to it.*

To study the decidability problem for smaller classes of equations, the language must be modified. We next state a few important results in this direction.

Theorem 2.6 (Presburger, [15])**.** *The positive existential theory of $\mathbb{N}$ in the language*

$$\{0, 1, +\}$$

is decidable.

This is one of the first results obtained in this direction. Translated to equations, it states that there exists an algorithm to decide whether a system of linear Diophantine equations has a solution in $\mathbb{N}$.

Theorem 2.7 (Lipshitz, [9])**.** *The positive existential theory of $\mathbb{N}$ in the language*

$$\{0, 1, +, |\}$$

is decidable.

This theorem, from 1978, shows that divisibility is *less expressive* than multiplication, in the following sense: we can define divisibility using multiplication, but not conversely (see Proposition 2.10 below).

Theorem 2.8 (Terrier, [19])**.** *The positive existential theory of $\mathbb{N}$ in the language*

$$\{c_i : i \in \mathbb{N}\} \cup \{f_k : k \in \mathbb{N}\} \cup \{<, >, |, \nmid\}$$

(where each c_i is interpreted as the number i, each f_k is interpreted as the function $n \mapsto n^k$, and $\nmid$ as the relation "does not divide") is decidable.

Theorem 2.9 (Semenov, [16]). *The positive existential theory of* $\mathbb{N}$ *in the language*

$$\{0, 1, +, E_2\}$$

(where E_2 *is interpreted as the function* $n \mapsto 2^n$*) is decidable.*

2.3 Reducing to Hilbert's Tenth Problem

In order to prove the undecidability of the positive existential theory of $\mathbb{N}$ or $\mathbb{Z}$ in some of the languages to be studied in this thesis, the next proposition will be useful. It reduces some decision problems to Hilbert's Tenth Problem, where we can use Theorem 2.2, Corollary 2.3 or Theorem 2.5.

Proposition 2.10. *Let* $\mathcal{L}$ *be a first order language that contains the symbols* 0, 1 *and* $+$*, and suppose these symbols are interpreted in* $\mathbb{Z}$ *as usual. If there exists a positive-existential* $\mathcal{L}$*-formula* $\phi(x, y, z)$ *such that*

$$z = xy \text{ if and only if } \mathbb{Z} \models \phi(x, y, z)$$

then the positive existential theory of $\mathbb{Z}$ *in the language* $\mathcal{L}$ *is undecidable.*

Proof. Suppose that this theory is decidable, and let $\mathcal{L}_R = \{0, 1, +, \cdot\}$ be the first-order language of rings. Given a positive existential $\mathcal{L}_R$-sentence F, we can obtain a positive existential $\mathcal{L}$-sentence F' by replacing an appearance of something of the form $x \cdot y$ by a new variable z, and inserting $\exists z \phi(x, y, z) \wedge$ into the sentence, right after the beginning of the sentence where all quantifiers $\exists$ appear, and iterating this procedure. We will then have

$$\mathbb{Z} \models F \text{ if and only if } \mathbb{Z} \models F'$$

so we would have an algorithm to decide whether F belongs to the theory of $\mathbb{Z}$, contradicting Corollary 2.3. □

Actually, the formulas we will want to construct do not need to define multiplication; squaring is enough, as this proposition shows:

Proposition 2.11. *Let* $\mathcal{L}$ *be a first order language that contains the symbols* 0, 1 *and* $+$*, and suppose these symbols are interpreted in* $\mathbb{Z}$ *as usual. If there exists a positive-existential* $\mathcal{L}$*-formula* $R(x, y)$ *such that*

$$y = x^2 \text{ if and only if } \mathbb{Z} \models R(x, y)$$

then the positive existential theory of $\mathbb{Z}$ *in the language* $\mathcal{L}$ *is undecidable.*

Proof. Let $\phi(x, y, z)$ be the $\mathcal{L}$-formula

$$\phi(x, y, z) : \exists q \exists w \exists s R(x, q) \wedge R(y, w) \wedge R(x + y, s) \wedge z + z = s - q - w.$$

This formula is satisfied by $\mathbb{Z}$ if and only if $2z = (x + y)^2 - x^2 - y^2$, so we have

$$z = xy \text{ if and only if } \mathbb{Z} \models \phi(x, y, z).$$

The conclusion follows from the previous proposition. □

Note that in these last two results we can replace $\mathbb{Z}$ with $\mathbb{N}$, and they still hold true (with similar proofs).

Chapter 3

Representation by diagonal forms

The problem presented in the Introduction as the main problem can be stated in the following ways :

Problem 3.1 (Representation by diagonal quadratic forms)**.** *Does there exist an algorithm to decide the existence of integer solutions to a system of equations of the form*

$$\sum_{j=1}^{n} a_{i,j} x_j^2 = b_i, \quad i = 1, \ldots, m \tag{3.1}$$

for any m, n positive integers, where the $a_{i,j}$ and the b_i are integers for $1 \leq i \leq m$, $1 \leq j \leq n$?

Problem 3.2. *Is the positive existential theory of $\mathbb{Z}$ in the language*

$$\mathcal{L}^2 = \{0, 1, +, P_2\},$$

with P_2 interpreted in $\mathbb{Z}$ as the predicate "is a square", decidable?

These problems are indeed equivalent :

Proposition 3.3. *Problems 3.1 and 3.2 are equivalent.*

Proof. Suppose the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}^2$ is decidable. Given a system of equations like the one in (3.1), we construct the positive existential $\mathcal{L}^2$-formula

$$F : \exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x_j = b_i \wedge \bigwedge_{j=1}^{n} P_2(x_j).$$

This formula F is satisfied in $\mathbb{Z}$ if and only if the original system of equations has an integer solution: as we can decide whether the formula F belongs to the theory of $\mathbb{Z}$ or not, we have a positive answer to Problem 3.1.

On the other hand, suppose we can decide the existence of integer solutions for systems like the one in (3.1). If F is a positive existential $\mathcal{L}^2$-formula, it can be interpreted in $\mathbb{Z}$ as a disjunction of systems of the form

$$\sum_{j=1}^{n} a_{i,j}x_j^2 + \sum_{k=1}^{r} b_{i,k}y_k = c_i, \quad i = 1, \ldots, m \tag{3.2}$$

with the $n + r$ unknowns x_j and y_k. Since every integer N can be written as $N = A^2 + B^2 - C^2$ for some integers A, B and C, the formula F belongs to the theory of $\mathbb{Z}$ if and only if a disjunction of systems of the form

$$\sum_{j=1}^{n} a_{i,j}x_j^2 + \sum_{k=1}^{r} b_{i,k}(z_k^2 + w_k^2 - q_k^2) = c_i, \quad i = 1, \ldots, m$$

with unknowns x_i, z_k, w_k and q_k has an integer solution. Since by hypothesis we can decide the latter, Problem 3.2 has a positive answer. □

3.1 Büchi's Problem

Trying to find an answer to Problem 3.1, J. R. Büchi posed an arithmetical problem (still open) [8]. In order to state it, we first give some definitions:

Definition. *A sequence $(x_i)_{i=0}^m$ of integers is a* Büchi sequence *if*

$$x_{i+2}^2 - 2x_{i+1}^2 + x_i^2 = 2, \quad i = 0, \ldots, m-2.$$

Definition. *A Büchi sequence $(x_i)_{i=0}^m$ is called* trivial *if $(x_i^2)_{i=0}^m$ is a sequence of consecutive squares.*

It is not difficult to verify that any sequence of consecutive integers is a trivial Büchi sequence. However, there exist non-trivial sequences, like (6,23,32,39). Büchi's Problem asks whether these "non-trivial" sequences have a common length bound:

Problem 3.4 (Büchi)**.** *Does there exist a positive integer M such that, if $(x_i)_{i=0}^{M-1}$ is a Büchi sequence, then it is trivial?*

Büchi proved that from a positive answer to Problem 3.4 a negative answer to Problem 3.2 would follow:

Theorem 3.5 (Büchi, [13])**.** *If Büchi's Problem 3.4 has a positive answer, then the Problem of representation by diagonal quadratic forms is undecidable.*

Proof. Suppose M is a positive integer such that Büchi's Problem has a positive answer. Consider the positive existential $\mathcal{L}^2$-formula

$$F(x,y) : \exists y_0 \dots \exists y_{M-1}$$
$$y = y_0 \wedge \bigwedge_{i=0}^{M-1} P_2(y_i) \wedge \bigwedge_{i=0}^{M-3} y_{i+2} - 2y_{i+1} + y_i = 2 \wedge y_0 + 2x + 1 = y_1.$$

As the sequence $(y_i)_{i=0}^{M-1}$ is of consecutive squares (due to the positive answer to Büchi's Problem), it is easy to see that $\mathbb{Z}$ satisfies $F(x,y)$ if and only if $y = x^2$. The conclusion follows from Propositions 2.11 and 3.3. □

3.2 Higher-degree diagonal forms

With the same motivation that led us to Problem 3.1, obtaining an undecidability result for integer solutions for a class of equations smaller than all Diophantine equations, Pheidas and Vidaux asked the following question for every integer $k \geq 3$:

Problem 3.6 (Representation by diagonal forms of degree k)**.** *Does there exist an algorithm to decide the existence of an integer solution to a system of equations of the form*

$$\sum_{j=1}^{n} a_{i,j} x_j^k = b_i, \quad i = 1, \dots, m \tag{3.3}$$

(with unknowns x_j) for any m, n positive integers, where the $a_{i,j}$ and the b_i are integers for $1 \leq i \leq m$, $1 \leq j \leq n$?

To establish the corresponding logical problem, for each k we will consider the first-order language

$$\mathcal{L}^k = \{0, 1, +, P_k\}$$

where P_k shall be interpreted in $\mathbb{Z}$ as the predicate "is a k-th power". For each k, we can now ask

Problem 3.7. *Is the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}^k$ decidable?*

We would like to prove these problems to be equivalent. For doing so, we will need the following theorem of Hilbert [4]:

Theorem 3.8 (Hilbert-Waring Theorem)**.** *For each positive integer k, there exists a smallest natural number $g(k)$ (known as* Waring's number for k*) such that every nonnegative integer can be expressed as a sum of exactly $g(k)$ k-th powers of nonnegative integers.*

We can now state the desired equivalence.

Proposition 3.9. *For any given integer $k \geq 3$, Problems 3.6 and 3.7 are equivalent.*

Proof. If the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}^k$ is decidable, given a system of equations like the one in (3.3) we can construct the $\mathcal{L}^k$-formula

$$F : \exists x_1 \dots \exists x_n \bigwedge_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x_j = b_i \wedge \bigwedge_{j=1}^{n} P_k(x_j).$$

This formula is satisfied in $\mathbb{Z}$ if and only if System (3.3) has a solution. We obtain a positive answer to Problem 3.6.

Conversely, a positive existential $\mathcal{L}^k$-formula F is satisfied in $\mathbb{Z}$ if and only if some disjunction of systems of equations of the form

$$\sum_{j=1}^{n} a_{i,j} x_j^k + \sum_{l=1}^{r} b_{i,l} y_l = c_i, \quad i = 1, \dots, m \tag{3.4}$$

with unknowns x_j, y_l has an integral solution. Let $g(k)$ be Waring's number for k. If k is odd, System (3.4) is equivalent to a system of equations of the form

$$\sum_{j=1}^{n} a_{i,j} x_j^k + \sum_{l=1}^{r} \left(b_{i,l} \left(\sum_{s=1}^{g(k)} y_{l_s}^k \right) \right) = c_i, \quad i = 1, \dots, m.$$

On the other hand, if k is even, System (3.4) is equivalent to the disjunction of the 2^r systems of the form

$$\sum_{j=1}^{n} a_{i,j} x_j^k + \sum_{l=1}^{r} \left(b_{i,l} \left(\pm \sum_{s=1}^{g(k)} y_{l_s}^k \right) \right) = c_i, \quad i = 1, \dots, m.$$

In either case, if the Problem of representation by diagonal forms of degree k is decidable, Problem 3.7 will also be. □

3.3 The n k-th powers problem

Definition. *Let $x = (x_i)_{i=1,\dots n}$ a sequence of integers. The* difference sequence *of x, denoted $\Delta(x) = (\Delta(x)_i)_{i=1,\dots,n-1}$, is defined by*

$$\Delta(x)_i = x_{i+1} - x_i$$

More generally, the k-th difference sequence *of x, $\Delta^k(x) = (\Delta^k(x)_i)_{i=1}^{n-k}$, is defined recursively by*

$$\Delta^1(x) = \Delta(x) \quad \textit{and} \quad \Delta^{k+1}(x) = \Delta(\Delta^k(x)).$$

Following Büchi's idea (see Theorem 3.5), Pheidas and Vidaux proposed the following generalizations :

Definition. *Let $k \geq 2$ be an integer. A sequence $(x_i)_{i=0}^m$ of integers (with $m \geq k$) is a* Büchi k-th powers sequence *if*

$$\Delta^k(x_i) = (k!)_{i=0}^{m-k}$$

where $(k!)$ is the constant sequence with every term equal to $k!$.

Definition. *A Büchi k-th powers sequence $(x_i)_{i=0}^m$ is called* trivial *if $(x_i^k)_{i=0}^m$ is a sequence of consecutive k-th powers.*

Problem 3.10 (n k-th powers problem)**.** *Let $k \geq 2$ be an integer. Does there exist a positive integer M such that, if $(x_i)_{i=0}^{M-1}$ is a Büchi k-th powers sequence, then it is trivial?*

Note that, for $k = 2$, this problem is Büchi's Problem. Moreover, Problem 3.10 is an analogue of Problem 3.4 in the sense that the following generalization of Theorem 3.5 holds :

Theorem 3.11 (Pheidas, Vidaux)**.** *For any given integer $k \geq 3$, if Problem 3.10 has a positive answer then the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}^k$ is undecidable.*

Pheidas and Vidaux proved this theorem for odd k in [13]. They finished it later in [14]. Refer to [11] for their complete proof.

In this work we give an alternative proof of Theorem 3.11. We will need the following lemma :

Lemma 3.12. *Given an integer x, the only solution to the system of linear equations (in the variables $x_1, \ldots, x_{k-1}$)*

$$(x+i)^k - x^k = i^k + \sum_{j=1}^{k-1} \binom{k}{j} x_{k-j} i^j, \quad i = 1, \ldots, k-1$$

is $x_j = x^j$ for each j.

Proof. Replacing each x_j for x^j, we get the equations

$$(x+i)^k - x^k = i^k + \sum_{j=1}^{k-1} \binom{k}{j} x^{k-j} i^j, \quad i = 1, \ldots, k-1$$

all of which are identified as the binomial formula. To prove uniqueness, we notice that the coefficient matrix of the system,

$$\begin{bmatrix} \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \cdots & \binom{k}{k-1} \\ \binom{k}{1}2 & \binom{k}{2}2^2 & \binom{k}{3}2^3 & \cdots & \binom{k}{k-1}2^{k-1} \\ \binom{k}{1}3 & \binom{k}{2}3^2 & \binom{k}{3}3^3 & \cdots & \binom{k}{k-1}3^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{k}{1}(k-1) & \binom{k}{2}(k-1)^2 & \binom{k}{3}(k-1)^3 & \cdots & \binom{k}{k-1}(k-1)^{k-1} \end{bmatrix},$$

can be written as a product VD, where V is a Vandermonde matrix

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 2 & 2^2 & 2^3 & \cdots & 2^{k-1} \\ 3 & 3^2 & 3^3 & \cdots & 3^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k-1 & (k-1)^2 & (k-1)^3 & \cdots & (k-1)^{k-1} \end{bmatrix}$$

and $D = \{d_{ij}\}$ is the diagonal $(k-1) \times (k-1)$-matrix given by $d_{ii} = \binom{k}{i}$. Both V and D are nonsingular, thus the solution shown is unique. □

Proof of Theorem 3.11. Fix $k \geq 3$. Suppose M is such that the n k-th powers problem has a positive answer, and consider the following $\mathcal{L}^k$-formulas ($\Delta^k(x)$ is the k-th difference sequence of the sequence $x = (x_1, \ldots, x_M)$):

$$S(x_1, \ldots, x_M) : \bigwedge_{i=1}^{M} P_k(x_i) \wedge \Delta^k(x) = (k!),$$

$$P(x_1,\dots,x_k) : \exists y_2 \dots \exists y_M S(x_k, y_2, \dots, y_M) \wedge \bigwedge_{i=1}^{k-1} \left(y_i - x_k = i^k + \sum_{j=1}^{k-1} \binom{k}{j} x_{k-j} i^j \right),$$

$$R(x,y) : \exists x_3 \dots \exists x_k P(x, y, x_3, \dots, x_k).$$

First note that, by the positive answer to Problem 3.10, $\mathbb{Z}$ satisfies $S(x_1,\dots,x_M)$ if and only if $(x_1,\dots,x_M)$ is a sequence of consecutive k-th powers.

For any integer x,

$$\mathbb{Z} \models S(x^k, (x+1)^k, \dots, (x+M-1)^k),$$

then, by the binomial formula,

$$\mathbb{Z} \models P(x, x^2, \dots, x^k).$$

We obtain that, for any integer x, $\mathbb{Z}$ satisfies $F(x, x^2)$.

Conversely, suppose that $\mathbb{Z}$ satisfies $P(x_1,\dots,x_k)$. There exists an integer u such that

$$x_k = u^k, \quad \text{and} \quad y_i = (u+i-1)^k, \text{ for } i = 1, \dots k-1$$

(For k odd, the sequence $(x_k, y_2, \dots, y_M)$ is increasing; for k even only one of the k-th roots of x_k satisfies $y_2 = (u+1)^k$, that is the desired u). By the previous lemma, we must have $x_i = u^i$ for all i. This shows that if $\mathbb{Z}$ satisfies $R(x,y)$, then there exists an integer u such that $x = u$ and $y = u^2$.

We have constructed an $\mathcal{L}^k$-formula $R(x,y)$ that is satisfied in $\mathbb{Z}$ if and only if $y = x^2$. By Proposition 2.11 we conclude the desired undecidability. □

Chapter 4

A variation on the square relation

Consider the first order language

$$\mathcal{L}' = \{0, 1, +, S\}$$

where S is interpreted as the binary relation

$$S(x, y) \text{ if and only if } xy \text{ is a square.}$$

As

$$x \text{ is a square if and only if } \mathbb{Z} \models S(x, 1),$$

if the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}'$ is decidable, then Problem 3.1 of representation by diagonal quadratic forms is decidable. So proving the undecidability of the positive existential theory of $\mathbb{Z}$ in this new language would be an approach to the main problem.

4.1 The consecutive right triangles problem

Definition. *A pair (x, k) of integers is said to be an* admissible pair *if the following are satisfied:*

i) x *is odd,*

ii) $2k - 1$ *is a perfect square, and*

iii) $k^2 - x^2$ *is a perfect square.*

A pair (x, k) of integers is said to be a good pair *if*

$$k = \frac{x^2 + 1}{2}.$$

Note that, a pair (x, k) satisfies item *iii)* of the definition if and only if there exists a right-angled triangle with integer sides such that $|x|$ is the length of one of the short sides and k is the length of the hypotenuse. As for all integers x we have

$$x^2 + \left(\frac{x^2 - 1}{2}\right)^2 = \left(\frac{x^2 + 1}{2}\right)^2,$$

(x, k) is a good pair if and only if $(|x|, k - 1, k)$ is a Pythagorean triple.

From this, two remarks follow. First, for every odd x there exists exactly one good pair having x as its first component. Secondly, as

$$2\left(\frac{x^2 + 1}{2}\right) - 1$$

is a square for any integer x, all good pairs are admissible. However, not all admissible pairs are good: consider, for example, $(15, 25)$.

Definition. *Given a pair (x, k) of integers, its* succesor pair *is the pair $(x + 2, k + 2x + 2)$. A sequence $P_0, \ldots, P_n$ of pairs is said to be* consecutive *if P_i is succesor to P_{i-1} for $1 \leq i \leq n$.*

Lemma 4.1. *Let $P_0, \ldots, P_n$ be a consecutive sequence of pairs. If any of the pairs is good, then all of them are.*

Proof. Suppose $P_i = (x_i, k_i)$, with $0 \leq i \leq n$, is a good pair. Then

$$k_{i-1} = k_i - 2x_{i-1} - 2 = \frac{(x_{i-1} + 2)^2 + 1}{2} - 2x_{i-1} - 2 = \frac{x_{i-1}^2 + 1}{2}$$

and

$$k_{i+1} = k_i + 2x_i + 2 = \frac{x_i^2 + 1}{2} + 2x_i + 2 = \frac{(x_i + 2)^2 + 1}{2} = \frac{x_{i+1}^2 + 1}{2}$$

so $P_{i-1} = (x_{i-1}, k_{i-1})$ and $P_{i+1} = (x_{i+1}, k_{i+1})$ are good pairs too. □

Consider the following problem :

Problem 4.2. *Is there a natural number M such that any consecutive sequence of pairs $(P_i)_{i=0,\dots,M-1}$ in where each P_i is admissible is necessarily made up of good pairs?*

This problem is analogous to Büchi's Problem 3.4, in the sense that a positive answer to it allows us to conclude undecidability:

Theorem 4.3. *Suppose Problem 4.2 has a positive answer. Then the positive existential theory of $\mathbb{Z}$ in the language $\mathcal{L}'$ is undecidable.*

Proof. Suppose that Problem 4.2 has a positive answer for some $M \in \mathbb{N}$. Consider the following $\mathcal{L}'$-formula:

$$A(x,k)\colon \exists y(x = 2y+1) \wedge S(2k-1,1) \wedge S(k+x,k-x).$$

Given a pair (x,k), $\mathbb{Z}$ satisfies $A(x,k)$ if and only if (x,k) is admissible.

Consider

$$G(x,k)\colon \exists x_0 \dots \exists x_{M-1} \exists k_0 \dots \exists k_{M-1} \bigwedge_{i=0}^{M-1} A(x_i,k_i) \wedge x = x_0 \wedge k = k_0$$
$$\wedge \bigwedge_{i=1}^{M-1} x_i = x_{i-1} + 2 \wedge \bigwedge_{i=1}^{M-1} k_i = k_{i-1} + 2x_{i-1} + 2.$$

Note that $\mathbb{Z}$ satisfies $G(x,y)$ if and only if (x,y) is the first pair of a consecutive sequence of M admissible pairs. As we are supposing M satisfies Problem 4.2, $\mathbb{Z}$ models $G(x,k)$ if and only if (x,k) is a good pair.

Consider the formula

$$Q(x,y)\colon \exists k\Big((G(x,k) \wedge y = 2k-1) \vee (G(x+1,k) \wedge y = 2k - 2x - 2)\Big).$$

Note that, if (x,k) is a good pair, then $x^2 = 2k-1$. Similarly, if $(x+1,k)$ is a good pair, then $x^2 = 2k - 2x - 2$. Also note that, for any integer x, it is impossible for x and $x+1$ to be first elements of good pairs, as one of them must be even. Then, by definition of a good pair, $\mathbb{Z}$ models $Q(x,y)$ if and only if $y = x^2$. □

4.2 Relation to Büchi's Problem

The problem we have formulated relates to Büchi's Problem:

Proposition 4.4. *Suppose Büchi's Problem 3.4 has got a negative answer. Then Problem 4.2 has also got a negative answer.*

We will need the following lemmas:

Lemma 4.5. *Two consecutive elements of a Büchi sequence cannot be of the same parity.*

Proof. Let $(x_i)_{i=0}^m$ be a Büchi sequence. For any $i \in \{0, \ldots, m-2\}$ we have

$$x_{i+2}^2 - 2x_{i+1}^2 + x_i^2 = 2. \tag{4.1}$$

Modulo 2, this equation states that x_{i+2} and x_i are of the same parity. Thus, modulo 4 Equation (4.1) becomes

$$2 = x_{i+2}^2 - 2x_{i+1}^2 + x_i^2 = x_i^2 - 2x_{i+1}^2 + x_i^2 = 2(x_i^2 - x_{i+1}^2)$$

(as the only squares modulo 4 are 1 and 0). This means that x_i and x_{i+1} have different parity, and so do x_{i+1} and x_{i+2}. □

Lemma 4.6. *Let $(x_i)_{i=0}^m$ be a Büchi sequence. If x_0^2 and x_1^2 are consecutive squares, the sequence is trivial.*

Proof. Let x be such that $x_0^2 = x^2$ and $x_1^2 = (x+1)^2$. We will show that

$$x_n = (x+n)^2 \tag{4.2}$$

for all $\in \{2, \ldots, m\}$ by induction on n.

For $n = 2$ we have

$$x_2^2 = 2 + 2x_1^2 - x_0^2 = 2 + 2(x+1)^2 - x^2 = x^2 + 4x + 4 = (x+2)^2$$

(using Equation (4.1)). Suppose that Equation (4.2) holds for $n \leq k$. Then

$$x_{k+2}^2 = 2 + 2x_{k+1}^2 - x_k^2 = 2 + 2(x+k+1)^2 - (x+k)^2 = (x+k+2)^2$$

(using Equation (4.1)). □

Proof of Proposition 4.4. Let M be a natural number. We will show how to construct a consecutive sequence of admissible pairs of length M with no good pairs in it. Let $a_0, \ldots, a_{2M}$ be a sequence of non-consecutive squares such that a_0 is even (no Büchi sequence has only odd terms, due to Lemma 4.5) and

$$a_{i+2} - 2a_{i+1} + a_i = 2, \quad i = 0, \ldots, 2M-2. \tag{4.3}$$

We define, for $i = 0, \ldots, M-1$,

$$\begin{aligned} x_i &= \frac{a_{2i+2} - a_{2i+1} - 1}{2} \\ k_i &= \frac{a_{2i+1} + 1}{2}. \end{aligned}$$

We claim that each pair (x_i, k_i) is admissible, and that the sequence

$$\Big((x_i, k_i)\Big)_i$$

is a sequence of consecutive pairs. Indeed, by Lemma 4.5, for any i, a_{2i+1} is an odd square (congruent to 1 modulo 4) and a_{2i+2} is an even square (congruent to 0 modulo 4), so x_i will be odd; $2k_i - 1 = a_{2i+1}$ is a square, and

$$k_i^2 - x_i^2 = (k_i + x_i)(k_i - x_i) = \frac{(a_{2i+2})(2a_{2i+1} - a_{2i+2} + 2)}{4} = \frac{(a_{2i+2})(a_{2i})}{4}$$

by Equation (4.3). Hence $k_i^2 - x_i^2$ a square. Moreover, for $i = 0, \ldots, M-2$ we have (using Equation (4.3) several times)

$$\begin{aligned} x_{i+1} &= \frac{a_{2i+4} - a_{2i+3} - 1}{2} \\ &= \frac{(2 + 2a_{2i+3} - a_{2i+2}) - a_{2i+3} - 1}{2} \\ &= \frac{2 + a_{2i+3} - a_{2i+2} - 1}{2} \\ &= \frac{2 + (2 + 2a_{2i+2} - a_{2i+1}) - a_{2i+2} - 1}{2} \\ &= \frac{4 + a_{2i+2} - a_{2i+1} - 1}{2} \\ &= x_i + 2 \end{aligned}$$

$$\begin{aligned} k_{i+1} &= \frac{a_{2i+3} + 1}{2} \\ &= \frac{(2 + 2a_{2i+2} - a_{2i+1}) + 1}{2} \\ &= \frac{(a_{2i+1} + 1) + 2(a_{2i+2} - a_{2i+1} - 1) + 4}{2} \\ &= k_i + 2x_i + 2. \end{aligned}$$

It only remains to prove that the sequence

$$\Big((x_i, k_i)\Big)_i$$

does not contain any good pair. For this we note that, if (x_0, k_0) were to be a good pair, then

$$\frac{x_0^2+1}{2} = k_0 = \frac{a_1+1}{2},$$

hence $a_1 = x_0^2$. Similarly, as (x_1, k_1) would also be a good pair (by Lemma 4.1),

$$\frac{x_1^2+1}{2} = k_1 = \frac{a_3+1}{2},$$

thus $a_3 = x_1^2$. But $x_1 = x_0 + 2$, and by Equation (4.3) we obtain

$$a_2 = \frac{a_3 + a_1 - 2}{2} = \frac{(x_0+2)^2 + x_0^2 - 2}{2} = (x_0+1)^2.$$

By Lemma 4.6, the sequence $(a_i)_{i=0}^{2M}$ would be a sequence of consecutive squares, contradicting the hypothesis. □

Chapter 5

Languages that include divisibility

5.1 A general result of Kosovskii for languages with addition and divisibility

Definition. *Let $\mathcal{L}$ be a first order language. An $\mathcal{L}$-formula $\phi(x, y)$ is called a* formula of polynomial growth *if there exist positive rational numbers a, b, c and d, with $d > 1$, such that*

i) for any pair (x, y) of natural numbers with nonzero x, if $\mathbb{N}$ models $\phi(x, y)$, then $y \leq ax^b$;

ii) for every natural number x there exists a natural number y such that $\mathbb{N}$ satisfies $\phi(x, y)$ and $y \geq cx^d$.

The following theorem gives a sufficient condition for a language that expresses addition and divisibility over the naturals to be undecidable.

Theorem 5.1 (Kosovskii, [7])**.** *Let $\mathcal{L}$ be a first order language containing $\{0, 1, +, |\}$ such that there exists a positive-existential $\mathcal{L}$-formula ϕ of polynomial growth. The positive existential theory of $\mathbb{N}$ in the language $\mathcal{L}$ is undecidable.*

For the sake of completeness, we will give the proof of this theorem, due to Kosovskii. Let $\mathcal{L}$ be a first order language containing $\{0, 1, +, |\}$.

Definition. *Let a and b be positive rational numbers. An $\mathcal{L}$-formula $\psi(x, y)$ is called a* formula of quadratic growth with constants a and b *if*

i) for any pair (x, y) of natural numbers with nonzero x, if $\mathbb{N}$ models $\psi(x, y)$, then $y \leq ax^b$;

ii) for every natural number x, $\mathbb{N}$ satisfies $\psi(x, x^2)$.

Definition. *An $\mathcal{L}$-formula $\psi(x, y)$ is called a* formula of quadratic growth *if there exist positive rational numbers a and b such that $\mathcal{L}$ is a formula of quadratic growth with constants a and b.*

Note that every formula of quadratic growth is also a formula of polynomial growth, with the same values for a and b, $c = 1$ and $d = 2$. The converse is not true, but, given a formula of polynomial growth, we can construct a formula of quadratic growth. This is what the next lemma shows:

Lemma 5.2. *Given an $\mathcal{L}$-formula of polynomial growth ϕ, there exists an $\mathcal{L}$-formula $F(x, y)$ consisting of a conjunction of formulas of the forms*

$$x_1 + x_2 = x_3 \quad \textit{and} \quad \phi(x_1, x_2)$$

such that F is of quadratic growth.

Proof. As ϕ is a formula of polynomial growth, there exist positive rationals a, b, c and d as in the definition. Let p, q, M be positive integers such that $cq = p$ and $d^M \geq 2$. Consider the formula

$$F(x, y) : \exists w \exists x_0 \ldots \exists x_M \\ x = x_0 \wedge \bigwedge_{i=1}^{M} \phi(x_{i-1}, x_i) \wedge q^{(M-1)d+1} x_M = p^{(M-1)d+1} y + w.$$

We claim that this formula F is of quadratic growth. To show it satisfies item *i)* of the definition, suppose that $(x, y) \in \mathbb{N}^2$ is such that $\mathbb{N}$ models $F(x, y)$. There exist $x_0, \ldots, x_M$ satisfying (as ϕ is of polynomial growth)

$$x_0 = x \text{ and } x_i \leq a x_{i-1}^b, \text{ for } 1 \leq i \leq M.$$

Hence, there exist positive rational numbers A and B such that $x_M \leq Ax^B$. Moreover, as $q^{(M-1)d+1} x_M \geq p^{(M-1)d+1} y$, there exists a positive rational number C such that $x_M \geq Cy$. We conclude that

$$y \leq \frac{A}{C} x^B,$$

as desired.

It remains to prove that F satisfies item *ii)* of the definition of formula of quadratic growth. We proceed as follows:

Given $x \in \mathbb{N}$, we set $x_0 = x$. Inductively for $i = 0, .., M-1$, we choose $x_{i+1} \in \mathbb{N}$ such that $\mathbb{N} \models \phi(x_i, x_{i+1})$ and $x_{i+1} \geq cx_i^d$ (this is possible since ϕ is of polynomial growth). By the end of this process, we have $x_M \geq c^{Md+1} x_0^{d^M}$, and thus

$$q^{(M-1)d+1} x_M \geq p^{(M-1)d+1} x^2.$$

So we choose $w = q^{(M-1)d+1} x_M - p^{(M-1)d+1} x^2$. □

Formulas of quadratic growth are useful if we are trying to define squaring in a language. However, we still need a formula to exclude the cases where $y \neq x^2$ to do so. Before we show how to obtain such a formula, we will need this arithmetical lemma:

Lemma 5.3. *If y, z be solutions to a system of relations*

$$q_i | a_i x + b_i, \quad i = 1, .., n$$

where x is the unknown and a_i, b_i and q_i are integers such that

i) for $i \neq j$, $\gcd(q_i, q_j) = 1$, and

ii) for every i, $\gcd(a_i, q_i) = 1$,

then $y - z$ is a multiple of $\prod q_i$.

Proof. If y and z are solutions to the system, we obtain

$$q_i | a_i(y - z), \quad i = 1, .., n.$$

Due to the coprimality conditions given, we get

$$q_i | y - z, \quad i = 1, .., n$$

and, from here,

$$\left(\prod q_i\right) \Big| y - z.$$

□

We can now construct the desired formula:

Lemma 5.4. *Let ψ be a $\mathcal{L}$-formula of quadratic growth with constants a and b. If c is a positive integer such that*

$$(c!)^{c+1} > a \quad \textit{and} \quad c > b,$$

then, for any $x \in \mathbb{N}$, $x \neq 0$, the system of relations

$$\begin{cases} ic!x + 1 | ic!y + x, & i = 1, .., c \\ \psi(x, y) \end{cases}$$

(with unknown y) has $y = x^2$ as a unique solution.

Proof. It is clear that $y = x^2$ is a solution to the system.

For $i \neq j$, $\gcd(ic!x + 1, jc!x + 1)$ must divide $(i - j)c!x$. As $|i - j| \leq c$, it follows that $\gcd(ic!x + 1, jc!x + 1)$ must divide $c!x$, and hence

$$\gcd(ic!x + 1, jc!x + 1) = 1.$$

Moreover, for every i, $\gcd(ic!x + 1, ic!) = 1$. Thus, any two solutions to this system must differ by a multiple of $\prod(ic!x + 1)$ (by Lemma 5.3). As

$$\prod_{i=1}^{c}(ic!x + 1) > \prod_{i=1}^{c} ic!x = c!^{c+1}x^c,$$

any two distinct solutions must differ by at least $c!^{c+1}x^c$. But, as for any solution y we have $y \leq ax^b < c!^{c+1}x^c$ (because ϕ is of quadratic growth and the hypothesis on c), the system cannot have two distinct solutions. □

Combining Lemmas 5.2 and 5.4, given a formula of polynomial growth we can construct a positive-existential formula for squaring in $\mathbb{N}$. This proves Theorem 5.1.

5.2 Some consequences of Kosovskii's Theorem

5.2.1 The language of k-th powers and divisibility

For each natural number $k \geq 2$, consider the first order language

$$\mathcal{L}^k_{\text{div}} = \{0, 1, +, |, P_k\}$$

where P_k is interpreted as the unary predicate "is a k-th power".

Definition. *For every $k \geq 2$, we define the polynomials*

$$R_k(t) := (t + 1)^k - t^k \in \mathbb{N}[t].$$

Note that the polynomial $R_k(t)$ is of degree $k-1$, $R_k(1) = 2^k - 1$ and

$$x^{k-1} \leq R_k(x) \leq 2^k x^{k-1} \tag{5.1}$$

for any nonzero $x \in \mathbb{N}$ (because $R_k(x)$ has only positive coefficients). Also note that R_k induces a function $R_k : \mathbb{N} \to \mathbb{N}$ which is strictly increasing, as

$$R_k(x+1) - R_k(x) = (x+2)^k - x^k.$$

Theorem 5.5. *The positive existential theory of* $\mathbb{N}$ *in each of the languages* $\mathcal{L}^k_{\mathrm{div}}$ *is undecidable.*

Proof. Fix $k \geq 2$. We will show that the positive existential $\mathcal{L}^k_{\mathrm{div}}$-formula

$$F(x,y) : \exists t \exists z \exists w \Big(P_k(y) \wedge 2^k x = z + w \wedge z = t + 1 \wedge P_k(y+z) \Big).$$

is of polynomial growth. This will prove the theorem using Theorem 5.1.

Let $(x,y) \in \mathbb{N}^2$ be such that $x \neq 0$ and $\mathbb{N} \models F(x,y)$. Since $\mathbb{N}$ models $F(x,y)$,

- there exists $u \in \mathbb{N}$ such that $y = u^k$,
- $2^k x \geq z$,
- $z > 0$, and
- $y + z$ is a k-th power.

Let us show that $R_k(u) \leq 2^k x$. Suppose the contrary. Then we have

$$u^k = y < y + z \leq y + 2^k x < u^k + R_k(u) = (u+1)^k.$$

Therefore, $y + z$ is a k-th power strictly in between two consecutive k-th powers, which is absurd. We have then (from Equation (5.1))

$$2^k x \geq R_k(u) \geq u^{k-1},$$

and thus

$$y = u^k \leq 2^{\frac{k^2}{k-1}} x^{\frac{k}{k-1}}.$$

Let $a = 2^{\frac{k^2}{k-1}}$ and $b = \frac{k}{k-1}$. Hence $y \leq a x^b$, as required in the first item of the definition of formula of polynomial growth.

Let x be a positive integer. There exists a natural number $x_0 \geq 1$ such that

$$R_k(x_0) \leq 2^k x < R_k(x_0 + 1) \tag{5.2}$$

(since R_k is strictly increasing).

Choosing $z = R_k(x_0)$, $t = R_k(x_0) - 1$ and $w = 2^k x - R_k(x_0)$, we see that

$$\mathbb{N} \models F(x, x_0^k).$$

Moreover, we have

$$\begin{aligned} x_0^k = \left(x_0^{k-1}\right)^{\frac{k}{k-1}} &\geq \left(\left(\frac{(x_0+1)}{2}\right)^{k-1}\right)^{\frac{k}{k-1}} \\ &\geq \left(\frac{R_k(x_0+1)}{2^{2k-1}}\right)^{\frac{k}{k-1}} \quad \text{(by Equation (5.1))} \\ &\geq \left(\frac{x}{2^{k-1}}\right)^{\frac{k}{k-1}} \quad \text{(by Equation (5.2))} \\ &= \frac{1}{2^k} x^{\frac{k}{k-1}}. \end{aligned}$$

As $\frac{k}{k-1} > 1$, this shows that item *ii)* of the definition of formula of polynomial growth is satisfied, with $c = 2^k$ and $d = \frac{k}{k-1}$. □

5.2.2 The language of an exponential function and divisibility

For each natural number $k \geq 2$, consider the first order language

$$\mathcal{L}_{\text{div}}^{\exp_k} = \{0, 1, +, |, n \mapsto k^n\}.$$

Theorem 5.6. *For each $k \geq 2$, the positive existential theory of $\mathbb{N}$ in the language $\mathcal{L}_{\text{div}}^{\exp_k}$ is undecidable.*

Proof. Fix $k \geq 2$. We will show that the $\mathcal{L}_{\text{div}}^{\exp_k}$-formula

$$F(x, y) : \exists z (k^z \leq x \wedge y \leq k^{2z+2})$$

is of polynomial growth and conclude with Theorem 5.1.

Given $x, y \in \mathbb{N}$, $x \neq 0$, such that $\mathbb{N}$ models $F(x, y)$, there exists $n \in \mathbb{N}$ such that

$$y \leq k^{2n+2} = (k^n)^2 k^2 \leq k^2 x^2.$$

Therefore, F satisfies item *i)* of the definition of formula of polynomial growth with $a = k^2$ and $b = 2$.

On the other hand, given $x > 0$, there exists $n \in \mathbb{N}$ such that

$$k^n \leq x < k^{n+1}.$$

Then, as $x^2 < k^{2n+2}$, the formula $F(x, x^2)$ is satisfied in $\mathbb{N}$. □

5.3 Weakening the divisibility relation

As mentioned in the Introduction, the main logical problem in our context is the problem of the undecidability of the positive existential theory of $\mathbb{Z}$ in the language

$$\mathcal{L}^2 = \{0, 1, +, P_2\}.$$

By Theorem 5.5, we know that the positive existential theory of $\mathbb{N}$ in the language $\mathcal{L}^2_{\text{div}}$ is undecidable. We will show a theorem somewhat analogous to Theorem 5.1. This theorem will allow us to weaken the divisibility relation, leaving the "is a square" relation untouched:

Theorem 5.7. *Let $\mathcal{L}$ be a first order language containing $\{0, 1, +, P_2\}$, where P_2 is interpreted over $\mathbb{N}$ as the predicate "is a square". If there exists a positive existential $\mathcal{L}$-formula $\phi(x, y)$ that satisfies*

i) if $y = x^2$, then $\mathbb{N}$ satisfies $\phi(x, y)$, and

ii) if $\mathbb{N}$ models $\phi(x, y)$ and x is nonzero, then x divides y,

then the positive existential theory of $\mathbb{N}$ in the language $\mathcal{L}$ is undecidable.

Proof. Let $\phi(x, y)$ be a formula satisfying the hypothesis of the theorem. Consider the $\mathcal{L}$-formula

$$F(x, y) : P_2(y) \wedge P_2(y + 2x + 1) \wedge \phi(x, y) \wedge \phi(x + 1, y + 2x + 1).$$

We will show that $\mathbb{N}$ models $F(x, y)$ if and only if $y = x^2$, and the conclusion will follow from Proposition 2.11.

First of all, it is clear that if $y = x^2$ then $\mathbb{N}$ satisfies $F(x, y)$. So let $x, y \in \mathbb{N}$ be such that $\mathbb{N} \models F(x, y)$. If $x = 0$, then y must also be 0, as both y and $y + 1$ must be squares.

Suppose that $x \neq 0$. Write $y = a^2$ (for nonnegative a). Let us show that $y \leq x^2$. If it is not the case, then we have

$$a^2 = y < y + 2x + 1 < y + 2a + 1 = (a + 1)^2$$

which is impossible as $y + 2x + 1$ is a square.

Let $t \in \mathbb{N}$ be such that $y = tx$ (such a t exists by hypothesis since $\mathbb{N}$ satisfies $\phi(x, y)$ and $x \neq 0$). As $\mathbb{N}$ satisfies $\phi(x+1, y+2x+1)$ and $x+1 \neq 0$, we have also

$$(x + 1)|(y + 2x + 1),$$

hence $x+1$ divides $y+x = tx+x$ and finally $x+1$ divides $t+1$. Therefore, we have $x \leq t$, and it follows that

$$x^2 \leq tx = y. \qquad \square$$

There exist languages satisfying the hypotheses of Theorem 5.7 whose positive existential theory is contained in the positive existential theory of $\mathbb{N}$ with addition, the "is a square" predicate and divisibility.

For example, for $k \geq 1$ consider the relation R_k defined by: $(x, y) \in R_k \subseteq \mathbb{N}^2$ if and only if there exists $t \in \mathbb{N}$ such that $y = tx$ and, for every prime p dividing t, $p^k \leq x$. About this definition, the following two obvious facts must be pointed out:

Lemma 5.8. *If x, y and k are positive integers, then*

a) $(x, y) \in R_k$ implies $x|y$;

b) if there exists an integer t such that $y = t^k x \leq x^2$, then $(x, y) \in R_k$.

Corollary 5.9. *For every $k \geq 1$, the positive existential theory of $\mathbb{N}$ in the language*

$$\mathcal{L}_k^2 = \{0, 1, +, P_2, R_k\}$$

(with P_2 interpreted as usual) is undecidable.

Proof. Fix $k \geq 1$. Consider the $\mathcal{L}_k^2$-formulas

$$F_n^k(x, y) : \exists a_1 \ldots \exists a_n \bigwedge_{i=1}^{n} (x, a_i) \in R_k \wedge y = \sum_{i=1}^{n} a_i, \text{ for } 1 \leq n \leq g(k),$$

$$G^k(x, y) : \bigvee_{i=1}^{g(k)} F_i^k(x, y),$$

where $g(k)$ is Waring's number for k, given by Hilbert-Waring Theorem 3.8.

Let us prove that the formula $G^k(x, y)$ satisfies the hypothesis of Theorem 5.7. If $\mathbb{N}$ satisfies $G^k(x, y)$, there exist $n \in \{1, \ldots, g(k)\}$ and natural

numbers $a_1, \ldots, a_n$ such that $y = \sum a_i$. By item a) of Lemma 5.8, x divides each a_i. Hence x divides y, and $G^k(x, y)$ verifies hypothesis *ii)* of the theorem.

It remains to prove that $G^k(x, y)$ satisfies hypothesis *i)* of Theorem 5.7. As any positive integer x can be written as sum of $n \leq g(k)$ positive k-powers $x_1, \ldots, x_n$, by item b) of Lemma 5.8 we obtain that, for $1 \leq i \leq n$, $(x, x_i x) \in R_k$, and thus

$$\mathbb{N} \models G^k(x, x^2). \qquad \square$$

Chapter 6

Diophantine problem over $\mathbb{Q}$ versus Diophantine homogeneous problem over $\mathbb{Z}$

We begin this chapter by stating a "folklore" result relating Hilbert's Tenth Problem over $\mathbb{Q}$ with a decidability problem over $\mathbb{Z}$ (cf. [5] or [12]) :

Theorem 6.1. *The decision problem for solutions of Diophantine equations in $\mathbb{Q}$ is algorithmically equivalent to the decision problem for nonzero solutions of homogeneous forms in $\mathbb{Z}$.*

This result can be extended to formally real number fields (finite extensions of $\mathbb{Q}$ where -1 cannot be written as a sum of squares).

Theorem 6.2. *Let K be a formally real number field. The decision problem for solutions of Diophantine equations in K is algorithmically equivalent to the decision problem for nonzero solutions of forms in O_K (the ring of integers of K).*

Before giving the proof of this theorem, we will need several definitions and lemmas.

As an extension of $\mathbb{Q}$, let K be of degree $n = n_1 + 2n_2$, where n_1 is the number of real conjugates for K. The n $\mathbb{Q}$-isomorphisms between K and each of its conjugates will be written as g_i, with $i = 1, \ldots, n$, such that for $i = 1, \ldots, n_1$ the isomorphism g_i is *onto* a real conjugate of K and, for $i = n_1 + 1, \ldots, n$, onto a complex conjugate.

Definition. *An element $x \in K$ is* totally positive *if, for each $i = 1, \ldots, n_1$, $g_i(x) \geq 0$.*

Definition. *Given $x \in K$, the* norm *of x is defined as*

$$N(x) = \prod_{i=1}^{n} g_i(x).$$

Lemma 6.3. *Let $A, B \in K$ with A totally positive. There exists $M \in \mathbb{N}$ such that, for any $k \geq M$, $kA - B$ is totally positive.*

Proof. Let $A_m = \min\{g_1(A), \ldots, g_{n_1}(A)\}$ and $B_m = \max\{g_1(B), \ldots, g_{n_1}(B)\}$. Choose M such that $MA_m - B_m \geq 0$. Then, for any $k \geq m$ and $i \in \{1, \ldots, n_1\}$, we have

$$g_i(kA - B) = kg_i(A) - g_i(B) \geq MA_m - B_m \geq 0. \qquad \square$$

Lemma 6.4. *If $A \in K$ is nonzero and totally positive then its norm is strictly positive.*

Proof. Given $i \in \{n_1 + 1, \ldots, n\}$, there exists some $j \in \{n_1 + 1, \ldots, n\}$, different from i, such that $g_j(A)$ is complex conjugate to $g_i(A)$. Thus

$$N(A) = \prod_{i=1}^{n_1} g_i(A) \prod_{i=n_1+1}^{n} g_i(A)$$

is positive, as A is totally positive and no $g_i(A)$ equals zero. $\square$

Lemma 6.5. *Let $A, B \in K$, with A totally positive and nonzero. Then*

$$\lim_{k \to \infty} N(kA - B) = \infty$$

Proof. As no $g_i(A)$ equals zero, $N(kA - B)$ is a polynomial in k of degree n and leading coefficient $N(A)$, which is positive by the preceding lemma. $\square$

Theorem 6.6 (Second Artin-Scheier theorem)**.** *An element $x \in K$ is totally positive if and only if it can be written as a sum of squares of elements in K.*

Proving this theorem requires several previous properties of totally positive elements and formally real fields. A detailed proof can be found in [18], page 259.

Combining this theorem with the previous lemmas, we obtain

Lemma 6.7. *Let $A, B \in O_K$ be elements that can be written as sums of squares of elements in O_K. There exists $M \in \mathbb{N}$ such that, for $k \geq M$, $kA - B$ can be written as a sum of squares of elements in O_K.*

Proof. By Lemma 6.3, there exists $k_0 \in \mathbb{N}$ such that $k_0A - B$ is totally positive. By Theorem 6.6, there exists $Q \in \mathbb{N}$ such that $Q(k_0A - B)$ can be written as a sum of squares of elements in O_K. Thus, as B is also a sum of squares in O_K, for each $k \geq Qk_0$ we have

$$kA - B = (k - Qk_0)A + Q(k_0A - B) + (Q - 1)B. \qquad \square$$

We can now tell when certain elements of O_K can be written as sums of squares. The next theorem will give us conditions to impose a uniform upper bound on the number of squares that add up to a number, much in the spirit of Lagrange's four squares theorem:

Theorem 6.8 (Siegel, [17])**.** *For each number field K there exist $M_K \in \mathbb{N}$ and $N_K \in \mathbb{R}$ such that every $x \in O_K$ with $N(x) \geq N_K$ that can be written as a sum of squares of elements in O_K can be written as a sum of exactly M_K squares of elements in O_K.*

Lemma 6.9. *Given a prime number p, there exist sequences (z_i) and (w_i) in $\mathbb{N}$ such that $\lim z_i = \infty$, $\lim w_i = \infty$ and, for each i, $z_i^2 - pw_i^2 = 1$.*

Proof. This is a known fact about Pell equations. See, for example, [6]. $\square$

As K is a finite extension of $\mathbb{Q}$, there must exist prime numbers whose square roots do not belong to K. Let p be one such prime.

Lemma 6.10. *Let K be a formally real number field, and let $x_0, \ldots, x_m$ be elements of O_K. The equation*

$$x_0^4 - \left(\sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{M_K} u_i^2\right)^2 + p\left(\sum_{i=1}^{M_K} v_i^2\right)^2 = 0 \tag{6.1}$$

(with unknowns u_i and v_i) has a solution in O_K with not all u_i and v_i equal to zero if and only if $x_0 \neq 0$.

Proof. Let

$$X = \sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{M_K} u_i^2 \text{ and } Y = \sum_{i=1}^{M_K} v_i^2.$$

If $x_0 = 0$, then Equation (6.1) becomes $X^2 - pY^2 = 0$. Therefore, as $\sqrt{p}$ does not belong to K, Equation (6.1) cannot have any solution with some nonzero u_i or v_i.

Conversely, if $x_0 \neq 0$, let $A = x_0^2$ and $B = \sum_{i=1}^{n} x_i^2$. Let us consider the sequences (z_i) and (w_i) given by Lemma 6.9. By Theorem 6.6, A is totally positive. By Lemmas 6.3 and 6.7 and by Theorem 6.8, there exists $k \in \mathbb{N}$ such that $z_k A - B$ and $w_k A$ can be written as sums of M_K squares of elements in O_K. Taking the u_i and the v_i as such elements, respectively, we obtain a solution of (6.1) satisfying the condition given. □

Proof of Theorem 6.2. Suppose that there exists an algorithm to decide solvability of diophantine equations in K. Let $F(x_1, \ldots, x_m)$ be an homogeneous form in O_K. It will have a nonzero solution in O_K if and only if the diophantine equation

$$F(1, x_2, \ldots, x_m)F(x_1, 1, \ldots, x_m) \ldots F(x_1, x_2, \ldots, 1) = 0$$

has a solution in K.

For the converse, suppose we can decide which forms over O_K have got nontrivial zeros in O_K, and let $f(x_1, \ldots, x_m) = 0$ be a diophantine equation in K. We homogenize f with a variable x_0, obtaining an homogenous form $F(x_0, \ldots, x_m)$ in O_K. Let d be the degree of F, and let p be a prime integer such that $\sqrt{p} \notin K$. We consider the homogeneous form

$$(F(x_0, \ldots, x_m))^8 + \left(x_0^4 - \left(\sum_{i=1}^{m} x_i^2 + \sum_{i=1}^{M_K} u_i^2 \right)^2 + p \left(\sum_{i=1}^{M_K} v_i^2 \right)^2 \right)^{2d}.$$

By the preceding lemma, this form will have a nontrivial zero over O_K if and only if F has got a zero over O_K with $x_0 \neq 0$, i.e., if and only if f has a solution in K. □

Bibliography

[1] R. Cori and D. Lascar, *Mathematical Logic, A Course with Exercises, Part II*, Oxford University Press (2001).

[2] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973).

[3] M. Davis, Y. Matiyasevich and J. Robinson, *Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution*, Proceedings of Symposia in Pure Mathematics **28**, 323-378 (1976).

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 5th Edition*, Oxford Science Publications (2002).

[5] K. H. Kim and F. W. Roush, *Problems Equivalent to Rational Diophantine Solvability*, Journal of Algebra **124**, 493-505 (1989).

[6] H. Koch, *Number theory: algebraic numbers and functions*, Graduate Studies in Mathematics, v. 24, AMS, 2000.

[7] N. K. Kosovskii, *On solutions of systems consisting of both word equations and word length inequalities*, Zap. Naucn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. **40**, 24-29 (1974).

[8] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, in The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer, 677-680, (1990).

[9] —— *The Diophantine problem for addition and divisibility*, Transactions of the American Mathematical Society **235**, 271-283 (1978).

[10] Y. Matiyasevich, *Enumerable sets are diophantine*, Dokladii Akademii Nauk SSSR, **191**, 279-282 (1970); English translation, Soviet Mathematics Doklady **11**, 354-358 (1970).

[11] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, to appear as Proceedings of the Hausdorff Institute of Mathematics, in Zapiski POMI, Steklov Institute of Mathematics, and in the Journal of Mathematical Sciences (2010).

[12] T. Pheidas, *Extensions of Hilbert's Tenth Problem*, The Journal of Symbolic Logic **59-2**, 372-397 (1994).

[13] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem : Questions of decidability for addition and n-th powers*, Fundamenta Mathematicae **185**, 171-194 (2005).

[14] —— *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238-2**, 349-366 (2008).

[15] M. Presburger, *On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation*, History and Philosophy of Logic **12-2**, 92-101 (1991).

[16] A. L. Semenov, *Logical theories of one-place functions on the set of natural numbers*, Math. USSR Izvestiya **22-3**, 587-618 (1984).

[17] C. L. Siegel, *Generalization of Waring's Problem to Algebraic Number Fields*, American Journal of Mathematics **66-1**, 122-136 (1944).

[18] K. Szymiczek, *Bilinear algebra: an introduction to the algebraic theory of quadratic forms*, Algebra, Logic and Applications series, v. 7, CRC, 1997.

[19] V. Terrier, *Decidability of the existential theory of the set of natural numbers with order, divisibility, power functions, power predicates, and constants*, Proceedings of the American Mathematical Society **114-3**, 809-816 (1992).

[20] R. C. Vaughan and T. D. Wooley, *Waring's Problem: A Survey.*

[21] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*, Contemporary Mathematics **270**, 261-274 (2000).