Generalized Hilbert's Tenth Problem

Francesco A. Zuccon

A thesis

in the

Department of Mathematics

Presented in Partial Fulfillment of the Requirements

for the degree of Master of Science, Mathematics at

Concordia University

Montreal, Québec, Canada

July 2025

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Mr. Francesco Zuccon

Entitled: Generalized Hilbert's Tenth Problem

and submitted in partial fulfillment of the requirements for the degree of

Master of Science

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair

_____ Examiner
Dr. Adrian Iovita

_____ Examiner

_____ Thesis Supervisor(s)
Dr. Carlo Pagano

_____ Thesis Supervisor(s)

Approved by _____
Dr. Lea Popovic Chair of Department or Graduate Program Director

Dr. Pascale Sicotte Dean of Faculty of Arts and Science

Generalized Hilbert's Tenth Problem

Francesco A. Zuccon

The aim of this work is to retrace the path to the solution of the classical Hilbert's Tenth Problem and the attempts trying to generalize it reaching, finally, a new result concerning its extension in number fields. First we deal with the classical case classifying diophantine functions as the recursive ones, using the diophantinity of the exponential as a key tool. In order to generalize the unsolvability of the diophantine problem to rings of integers of number fields the line is to simulate the core of the classicl proof, which seems to be more natural in the setting of totally real number fields as shown by the work of Denef and Lipshitz. After that few attempts were done to reach a general result, Pheidas was able to use the Elliptic Curves to obtain a new criteria which, in its generalized version of Shlapentokh, is the key together with the new additive combinatorics techniques of Pagano-Koymans to the proof of the general case.

Contents

Chapter 1

The Classic Case: MRDP Theorem

In the beginning of the twentieth century, at the International Congress of mathematicians, David Hilbert presented a list of problems, which exerted great influence on the development of mathematics in the twentieth century. The tenth problem on the list had to do with solving Diophantine equations. Hilbert was interested in the construction of an algorithm which could determine whether an arbitrary polynomial equation in several variables had solutions in the integers.
Here is his wording, translated to English:

Given a Diophantine equation with any number of unknown quantities and with integral numerical coefficients: to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

In this chapter, we will show that no such algorithm exists mainly following the line exposed in [1], collecting the main results given by Martin Davis, Julia Robinson, and Hilary Putnam in the 1950s and 1960s, with the final missing piece that was given in 1970 by Yuri Matiyasevic.

1.1 Diophantine sets

First of all, the notion of *diophantine set* will be developed, being fundamental during the whole chapter.

Definition 1.1.1. $n \in \mathbb{N} : S \subseteq \mathbb{Z}^n$ is a *diophantine set* if $\exists m \in \mathbb{N} \ \wedge \ \exists P \in$

$\mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that:

$$S = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \exists (y_1, \ldots, y_m) \in \mathbb{Z}^m : P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

In this case the polynomial P is called *representative* for the set S, which can be denoted as S_P.

Remark 1.1.2. It is evident that finite unions or intersections of Diophantine sets (in both senses of integers or positive integers) are again Diophantine:

$$\bigcup_{1 \le i \le n} S_{P_i} = S_{\prod_{1 \le i \le n} P_i} , \quad \bigcap_{1 \le i \le n} S_{P_i} = S_{\sum_{1 \le i \le n} P_i^2} .$$

where in the second equality the polynomials are considered with the same variables $x_1, \ldots, x_n$, but different variables $y_{i,1}, \ldots, y_{i,m_i}$.

Lemma 1.1.3. *$S \subseteq \mathbb{Z}^n$ Diophantine $\implies$ $S \cap \mathbb{N}^n$ Diophantine.*

Proof. Recalling the *Lagrange's four-squares Theorem* which states that every positive integer is a sum of four squares of integers, then it follows from:

$$S = S_P : S_P \cap \mathbb{N}^n = S_{P(x_1,\ldots,x_n,y_1,\ldots,y_m)} \cap \bigcap_{i=1}^{n} S_{(x_i - a_i^2 - b_i^2 - c_i^2 - d_i^2)}$$

which is Diophantine by Remark 1.2. □

Example 1.1.4. Here a few elementary examples:

- Divisibility: $\{(x, y) \in \mathbb{Z}^2 : x \mid y\} = \{(x, y) \in \mathbb{Z}^2 \ \exists z \in \mathbb{Z} : xz = y\}$.
- Ordering relation:$\{(x, y) \in \mathbb{Z}^2 : x < y\} = \{(x, y) \in \mathbb{Z}^2 \ \exists (a, b, c, d) \in \mathbb{Z}^4 : x + a^2 + b^2 + c^2 + d^2 + 1 = y\}$.
- Non-square numbers: $\{x \in \mathbb{Z} : \nexists y \in \mathbb{Z} \setminus \{\pm 1\} : y^2 \mid x\} = \{\alpha \in \mathbb{Z} \ \exists (a, b, c, d, x, y, w, z, p, q, r, s) \in \mathbb{Z}^{12} : (a^2 + b^2 + c^2 + d^2)^2 + x^2 + y^2 + w^2 + z^2 + 1 = \alpha = (a^2 + b^2 + c^2 + d^2 + 1)^2 - (p^2 + q^2 + r^2 + s^2 + 1)\}$. Note that thanks to 1.1.2, 1.1.3 and the previous example this can be seen in the following easier and more natural description: $\{x \in \mathbb{Z} \ \exists n \in \mathbb{Z} : n > 0 \wedge n^2 < x < (n + 1)^2\}$

Definition 1.1.5. A function $f \in \bigcup_{n \in \mathbb{N}} Hom_{Set}(\mathbb{Z}^n, \mathbb{Z})$ is called *Diophantine* if its graph $\Gamma(f) = \{(x_1, \ldots, x_n, y) \in \mathbb{Z}^{n+1} : y = f(x_1, \ldots, x_n)\}$ is a Diophantine set.

The claim of the first half of this chapter is precisely the following theorem:

Theorem 1.1.6. *The function* $exp : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}$ *such that* $exp(a, b) = a^b$ *is diophantine.*

Note that the domain isn't a power of $\mathbb{Z}$, but can be seen that way extending $exp\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ or just considering the more restrictive condition for natural numbers of 1.1.3.

1.2 Special form of Pell's equation

1.2.1 Historical background

As said in the introduction, H10 was reduced to 1.1.6 by Davis and Robinson, but Robinson was also able to state a technical condition that, if checked, would have implied the theorem.
The core of the idea found by Matiyasevich to verify this abstract condition lies in the following properties of Fibonacci's number.

Defining the Fibonacci's number $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$ per $n > 1$ and the golden ratio $\phi = \frac{1+\sqrt{5}}{2}$, one has the key properties:

$$F_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}} \tag{1.1}$$

$$F_m^2 \mid F_n \implies F_m \mid n \tag{1.2}$$

The first property underlines the exponential character of the sequence, the second gives a diophantine control of the indexes thanks to the first example in 1.1.4.

After this brilliant trick sensed by Matiyasevich, Robinson was able to convert it in a clever way with another sequence satisfying a similar recursive relation and preserving an analogue of the two key properties presented above, thanks to which sequence the abstract condition could have been avoided.
In particular, she was able to reduce 1.1.6 to the diophantinity of the function that associates to a positive integer n the correspondent Fibonacci's number F_n, or, as it will be shown, the analogue of this function but replacing to Fibonacci's numbers the recursive sequence found after.
This is the approach presented below taking inspiration from [1], but proceeding in a more constructive and intuitive way.

1.2.2 Path to a special exponential diophantinity

As mentionted before, the first attempt to prove the diophantinity of the exponential function is to try to prove the diophantinity of a certain function which has an exponential character similar to the the property (1) of Fibonacci's numbers, and which canonically builds a bridge from exponentiation to polynomials, which can naturally be found in Pell's equation:

$$x^2 - Ny^2 = 1 \tag{1.3}$$

Indeed, by Dirichlet's unit theorem applied to the number field $\mathbb{Q}(\sqrt{N})$ (for N non-square), it turns out that the rank of the group of units of the ring of integers is one, so that in particulare every solution of (3) is a power of a fundamental unit.

Furthermore, the theory of continued fractions gives an explicit procedure to find the fundamental unit, thanks to the continued fraction of $\sqrt{N}$ that can be expressed as $[a_0, \overline{B, 2a_0}]$, where B is a palindromic vector of integers all of size strictly bounded by $a_0 = \lfloor \sqrt{N} \rfloor$, in which case the fundamental unit can be recover as the numerator and denominator of the rational number $x/y = [a_0, B]$ if the lenght of the vector B is odd, otherwise $x/y = [a_0, B, 2a_0, B]$.

For our purpose, the equation (3) is useful cause, once fixed the fundamental solution (x_1, y_1), one has the identity $x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n$ which is an exponential expression that can be encoded in a polynomial (which is (3)).
The intuition found by Robinson was a particular choice for N in (3) so that the fundamental unit is clear even without recalling all the results cited above about Dirichlet's theorem or continued fraction (indeed, it is not in general easy to describe explicitly the palindromic vector B), so the equation in which there will be the focus for the rest of the discussion is remarked in the following definition:

Definition 1.2.1. Let $a > 1$ integer and consider the special Pell's equation:

$$x^2 - (a^2 - 1)y^2 = 1 \tag{1.4}$$

define the n-th solution (n-th power of the fundamental unit which existence will explicitly be established in the following lemma) as $(x_n(a), y_n(a))$.
In particular, by the discussion above or, more elementary, thanks to 1.2.3 and 1.2.4 below, it turns out:

$$x_n(a) + y_n(a)\sqrt{a^2 - 1} = (x_1(a) + y_1(a)\sqrt{a^2 - 1})^n$$

Remark 1.2.2. Notice that the choice $N = a^2 - 1$ makes evident the trivial solution $(x_1(a), y_1(a)) = (a, 1)$, and indeed the following lemma will prove that is the fundamental unit, as in this case there is a trivial continued fraction expansion: $\sqrt{a^2-1} = [a, \overline{1, 2a}]$.

Remark 1.2.3. For a general Pell's equation in the form of (3), one has trivially that if $(x, y), (w, z)$ are solutions, then also their product $(p, q) = (xw + Nyz, xz + yw)$ (as numbers in $\mathbb{Z}[\sqrt{N}]$) is again a solution:

$$p^2 - Nq^2 = (p + q\sqrt{N}) \cdot (p - q\sqrt{N}) =$$

$$= (x + y\sqrt{N}) \cdot (w + z\sqrt{N}) \cdot (x - y\sqrt{N}) \cdot (w - z\sqrt{N}) =$$

$$= (x + y\sqrt{N}) \cdot (x - y\sqrt{N}) \cdot (w + z\sqrt{N}) \cdot (w - z\sqrt{N}) = 1 \cdot 1 = 1$$

Lemma 1.2.4. *The following hold:*

i. $\forall a \geq 2,\ \nexists\, x, y \in \mathbb{Z}$ *such that* $1 < x + \sqrt{a^2-1}\ y < a + \sqrt{a^2-1} \ \wedge\ x^2 - (a^2-1)y^2 = 1$.

ii. $\{(x, y) \in \mathbb{N}^2 : x^2 - (a^2-1)y^2 = 1\} = \{(x_n(a), y_n(a)) : n \in \mathbb{N}\}$

Proof. i. By absurd assume it's true, then by the identity:

$$(x + \sqrt{a^2-1}\ y)(x - \sqrt{a^2-1}\ y) = x^2 - (a^2-1)y^2 = 1$$

One can deduce from $1 < x + \sqrt{a^2-1}\ y < a + \sqrt{a^2-1}$ that it has to be $a - \sqrt{a^2-1} < x - \sqrt{a^2-1}\ y < 1$, so that:

$$-1 < -x + \sqrt{a^2-1}\ y < -a + \sqrt{a^2-1}$$

which added to the inequality taken in the hypothesis gives:

$$0 < 2y\sqrt{a^2-1} < 2\sqrt{a^2-1}$$

so that it follows $0 < y < 1$, a contradiction for $y \in \mathbb{Z}$ ↯.
ii. Suppose by absurd

$$\exists (\overline{x}, \overline{y}) \in \{(x, y) \in \mathbb{N}^2 : x^2 - (a^2-1)y^2 = 1\} \setminus \{(x_n(a), y_n(a)) : n \in \mathbb{N}\}$$

then being $x_1(a) + y_1(a)\sqrt{a^2-1} = a + \sqrt{a^2-1} > 1$, the sequence $s_n(a) = x_n(a) + y_n(a)\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n$ is increasing in n, so that $\exists! n_0 \in \mathbb{N}$ (which must be greater than 1 cause of the previous claim) such that:

$$s_{n_0}(a) < \overline{x} + \overline{y}\sqrt{a^2-1} < s_{n_0+1}(a) = s_{n_0}(a) \cdot (a + \sqrt{a^2-1})$$

So that in particular diving by $s_n(a)$:

$$1 < \frac{\overline{x} + \overline{y}\sqrt{a^2-1}}{s_n(a)} < a + \sqrt{a^2-1}$$

But rationalizing multipling and dividing by $x_{n_0}(a) - y_{n_0}(a)\sqrt{a^2-1}$:

$$1 < (\overline{x} + \overline{y}\sqrt{a^2-1}) \cdot (x_{n_0}(a) - y_{n_0}(a)\sqrt{a^2-1}) < a + \sqrt{a^2-1}$$

which is a solution (thanks to 1.2.3) that contradicts *i.*. □

So once stated this crucial lemma it is possible to make clear the main goal of this entire section, which was announced to be the diophantinity of a particular function of exponential character:

Theorem 1.2.5. *The function $x : \mathbb{N} \times \mathbb{N}_{>1} \to \mathbb{N}$ such that $x(k,a) = x_k(a)$ is diophantine.*

In particular, to reach this purpose one has to find a representative polynomial $P(x_1, x_2, x_3, y_1, \ldots, y_m) \in \mathbb{Z}[x_1, x_2, x_3, y_1, \ldots, y_m]$ such that (recalling $\Gamma_x = \{(x,k,a) : x = x_k(a)\}$):

$$\Gamma_x = \{(x,k,a) \in \mathbb{N}^3 : \exists (y_1, \ldots, y_m) \in \mathbb{N}^m : P(x,k,a,y_1,\ldots,y_m) = 0\}$$

By 1.1.2 one can reach the construction of the polynomial by steps using a sistem of more elementary polynomials that one aims to be vanishing simultaneously, so that it is natural from 1.2.4 to define the first equation of the system:

$$S = \begin{cases} \text{I} : x^2 - (a^2-1)y^2 = 1 \end{cases}$$

This way, thanks to 1.2.4, $\exists i \in \mathbb{N} : x = x_i(a)$, so the rest of the system will be about trying to force $i = k$. To do that, one has to investigate the properties of the set of solutions of the special Pell's equation (1.4).
Indeed, again by 1.2.4 one can define the isomorphism of monoids $\phi_a : \mathbb{N} \to S_a := \{(x,y) \in \mathbb{N}^2 : x^2 - (a^2-1)y^2 = 1\}$ setting in the most natural way $\phi_a(n) := (x_n(a), y_n(a))$, but one has to describe in a more precise way its behaviour from both the additive and the multiplicative point of views, as shown in the next lemma, which contains all the basic properties of (1.4):

Lemma 1.2.6. *The followings hold:*

i. $x_{n\pm m}(a) = x_n(a) \cdot x_m(a) \pm y_n(a) \cdot y_m(a) \cdot (a^2-1)$.

ii. $y_{n\pm m}(a) = x_m(a) \cdot y_n(a) \pm x_n(a) \cdot y_m(a)$.

iii. $x_{n+1}(a) = 2a \cdot x_n(a) - x_{n-1}(a)$.

iv. $y_{n+1}(a) = 2a \cdot y_n(a) - y_{n-1}(a)$.

v. $\forall n \in \mathbb{N} : x_{n+1}(a) > x_n(a) \geq a^n \ \wedge \ x_n(a) \leq (2a)^n$.

vi. $\forall n \in \mathbb{N} : y_{n+1}(a) > y_n(a) \geq n \ \wedge \ y_n(a) < (2a)^n$.

vii. $x_{n\cdot m}(a) = \sum_{i=0,\ i\equiv_2 0}^{m} \binom{m}{i} \cdot x_n(a)^{m-i} \cdot y_n(a)^i \cdot (a^2-1)^{\frac{i}{2}}$.

viii. $y_{n\cdot m}(a) = \sum_{i=0,\ i\equiv_2 1}^{m} \binom{m}{i} \cdot x_n(a)^{m-i} \cdot y_n(a)^i \cdot (a^2-1)^{\frac{i-1}{2}}$.

Proof. Those are just trivial computations:

$$x_{n\pm m}(a) + y_{n\pm m}(a) \cdot \sqrt{a^2-1} = (a + \sqrt{a^2-1})^{n\pm m} =$$

$$= (a + \sqrt{a^2-1})^{n} \cdot (a + \sqrt{a^2-1})^{\pm m} =$$

$$= (x_n(a) + y_n(a)\sqrt{a^2-1}) \cdot (x_m(a) \pm y_m(a)\sqrt{a^2-1}) =$$

$$= (x_n(a)\cdot x_m(a) \pm (a^2-1)\cdot y_n(a)\cdot y_m(a)) + (x_m(a)\cdot y_n(a) \pm x_n(a)\cdot y_m(a))\sqrt{a^2-1}$$

which proves *i.* and *ii.*.
Then, applying this addition formulas for $m = \pm 1$ one can obtain *iii.* and *iv.*:

$$x_{n+1}(a) = a \cdot x_n(a) + y_n(a) \cdot (a^2-1) \ \wedge \ x_{n-1}(a) = a \cdot x_n(a) - y_n(a) \cdot (a^2-1)$$

Adding both of them, one has $x_{n+1}(a) + x_{n-1}(a) = 2a \cdot x_n(a)$, the claim of *iii.*. Analogously for *iv.*:

$$y_{n+1}(a) = a \cdot y_n(a) + x_n(a) \ \wedge \ \ y_{n-1}(a) = a \cdot y_n(a) - x_n(a)$$

$$\implies y_{n+1}(a) + y_{n-1}(a) = 2a \cdot y_n(a)$$

Thanks to these recursive formulas (which is very similar to the one of Fibonacci's numbers), one can easily prove *v.* and *vi.* by induction.
The base steps are tautologies, and for $n > 1$ using *iii.* & *iv.* and the inductive hypothesis $x_n(a) > x_{n-1}(a)$ and $x_n(a) \geq a^n$, so as $y_n(a) > y_{n-1}(a)$ and $y_n(a) \geq n$:

$$x_{n+1}(a) = 2a\cdot x_n(a) - x_{n-1}(a) > 2\cdot x_n(a) - x_n(a) = x_n(a) \implies x_{n+1}(a) > x_n(a)$$

$$x_{n+1}(a) = 2a\cdot x_n(a) - x_{n-1}(a) > 2a\cdot x_n(a) - x_n(a) = (2a-1)\cdot x_n(a) > a\cdot x_n(a)$$

$$\implies x_{n+1}(a) \geq a^{n+1}$$

$$x_{n+1}(a) = 2a \cdot x_n(a) - x_{n-1}(a) < 2a \cdot x_n(a) < 2a \cdot (2a)^n = (2a)^{n+1}$$

$$y_{n+1}(a) = 2a \cdot y_n(a) - y_{n-1}(a) > 2a \cdot y_n(a) - y_n(a) = y_n(a) \geq n$$
$$\implies y_{n+1}(a) > y_n(a) \ \wedge \ y_{n+1}(a) \geq n+1$$
$$y_{n+1}(a) = 2a \cdot y_n(a) - y_{n-1}(a) < 2a \cdot y_n(a) < 2a \cdot (2a)^n = (2a)^{n+1}$$

Finally, for *vii.* and *viii.* using the binomial theorem:

$$x_{n\cdot m}(a) + y_{n\cdot m}(a)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^{n\cdot m} = ((a+\sqrt{a^2-1})^n)^m =$$
$$= (x_n(a) + y_n(a)\sqrt{a^2-1})^m = \sum_{i=0}^{m} \binom{m}{i} \cdot x_n(a)^{m-i} y_n(a)^i (\sqrt{a^2-1})^i$$

which is the thesis isolating the coordinates in $\mathbb{Z}[\sqrt{a^2-1}]$, depending on the parity of indexes. □

The previous lemma shows the fundamental basic properties of (1.4), and since the aim of the system to describe Γ_x is to control the index of the solution, then 1.2.6 *vi.* suggests to impose the equation:

$$S = \begin{cases} \text{I} : x^2 - (a^2-1)y^2 = 1 \\ \text{II} : y \geq k \end{cases}$$

In particular, thanks to 1.2.4 equation I tells that $\exists i \in \mathbb{N}$ such that $x = x_i(a)$, $y = y_i(a)$, so now the point of the system is to try to impose the condition $i = k$ in a diophantine way.
The intuition beyond the reason of the choices in adding the next polynomial equations to this temporary system, is based on an elementary, namely to impose $i \equiv_d k$ for a certain module d such that $0 \leq i < d \ \wedge \ 0 \leq k < d$.

The next theorem (1.2.9) is the core to impose a such equivalence relation between indeces of solutions of Pell's equations of the form of (1.4), but first two lemmas are needed:

Lemma 1.2.7. *$x_{2n\pm i}(a) \equiv_{x_n(a)} -x_i(a)$, in particular $x_{4n\pm i}(a) \equiv_{x_n(a)} x_i(a)$.*

Proof. By 1.2.6 *i.* and *ii.* it follows:

$$x_{2n\pm i}(a) = x_n(a) \cdot x_{n\pm i}(a) + y_n(a) \cdot y_{n\pm i}(a) \cdot (a^2-1) \equiv_{x_n(a)}$$
$$\equiv_{x_n(a)} y_n(a) \cdot y_{n\pm i}(a) \cdot (a^2-1) = y_n(a) \cdot (x_i(a) \cdot y_n(a) \pm x_n(a) \cdot y_i(a)) \cdot (a^2-1) \equiv_{x_n(a)}$$
$$\equiv_{x_n(a)} x_i(a) \cdot y_n(a)^2 \cdot (a^2-1) = x_i(a) \cdot (x_n(a)^2 - 1) \equiv_{x_n(a)} -x_i(a)$$

with the last equality given by Pell's equation: $(a^2-1) \cdot y_n(a)^2 = x_n(a)^2 - 1$. Finally:

$$x_{4n\pm i}(a) \equiv_{x_n(a)} -x_{2n\pm i}(a) \equiv_{x_n(a)} -x_i(a)$$

□

Lemma 1.2.8. $x_i(a) \equiv_{x_n(a)} x_j(a) \ \wedge \ 0 \leq i \leq j \leq 2n \ \wedge \ n > 0 \implies i = j \ \vee \ a = 2, \ n = 1, \ i = 0, \ j = 2.$

Proof. Suppose $x_n(a) \equiv_2 1$, let $q := (x_n(a) - 1)/2$, then a set of mutually incongruent residues modulo $x_n(a)$ is given by $-q, -q+1, \ldots, 0, \ldots, q-1, q$, but then $1 = x_0(a) < x_1(a) < \cdots < x_{n-1}(a) \leq \lfloor x_n(a)/a \rfloor \leq \lfloor x_n(a)/2 \rfloor = q$, but one has the congruences $x_{2n-i}(a) \equiv_{x_n(a)} -x_i(a)$, so that in particular it holds: $x_{2n}(a) \equiv_{x_n(a)} -x_0(a), \ldots, x_{n+1}(a) = x_{2n-(n-1)}(a) \equiv_{x_n(a)} -x_{n-1}(a)$, so that in this case the claim is clear.
If $x_n(a) \equiv_2 0$, let $q := x_n(a)/2$, then a set of mutually incongruent residues modulo $x_n(a)$ is given by $-q+1, -q+2, \ldots, 0, \ldots, q-1, q$, so that the same reasoning as before holds, except if $x_{n-1}(a) = q \wedge x_{n+1}(a) \equiv_{x_n(a)} -q \equiv_{x_n(a)} q$. But, in this case $x_n(a) = 2x_{n-1}(a)$, and by $x_n(a) = ax_{n-1}(a) + y_{n-1}(a) \cdot (a^2 - 1)$ it forces $a = 2 \wedge y_{n-1}(a) = 0$, so that $n = 1$, then $j = n+1 = 2$, $i = n-1 = 0$, which is the thesis. □

Theorem 1.2.9. $0 < i \leq n : x_i(a) \equiv_{x_n(a)} x_j(a) \implies j \equiv_{4n} \pm i.$

Proof. Writing $j = 4nq + k$ with $0 \leq k < 4n$, from 1.2.7 then $x_j(a) \equiv_{x_n(a)} x_k(a)$.
Suppose now $0 \leq k \leq 2n$, then by 1.2.8 one has $i = k$ or $k = 0$ and $i = 2 > 1 = n$ which is impossible.
Finally if $2n < k < 4n$, then $0 \leq m := 4n - k < 2n$ so that by 1.2.7 $x_j(a) \equiv_{x_n(a)} x_k(a) \equiv_{x_n(a)} x_m(a)$, to which case the previous reasoning can be applied. □

At this point one has the ingredient for trying to upgrade the system of equation for describing the graph of the function in 1.2.5. Indeed, to use 1.2.9 one needs at least three Pell's equations of the form (1.4) and such that the hypothesis of the theorem is satified, so the enriched system now is:

$$S = \begin{cases} \text{I} : x^2 - (a^2 - 1)y^2 = 1 \\ \text{II} : y \geq k \\ \text{III} : u^2 - (a^2 - 1)v^2 = 1 \\ \text{IV} : s^2 - (a^2 - 1)t^2 = 1 \\ \text{V} : s \equiv_u x \end{cases}$$

In particular, this system tells us the following:

$$\exists i, j, n \in \mathbb{N} : x = x_i(a), \ y = y_i(a), \ u = x_n(a), \ v = y_n(a), \ s = x_j(a), \ t = y_j(a)$$

$$s \equiv_u x \iff x_i(a) \equiv_{x_n(a)} x_j(a) \implies j \equiv_{4n} \pm i \ (1.2.9).$$

At this point, one could try to impose $k \equiv_{4n} j$ and $k \leq n \ \wedge \ i \leq n$, so that $k = i$, but the definition of n is random, so there's not an immediate

diophantine way to avoid this difficulty.
But, we already have $k \leq y$ by II and $i \leq y_i(a) = y$ by 1.2.6 *vi.*, in particulare for the second condition is sufficient $y \leq n$.
A suggestion to how impose a similar condition in a diophantine way is suggested by 1.2.6 *vii.* and *viii.*, which can be formalized as in the following lemma:

Lemma 1.2.10. *The following hold:*

i. $y_n(a) \mid y_t(a) \iff n \mid t$.

ii. $y_n(a)^2 \mid y_t(a) \iff y_n(a) \mid t$.

Proof. *i.* ($\Leftarrow$) by 1.2.6 *vi.*.
($\Rightarrow$): by absurd suppose $y_n(a) \mid y_t(a)$ and $n \nmid t$ so that one can write $t = qn+r$ with $0 < r < n$, then by 1.2.6 *ii.*:

$$y_n(a) \mid y_t(a) = y_{qn+r}(a) = x_{qn}(a) \cdot y_r(a) + x_r(a) \cdot y_{qn}(a)$$

But one knows by the previous implication that $y_n(a) \mid y_{qn}(a)$, so that it follows that $y_n(a) \mid x_{qn}(a) \cdot y_r(a)$, which is a contradiction: indeed $y_n(a) \mid y_{qn}(a) \wedge (x_{qn}(a), y_{qn}(a)) = 1 \implies (x_{qn}(a), y_n(a)) = 1$ and also $0 < r < n \implies 0 < y_r(a) < y_n(a) \implies y_n(a) \nmid y_r(a)$, so that $y_n(a) \nmid x_{qn}(a) \cdot y_r(a)$.

ii. By 1.2.6 *vi.* it holds $y_{n \cdot m}(a) \equiv_{y_n(a)^3} m \cdot x_n(a)^{m-1} \cdot y_n(a)$, in particular:
($\Leftarrow$) $y_n(a) \mid t \implies \exists m \in \mathbb{N} : t = y_n(a) \cdot m$, in particular by what remarked:

$$y_t(a) = y_{y_n(a) \cdot m}(a) \equiv_{y_n(a)^3} t \cdot x_n(a)^{t-1} \cdot y_n(a) = m \cdot x_n(a)^{t-1} \cdot y_n(a)^2$$

which means $y_t(a) \equiv_{y_n(a)^2} 0$.
($\Rightarrow$) $y_n(a)^2 \mid y_t(a) \implies y_n(a) \mid y_t(a) \implies n \mid t$ by *i.*, so that $\exists m \in \mathbb{N} : t = n \cdot m$, in particular by what remarked:

$$0 \equiv_{y_n(a)^2} y_t(a) = y_{n \cdot m}(a) \equiv_{y_n(a)^3} m \cdot x_n(a)^{m-1} \cdot y_n(a)$$

which means $y_n(a)^2 \mid m \cdot x_n(a)^{m-1} \cdot y_n(a)$, equivalently $y_n(a) \mid m \cdot x_n(a)^{m-1}$, but $(x_n(a), y_n(a)) = 1$, so that $y_n(a) \mid m$, and by $t = n \cdot m$ then $y_n(a) \mid t$. □

Remark 1.2.11. Notice that 1.2.10 *ii.* gives the analogue of the property (1.2) of Fibonacci's numbers to the sequence $\{y_n(a) : n \in \mathbb{N}\}$, property that will play a key role in proving 1.2.5: indeed, as already underlined, one has to control in a diophantine way the index of a solution of the special Pell's equation.

Thanks to this remark and the previous lemma, a suggestion to translate our two conditions $k \equiv_{4n} j$ and $k \leq n \ \wedge \ i \leq n$ is just imposing $y \mid n$, so that of course $y \leq n$ which was remarked to be sufficient for the second condition, and the first now can be expressed in an easier way which makes no differences thanks to the stronger bounds $k \leq y \ \wedge \ i \leq y$, namely $k \equiv_{4y} j$. So to express the first of this two new conditions, namely $y \mid n$, thanks to 1.2.10 *ii.* one can express this equivalently with $y^2 = y_i(a)^2 \mid y_n(a) = v$ which is now a diophantine condition.
In particular the system should look like:

$$S = \begin{cases} \text{I} : x^2 - (a^2-1)y^2 = 1 \\ \text{II} : y \geq k \\ \text{III} : u^2 - (a^2-1)v^2 = 1 \\ \text{IV} : s^2 - (a^2-1)t^2 = 1 \\ \text{V} : s \equiv_u x \\ \text{VI} : y^2 \mid v \end{cases}$$

The second condition is $k \equiv_{4y} j$, but again there's the same problem as before: the index j exists, but has no explicit diophantine definition.
To avoid this problem, there's a trivial property that is suggested by 1.2.6 *vi.* remarked in the following lemma:

Lemma 1.2.12. $y_j(a) \equiv_{a-1} j$

Proof. $n = 0, 1$ is an equality: $y_0(a) = 0$, $y_1(a) = 1$, then for $j > 1$ by induction with 1.2.6 *vi.*:

$$y_{j+1}(a) = 2a \cdot y_j(a) - y_{j-1}(a) \equiv_{a-1} 2y_j(a) - y_{j-1}(a) \equiv_{a-1} 2j - (j-1) = j+1$$

□

In particular, the conditions $k \equiv_{4y} j$ can be expressed thanks to 1.2.12 to the diophantine conditions $k \equiv_{4y} y_j(a) = t$ and $4y \mid a-1$, so that finally a candidate for the final system is clear:

$$S = \begin{cases} \text{I} : x^2 - (a^2-1)y^2 = 1 \\ \text{II} : y \geq k \\ \text{III} : u^2 - (a^2-1)v^2 = 1 \\ \text{IV} : s^2 - (a^2-1)t^2 = 1 \\ \text{V} : s \equiv_u x \\ \text{VI} : y^2 \mid v \\ \text{VII} : k \equiv_{4y} t \\ \text{VIII} : 4y \mid a-1 \end{cases}$$

Recollecting everything done till this point, one can state the following theorem, which is pretty close to the claim of 1.2.5:

Theorem 1.2.13. *Let a, k, x, y, u, v, s, t such that it is satisfied the system:*

$$S = \begin{cases} I : x^2 - (a^2-1)y^2 = 1 \\ II : y \geq k \\ III : u^2 - (a^2-1)v^2 = 1 \\ IV : s^2 - (a^2-1)t^2 = 1 \\ V : s \equiv_u x \\ VI : y^2 \mid v \\ VII : k \equiv_{4y} t \\ VIII : 4y \mid a-1 \end{cases}$$

Then it must be $x = x(a,k)$.

Proof. By 1.2.4 and equations I,III,IV $\exists i, j, n \in \mathbb{N}$ such that $x = x_i(a),\ y = y_i(a)$,
$u = x_n(a),\ v = y_n(a),\ s = x_j(a),\ t = y_j(a)$.
In particular, equation V can be read as $x_i(a) \equiv_{x_n(a)} x_j(a) \implies j \equiv_{4n} \pm i$ by 1.2.9, but equation VI is telling $y^2 = y_i(a)^2 \mid y_n(a)^2 = v^2 \iff y \mid n$ by 1.2.10 *ii.*, so that $j \equiv_{4y} \pm i$.
Applying 1.2.12 one has $t \equiv_{a-1} j$ which combined with equation VIII leads to $t \equiv_{4y} j$, and then equation VII gives $k \equiv_{4y} t \equiv_{4y} j$.
In particular, by these two observations one has $k \equiv_{4y} \pm i$, but by 1.2.6 *vi.* one has $i \leq y_i(a) = y$ and by II $k \leq y$, so it must happen $k = i$, equivalently $x = x_k(a)$ which is the thesis. □

Remark 1.2.14. 1.2.13 tells that:

$$\Gamma_x \subseteq \{(x,k,a) \in \mathbb{N}^3 : \exists (y_1, \dots, y_m) \in \mathbb{N}^m : P(x,k,a,y_1,\dots,y_m) = 0\}$$

with $P(x,k,a,y_1,\dots,y_m)$ obtained by translating diophantinely the system S of the statement:

$$S = \begin{cases} I : x^2 - (a^2-1)y^2 = 1 \\ II : y = k + m \\ III : u^2 - (a^2-1)v^2 = 1 \\ IV : s^2 - (a^2-1)t^2 = 1 \\ V : s = qu + x \\ VI : v = r \cdot y^2 \\ VII : t = 4yd + k \\ VIII : a - 1 = 4y \cdot f \end{cases}$$

In particular $P(y,u,v,s,t,m,q,r,d,f) = (x^2 - (a^2-1)y^2 - 1)^2 + (y - k - m)^2 + (u^2 - (a^2-1)v^2 - 1)^2 + (s^2 - (a^2-1)t^2 - 1)^2 + (s - qu - x)^2 + (v -$

$r \cdot y^2)^2 + (t - 4yd - k)^2 + (a - 1 - 4y \cdot f)^2$.
Clearly, to obtain 1.2.5 is sufficient to prove the other inclusion, but, given $(x, k, a) \in \mathbb{N}^3$, trying to construct a solution to the system seems not natural cause to satisfy I $y = y_k(a)$ is forced by $x = x_k(a)$, but one still needs $4y \mid a - 1$, which might not happen since they are now both fixed.
Since the role of equation VIII is passing from the congruence of 1.2.12 $t \equiv_{a-1} j$ to $t \equiv_{4y} j$, then one can try to replace the variable a in VIII with a free variable that preserves this property, namely b satisfying $b \equiv_{4y} 1$, but in order to obtain $t \equiv_{4y} j$, one now needs $t \equiv_{b-1} j$, so that it is needed to change the system:

$$S = \begin{cases} \text{I} : x^2 - (a^2 - 1)y^2 = 1 \\ \text{II} : y \geq k \\ \text{III} : u^2 - (a^2 - 1)v^2 = 1 \\ \text{IV} : s^2 - (b^2 - 1)t^2 = 1 \\ \text{V} : s \equiv_u x \\ \text{VI} : y^2 \mid v \\ \text{VII} : k \equiv_{4y} t \\ \text{VIII} : 4y \mid b - 1 \end{cases}$$

The only problem in the way back of 1.2.13 is that it was used $s \equiv_u x$ as $x_i(a) \equiv_{x_n(a)} x_j(a)$, which now will be $x_i(a) \equiv_{x_n(a)} x_j(b)$, so to be able to use 1.2.12 one needs to check that choosing b such that $b \equiv_c a$ for a certain c, preserves the congruences also for the solutions, which is shown by the next lemma:

Lemma 1.2.15. $a \equiv_c b \implies \forall n \in \mathbb{N} : x_n(a) \equiv_c x_n(b) \ \wedge \ y_n(a) \equiv_c y_n(b)$

Proof. Proceeding by induction, for $n = 0, 1$:

$$x_0(a) = 1 = x_0(b), \ x_1(a) = a \equiv_c b = x_1(b)$$

$$y_0(a) = 0 = y_0(b), \ y_1(a) = 1 = y_1(b)$$

Then for $n > 1$ using 1.2.6 *iii.* & *iv.*:

$$x_{n+1}(a) = 2a \cdot x_n(a) - x_{n-1}(a) \equiv_c 2b \cdot x_n(b) - x_{n-1}(b) = x_{n+1}(b)$$

$$y_{n+1}(a) = 2a \cdot y_n(a) - y_{n-1}(a) \equiv_c 2b \cdot y_n(b) - y_{n-1}(b) = y_{n+1}(b)$$

□

In particular, now one has to choose a suitable c such that it is valid $x_i(a) \equiv_{x_n(a)} x_j(a) \equiv_c x_j(b)$, and it is then natural to impose $c = x_n(a) = u$.
At last, one can notice that to satisfy equation VIII it seems pretty convenient to have $(u, 4y) = 1$ in order to apply the Chinese remainder theorem.
But one has $y \mid v \ \wedge (v, u) = 1 \implies (y, u) = 1$, so one just needs $(2, u) = 1$, which is something that can be imposed thanks to the next remark:

Remark 1.2.16. By 1.2.6 *iv.* one has $y_{n+1} \equiv_2 y_{n-1}$, so that by the base cases $y_0 \equiv_2 0 \ \wedge \ y_1 \equiv_2 1$ inductively: $\forall n \in \mathbb{N} : y_{2n} \equiv_2 0 \ \wedge \ y_{2n+1} \equiv_2 1$.
In particular, by $(x_n(a), y_n(a)) = 1$: $\forall n \in \mathbb{N} : x_{2n} \equiv_2 1 \ \wedge \ x_{2n+1} \equiv_2 0$.

Theorem 1.2.17. *Let* $(x, k, a) \in \mathbb{N}^3$*:* $x = x_k(a) \iff S$ *can be satisfied in* $\mathbb{N}$*, where*

$$S = \begin{cases} I : x^2 - (a^2 - 1)y^2 = 1 \\ II : y \geq k \\ III : u^2 - (a^2 - 1)v^2 = 1 \\ IV : s^2 - (b^2 - 1)t^2 = 1 \\ V : s \equiv_u x \\ VI : y^2 \mid v \\ VII : k \equiv_{4y} t \\ VIII : b \equiv_{4y} 1 \ \wedge \ b \equiv_u a \end{cases}$$

Proof. ($\Longleftarrow$): proceeding as in 1.2.13, by 1.2.4 and equations I,III,IV $\exists i, j, n \in \mathbb{N}$ such that $x = x_i(a), \ y = y_i(a), \ u = x_n(a), \ v = y_n(a), \ s = x_j(a), \ t = y_j(a)$.
In particular, equation V can be read as $x_i(a) \equiv_{x_n(a)} x_j(b)$, but by 1.2.15 and equation VIII one has $x_j(b) \equiv_{x_n(a)} x_j(a)$, so $x_i(a) \equiv_{x_n(a)} x_j(a) \implies j \equiv_{4n} \pm i$ by 1.2.9.
Furthermore, equation VI is telling $y^2 = y_i(a)^2 \mid y_n(a)^2 = v^2 \iff y \mid n$ by 1.2.10 *ii.*, so that $j \equiv_{4y} \pm i$.
Applying 1.2.12 one has $t \equiv_{b-1} j$ which combined with equation VIII leads to $t \equiv_{4y} j$, and then equation VII gives $k \equiv_{4y} t \equiv_{4y} j$.
In particular, by these two observations one has $k \equiv_{4y} \pm i$, but by 1.2.6 *vi.* one has $i \leq y_i(a) = y$ and by II $k \leq y$, so it must happen $k = i$, equivalently $x = x_k(a)$ which is the claim.
($\Longrightarrow$): defining $y = y_k(a)$, I is satisfied by 1.2.4 having $x = x_k(a)$ by hypothesis, but also II thanks to 1.2.6 *vi.*.
Setting then $n = 2ky, \ u = x_n(a), \ v = y_n(a)$, III is satisfied, but by 1.2.10 *ii.* since $y = y_k(a) \mid n$, then $y^2 \mid y_n(a) = v$ so that $\exists r \in \mathbb{N}$ such that $v = r \cdot y^2$ satisfying VI.
Furthermore, $y \mid v \ \wedge (v, u) = 1 \implies (y, u) = 1$ and by 1.2.16 $(u, 2) = 1$, so that $(u, 4y) = 1$ and one can apply the Chinese Remainder Theorem to find b such that $b \equiv_u a \ \wedge \ b \equiv_{4y} 1$, so that VIII is satisfied.
Then, setting $s = x_k(b), \ t = y_k(b)$, IV is satisfied, and by $b \equiv_u a$ one has $s = x_k(b) \equiv_u x_k(a) = x$ thanks to 1.2.15, so that also V is satisfied.
Finally, by 1.2.12 one has $t \equiv_{b-1} k$, but VIII holds so $b \equiv 4y1$, in particular one has $t \equiv_{4y} k$ which is VII and the system is satisfied. □

In particular, in a similar procedure such as in 1.2.14, one can explicitly

construct the polynomial to describe the graph of the function, $x(k,a) = x_k(a)$, which proves 1.2.5.

1.3 Fibonacci's Diophantinity and Exponential

In this subsection the goal is to prove 1.1.6 using 1.2.5 proved in the previous section, and the technique will be in substance trivial, imposing for a certain h:

$$n^k \equiv_h m \ \wedge \ n^k < h \ \wedge \ m < h. \tag{1.5}$$

For this purpose one can notice that, working in $\mathbb{Z}[\sqrt{a^2-1}]$ and so defining $\epsilon_a = a + \sqrt{a^2-1}$, 1.2.5 could be interpreted as

$$\textit{The function } \epsilon : \mathbb{N} \times \mathbb{N}_{>1} \to \mathbb{Z}[\sqrt{a^2-1}] \textit{ s. t. } \epsilon(k,a) = {\epsilon_a}^k \textit{ is diophantine.}$$

In particular, for reaching 1.1.6 one has to replace in a diophantine way ϵ_a with a generic $n \in \mathbb{N}$, and for this aim one has to build a system of equations which will then include the ones (I-VIII) of the previous section.
Furthermore, supposing one can replace n in the reasoning then:

$$n^k = {\epsilon_a}^k = x_k(a) + y_k(a) \cdot \sqrt{a^2-1} \equiv_{\epsilon_a - n} x_k(a) + y_k(a) \cdot (n-a).$$

And noticing $N_{\mathbb{Q}(\sqrt{a^2-1})/Q}(\epsilon_a - n) = 2an - n^2 - 1$, applying the norm to the equivalence one should reach the next result:

Lemma 1.3.1. $x_k(a) + y_k(a) \cdot (n-a) \equiv_{2an-n^2-1} n^k$.

Proof. Trivial induction using 1.2.6 *iii.* & *iv.* □

Thanks to 1.3.1, one can choose in 1.5 the natural $h = 2an - n^2 - 1$, so that the system will need to include the condition $x_k(a) + y_k(a) \cdot (n-a) \equiv_{2an-n^2-1} m$, equivalently:

$$\text{IX} : (x + y(n-a) - m)^2 = f^2 \cdot (2an - n^2 - 1)^2$$

But then one has to try to impose $m < 2an - n^2 - 1$ & $n^k < 2an - n^2 - 1$, but the first one is itself diophantine, so:

$$\text{X} : m < 2an - n^2 - 1$$

For the second condition $n^k < 2an - n^2 - 1$ one has to notice that in the updated system (I-X) one has as free variables just a, k, but k needs to

be generic in this new system so as for n, while the choice of a can be manipulated in such a way to obtain the desired bound.
In particular, thanks to 1.2.6 *v.* & *vi.* one can try to impose:

$$a^2 - (w^2 - 1)c^2 = 1$$

So that, it holds $a = x_j(w) \geq w^j$.
But it was seen a way to bound the index: indeed, by 1.2.12 one has $c = y_j \equiv_{w-1} j$, so that imposing the diophantine condition $w - 1 \mid c$, it must happen $w - 1 \mid j$, in particular $w - 1 \leq j$, so that the bound would be:

$$a = x_j(w) \geq w^j \geq w^{w-1}$$

Then one can conclude imposing the diophantine conditions $w > n$ & $w-1 \geq k$, so that we have obtained the bound $a \geq n^k$, which reaches to the claimed bound thanks to next lemma:

Lemma 1.3.2. $a > n^k \implies 2an - n^2 - 1 > n^k$

Proof. Defining $g(n) = 2an - n^2 - 1$, one can notice that it is an increasing function in the region $a > n^k \geq n$ by $g'(n) = 2a - 2n > 0$, then since $g(1) = 2a - 2 \geq a$, then the claim follows by monotony being $g(n) \geq a \ \forall n : a > n^k$. □

Recollecting all the previous ideas, finally the more precise statement of 1.1.6 is reachable:

Theorem 1.3.3. *Let* $(m, n, k) \in \mathbb{N}^3$*:* $m = n^k \iff S$ *can be satisfied in* $\mathbb{N}$*, where*

$$S = \begin{cases} I : x^2 - (a^2 - 1)y^2 = 1 \\ II : y \geq k \\ III : u^2 - (a^2 - 1)v^2 = 1 \\ IV : s^2 - (b^2 - 1)t^2 = 1 \\ V : s \equiv_u x \\ VI : y^2 \mid v \\ VII : k \equiv_{4y} t \\ VIII : b \equiv_{4y} 1 \ \wedge \ b \equiv_u a \\ IX : (x + y(n - a) - m)^2 = f^2 \cdot (2an - n^2 - 1)^2 \\ X : m < 2an - n^2 - 1 \\ XI : a^2 - (w^2 - 1) \cdot (w - 1)^2 \cdot z^2 = 1 \\ XII : w > n \ \wedge \ w - 1 \geq k \end{cases}$$

Proof. ($\Longleftarrow$): by the solvability of (I-VIII) and thanks to 1.2.13 it must happen that $x = x_k(a)$ & $y = y_k(a)$.
By IX and 1.3.1:

$$m \equiv_{2an-n^2-1} x + y \cdot (n-a) = x_k(a) + y_k(a) \cdot (n-a) \equiv_{2an-n^2-1} n^k$$

Also, X implies $m < 2an - n^2 - 1$, so that for the thesis is sufficient to check $n^k < 2an - n^2 - 1$.
But as seen before, from XI and 1.2.6 *v.* $a = x_j(w) \geq w^j$, and by 1.2.12 one has $0 \equiv_{w-1} (w-1)z = y_j \equiv_{w-1} j$, which means $w - 1 \mid j$, in particular $w - 1 \leq j$, so that finally thanks to XII the bound would be:

$$a = x_j(w) \geq w^j \geq w^{w-1} > n^k$$

and by 1.3.2 this implies $2an-n^2-1 > n^k$, which combined with $2an-n^2-1 > m$ and $m \equiv_{2an-n^2-1} n^k$ necessarily leads to $m = n^k$ as desired.
($\Longrightarrow$): given $(m, n, k) \in \mathbb{N}^3$ such that $m = n^k$, one can choose $w > n$ and $w > k$ to satisfy XII, then define $a = x_{w-1}(w)$ and $c = y_{w-1}(w)$, so that by 1.2.12 $c = y_{w-1}(w) \equiv_{w-1} w - 1 \equiv_{w-1} 0$, so that one can also define z such that $c = (w-1) \cdot z$ to satisfy XI.
In particular, with the same reasoning as in the previous implication one obtains again $a > n^k$, which by 1.3.2 implies $2an - n^2 - 1 > n^k = m$ to obtain X.
Then set $x = x_k(a)$ and $y = y_k(a)$, by 1.3.1 one has:

$$x + y \cdot (n-a) = x_k(a) + y_k(a) \cdot (n-a) \equiv_{2an-n^2-1} n^k = m$$

so that one can find an f to satisfy IX.
Finally, having set $x = x_k(a)$, I-VIII are satisfiable by 1.2.13. □

1.4 Binomial and Factorial are Diophantine

The result reached in the previous section, 1.1.6, has the task to prove that as much sets as possible are diophantine, as shown later in
To see the power of 1.1.6, the aim is now to show that the binomial function $((n,k) \mapsto \binom{n}{k})$ and the factorial function $(n \mapsto n!)$ are diophantine.

Remark 1.4.1. The floor function is diophantine:

$$c = \left\lfloor \frac{a}{b} \right\rfloor \iff c \cdot b \leq a < (c+1) \cdot b$$

Remark 1.4.2. For any $u > 2^n$

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor = \sum_{i=k}^{n} \binom{n}{i} u^{i-k} \equiv_u \binom{n}{k}$$

Indeed, $\frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} \binom{n}{i} u^{i-k}$, but by the binomial theorem:

$$\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} \leq u^{-1} \cdot \sum_{i=0}^{k-1} \binom{n}{i} \leq u^{-1} \cdot 2^n < 1$$

.

Theorem 1.4.3. *$b(n,k) = \binom{n}{k}$ is diophantine.*

Proof. One has:

$$m = \binom{n}{k} \iff \exists u : u > 2^n \ \wedge \ m < u \ \wedge \ \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv_u m$$

Indeed, $u > 2^n$ is a diophantine expression by 1.1.6, so as $m < u$, but also $\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv_u m$ is diophantine thanks to 1.4.1.
By the binomial theorem it implies $u > 2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \geq \binom{n}{k} \ \forall 1 \leq k \leq n$, but also $m < u$, and by 1.4.2 $\binom{n}{k} \equiv_u \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv_u m$, so it must be $m = \binom{n}{k}$.
For the other direction just $u = 2^n + 1$ is sufficient. □

Lemma 1.4.4. $r > (2n)^{n+1} \implies n! = \left\lfloor \frac{r^n}{\binom{r}{n}} \right\rfloor$

Proof.

$$\frac{r^n}{\binom{r}{n}} = \frac{r^n \cdot n!}{r(r-1)\cdots(r-n+1)} = n! \cdot \frac{1}{(1-\frac{1}{r})\cdots(1-\frac{n-1}{r})}$$

$$\implies n! \leq \frac{r^n}{\binom{r}{n}} \leq n! \cdot \left(1 - \frac{n}{r}\right)^{-n}$$

$$\left(1 - \frac{n}{r}\right)^{-1} = \sum_{k=0}^{+\infty} \left(\frac{n}{r}\right)^k \leq 1 + \frac{n}{r} \cdot \sum_{k=0}^{+\infty} 2^{-k} = 1 + \frac{2n}{r}$$

$$\left(1 + \frac{2n}{r}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \left(\frac{2n}{r}\right)^k < 1 + \frac{2n}{r} \cdot \sum_{k=1}^{n} \binom{n}{k} \leq 1 + \frac{2n}{r} \cdot 2^n$$

$$\implies \frac{r^n}{\binom{r}{n}} < n! + \frac{2n \cdot n! \cdot 2^n}{r} < n! + \frac{2n \cdot n^n \cdot 2^n}{r} = n! + \frac{(2n)^{n+1}}{r} < n! + 1$$

□

Theorem 1.4.5. *$f(n) = n!$ is diophantine.*

Proof. By 1.4.4:

$$m = n! \iff \exists a, b, r : m = \left\lfloor \frac{a}{b} \right\rfloor \ \wedge \ a = r^n \ \wedge \ b = \binom{r}{n} \ \wedge \ r > (2n)^{n+1}$$

which are all diophantine expression thanks to 1.4.2 & 1.1.6 & 1.4.3. □

Corollary 1.4.6. *$\mathbb{P} = \{p \in \mathbb{N} : p \text{ prime}\}$ is diophantine.*

Proof. By Wilson's Theorem $\mathbb{P} = \{n \in \mathbb{N} : (n-1)! \equiv_n -1\}$ which is a diophantine expression thanks to 1.4.5. □

1.5 Recursive Functions

In last part of the chapter, using the powerful tool obtained in the previous sections, namely the diophantinity of the exponential function, the goal is to prove that the set of diophantine sets (or functions) coincides with the one of recursive sets (or functions respectively), which was once known as Davis' Conjecture, thanks to which it is pretty clear the undecidability of Hilberth's Tenth Problem.
First of all, the notion of *Recursive Function* will be developed, being fundamental during the whole discussion.

Definition 1.5.1. For $f, g \in Hom_{Set}(\mathbb{N}^{n+1}, \mathbb{N})$ define the *minimalization* of f and g as $h(x_1, \dots, x_n) = min_y(f(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, y))$ if defined everywhere.
For $f \in Hom_{Set}(\mathbb{N}^n, \mathbb{N})$ and $g \in Hom_{Set}(\mathbb{N}^{n+2}, \mathbb{N})$ define the *primitive recursion* of g based on f as

$$h(x_1, \dots, x_n, 1) = f(x_1, \dots, x_n)$$

$$h(x_1, \dots, x_n, t+1) = g(t, h(x_1, \dots, x_n, t), x_1, \dots, x_n)$$

For a subset $S \subseteq \bigcup_{n\in\mathbb{N}} Hom_{Set}(\mathbb{N}^n, \mathbb{N})$, it will be denoted $S = \overline{S}$ if S is closed under composition, minimalization and primitive recursion.
Defining few elementary functions:

$$c(x) = 1, \ s(x) = x + 1, \ \pi_i^n(x_1, \dots, x_n) = x_i$$

A *Recursive Function* is an element of the following set:

$$R = \bigcap_{S\in\mathcal{F}} S$$

$$\mathcal{F} = \{S \subseteq \bigcup_{n\in\mathbb{N}} Hom_{Set}(\mathbb{N}^n, \mathbb{N}) : c, s, \pi_i^n \in S \ \forall i, n \in \mathbb{N} \ \wedge \ S = \overline{S}\}$$

The main result of this first section is the following theorem:

Theorem 1.5.2. $f \in \bigcup_{n\in\mathbb{N}} Hom_{Set}(\mathbb{N}^n, \mathbb{N}) : f$ *diophantine* $\iff$ *recursive.*

Two easy but useful lemma to start investigating recursive functions:

Lemma 1.5.3. $P(x_1, \dots, x_n) \in \mathbb{N}[x_1, \dots, x_n]$ *is recursive.*

Proof. $f_1(x, y) = x + y$ is recursive thanks to primitive recursion applied to the elementary functions:

$$f_1(x, 1) = s(x),\ f_1(x, y + 1) = g(y, f_1(x, y), x)\ s.t.\ g = s \circ \pi_2^3$$

$f_2(x, y) = x \cdot y$ is recursive thanks to primitive recursion applied to the elementary functions and to f_1:

$$f_2(x, 1) = \pi_1^1(x),\ f_2(x, y + 1) = g(y, f_2(x, y), x)\ s.t.\ g = f_1 \circ (\pi_2^3, \pi_3^3)$$

Finally, $h_k(x) = k$ constant function is recursive thanks to induction and f_1:

$$h_1(x) = c(x)\ recursive,\ h_{k+1}(x) = f_1(h_k(x), c(x))$$

The claim follows from finitely many compositions of f_1, f_2 and $h_k : k \in \mathbb{N}$. □

Lemma 1.5.4. *For $a, b \in \mathbb{N}$, define by Euclid's Algorithm $q, r : a = qb + r$ with $0 \le r < b$, then the functions $q(a, b) = q$ and $r(a, b) = r$ are recursive.*

Proof. Defining the recursive functions $Z(0) = 1$, $Z(x + 1) = 0$, $pred(0) = 0$, $pred(x+1) = x = \pi_1^1(x)$ and $sub(x, 0) = x$, $sub(x, y+1) = pred(sub(x, y))$, then one can define as a recursive function

$$\Theta(x, y) = \begin{cases} 1\ if\ x \le y \\ 0\ if\ y < x \end{cases}$$

$$\Theta(x, 0) = Z(x),\ \Theta(x, y + 1) = \Theta(pred(x), y)$$

In particular, $q(a, b) = min_q(\Theta(((q + 1)b), a) = 0)$ recursive.
Finally, $r(a, b) = sub(a, q(a, b) \cdot b)$. □

For the easier implication ($\Longrightarrow$) of 1.5.2 the key ingredient will be the *Sequence Number Theorem*, but first one needs the following result called *Cantor's Pairing Function Theorem*:

Theorem 1.5.5. $\exists P \in Hom_{Set}(\mathbb{N}^2, \mathbb{N}), L, R \in Hom_{Set}(\mathbb{N}, \mathbb{N})$ *diophantine and recursive functions such that:*

- $\forall x, y \in \mathbb{N} : L(P(x,y)) = x \ \wedge \ R(P(x,y)) = y.$
- $\forall z \in \mathbb{N} : P(L(z), R(z)) = z \ \wedge \ L(z) \leq z \ \wedge \ R(z) \leq z.$

Proof. Let

$$T(n) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

which is an increasing function in the variable n, so that $\forall z \in \mathbb{N}^+ \exists! n_z \in \mathbb{N} : T(n_z) < z \leq T(n_z + 1)$, so there is a unique representation of positive integers as $z = T(n_z) + y_z, \ 0 < y_z \leq n_z + 1$, equivalently there is a unique representation $z = T(x_z + y_z - 2) + y_z$ defining $x_z = n_z - y_z + 2$, so that one can define the desired functions:

$$L(z) = x_z, \quad R(z) = y_z, \quad P(x,y) = T(x+y-2) + y$$

which trivially satisfy the desired conditions.
Finally, being P a polynomial with positive coefficients, it is then recursive by 1.5.3, for recursivity of R and L:

$$R(z) = min_y \left(\prod_{x=0}^{z} |P(x,y) - z| = 0 \right)$$

$$L(z) = min_x \left(\prod_{y=0}^{z} |P(x,y) - z| = 0 \right)$$

□

Finally one is able to prove the *Sequence Number Theorem*:

Theorem 1.5.6. *$\exists S \in Hom_{Set}(\mathbb{N}^2, \mathbb{N})$ diophantine and recursive function such that:*

- $\forall i \in \mathbb{N} : S(i,u) \leq u$
- $\forall n \in \mathbb{N}, \forall (a_1, \ldots, a_n) \in \mathbb{N}^n, \exists u \in \mathbb{N} \ s.t. \ \forall i \in \{1, \ldots, n\} : S(i,u) = a_i$

Proof. By Euclid's Algorithm one can define $q(i,u), \ S(i,u)$ such that

$$L(u) = q(i,u)[1 + iR(u)] + S(i,u)$$

so that one has the first property $S(i,u) \leq L(u) \leq u$ by 1.5.5.
The diophantinity of $S(i,u)$ is clear by $\Gamma_S = \{(w,i,n) \in \mathbb{N}^3 \ s.t. \ \exists (x,y,z,v) \in \mathbb{N}^4 : Q(u,x,y) = H(x,w,z,i,y) = K(i,y,w,v) = 0\}$, with $Q(u,x,y) =$

$2u-(x+y-2)(x+y-1)-2y$, $H(x,w,z,i,y)=x-w-z(1+iy)$ and $K(i,y,w,v)=1-iy-w-v+1$.
Finally, for $a_1,\dots,a_n\in\mathbb{N}^+$, choosing $y\geq max\{a_i : i\in\{1,\dots,n\}\}$ such that $k\mid y\ \forall k\in\{1,\dots,n\}$, so that $\{1+ky : k\in\{1,\dots,n\}\}$ are pairwise coprime numbers: indeed if $d\mid 1+iy\ \wedge\ d\mid 1+jy$ for $1\leq i<j\leq n$, then $d\mid[j(1+iy)-i(1+jy)]=j-i$, in particular $d\leq n$, so that $d\mid y$, but by hypothesis also $d\mid 1+iy$, so that $d=1$.
In particular, by the Chinese Remainder Theorem $\exists x\in\mathbb{N} : x\equiv_{1+iy} a_i\ \forall i\in\{1,\dots,n\}$, so choosing $u=P(x,y)$, one has $x=L(u),\ y=R(u)$, so that $L(u)\equiv_{1+iR(u)} a_i$ and by definition it follows $S(i,u)=a_i$.
Finally, S is recursive thanks to 1.5.4 being the remainder of recursive functions. □

Thanks to this result, it is now possible to prove the easier implication ($\Longrightarrow$) of 1.5.2:

Proof. Let $P(x_1,\dots,x_n,y,t_1,\dots,t_m)$ the polynomial that vanishes for a certain $(t_1,\dots,t_m)\in\mathbb{N}^m\iff y=f(x_1,\dots,x_n)$, being f diophantine.
Then, one may express this vanishing as an equality between polynomials with non negative coefficients:

$$Q(x_1,\dots,x_n,y,t_1,\dots,t_m)=R(x_1,\dots,x_n,y,t_1,\dots,t_m)$$

By 1.5.6, one can codify for a certain $u\in\mathbb{N}$ the sequence $y=S(1,u),t_i=S(i+1,u) : 1\leq i\leq m$, so that:

$$f(x_1,\dots,x_n)=S(1,min_u(Q(x_1,\dots,x_n,S(1,u),S(2,u),\dots,S(m+1,u)=$$

$$=R(x_1,\dots,x_n,S(1,u),S(2,u),\dots,S(m+1,u))))$$

□

1.6 Bounded Quantifiers

In this section, the main goal is to prove a general theorem on diophantine sets which will be proved thanks to the diophantinity of the exponential and that will be used to prove the less trivial implication ($\Longleftarrow$) of 1.5.2.
First of all, the statement of the main result of the section:

Theorem 1.6.1. *$\forall P\in\mathbb{N}[z_1,\dots,z_{n+m+2}]$ the following set is diophantine:*

$$S=\{(x_1,\dots,x_n)\in\mathbb{N}^n : (\forall k)_{\leq y}\exists(y_1,\dots,y_m) : P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)=0\}$$

The importance of this result can be seen in a simple example:

Example 1.6.2. $\mathbb{P} = \{p \in \mathbb{N} : p \text{ prime}\}$ is diophantine as corollary of Wilson's Theorem and the diophantinity of the factorial function as shown in 1.4.6, but one can see it immediately thanks to 1.6.1:

$$\mathbb{P} = \{x \in \mathbb{N} : x > 1 \wedge (\forall y, z)_{\leq x}[y \cdot z < x \vee y \cdot z > x \vee y = 1 \vee z = 1]\}$$

Using 1.6.1 it is now easy to see ($\Longleftarrow$) of 1.5.2:

Proof. Let D the set of diophantine functions, then clearly $c(x) = 1, s(x) = x + 1$, $\phi_i^n(x_1, \ldots, x_n) = x_i \in D$, so that it is sufficient to check $D = \overline{D}$ by minimality of recursive functions.
Composition: let $f(y_1, \ldots, y_m), g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)$ be diophantine functions, $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$ is diophantine cause finite intersections of diophantine sets are still diophantine.
Minimalization: let $h(x_1, \ldots, x_n) = min_y(f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y))$ for f, g diophantine functions, then:

$$y = h(x_1, \ldots, x_n) \iff \phi_1 \wedge \phi_2$$

where:

$$\phi_1 = \exists z : z = f(x_1, \ldots, x_n, y) \wedge z = g(x_1, \ldots, x_n, y)$$

$$\phi_2 = (\forall t)_{\leq y}(t = y \ \vee (\exists u, v : u = f(x_1, \ldots, x_n, t)$$

$$\wedge \ v = g(x_1, \ldots, x_n, t) \wedge (u < v \vee u > v)))$$

With ϕ_1 diophantine formula and ϕ_2 diophantine formula too thanks to 1.6.1, so that h is diophantine.
Primitive recursion: let $h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$ and $h(x_1, \ldots, x_n, t+1) = g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n)$ for f, g diophantine functions, then using 1.5.6

$$y = h(x_1, \ldots, x_n, t) \iff \exists u : \phi_1(u) \wedge \phi_2(u) \wedge \phi_3(u)$$

where:

$$\phi_1(u) = \exists v : v = f(x_1, \ldots, x_n, y) \wedge v = S(1, u)$$

$$\phi_2(u) = (\forall z)_{\leq t}(z = t \ \vee (\exists v : v = S(z+1, u) \wedge v = g(z, S(z, u), x_1, \ldots, x_n, t)))$$

$$\phi_3(u) = y = S(t, u)$$

All diophantine formulas thanks to 1.5.6 and 1.6.1. □

For the proof of 1.6.1, first a lemma generalizing both exponential and factorial diophantinity is needed:

Lemma 1.6.3. *$h(a, b, y) = \prod_{k=1}^{y}(a + bk)$ is a diophantine function.*

Proof. The idea is to find $M(a,b,y), f(a,b,y)$ diophantine functions such that $0 \leq h(a,b,y) < M(a,b,y) \wedge (b, M(a,b,y)) = 1$ so that $\exists q = q(a) : qb \equiv_{M(a,b,y)} a$, and finally aiming for $h(a,b,y) \equiv_{M(a,b,y)} f(a,b,y)$.
In particular, a trivial bound is $h(a,b,y) \leq (a+by)^y$, but to impose the second condition one might choose $M(a,b,y) = b(a+by)^y+1$ (trivially diophantine), then:

$$h(a,b,y) \equiv_{M(a,b,y)} \prod_{k=1}^{y}(bq+bk) = b^y \frac{(q+y)!}{y!} = b^y y! \binom{q+y}{y}$$

and in the previous chapter it was established the diophantinity of a function such as $f(a,b,y) = b^y y! \binom{q(a)+y}{y}$. □

To prove 1.6.1 one can notice that, taken $y_1^{(k)}, \ldots, y_m(k)$ solution associated to each $k \leq y$, then defining $u = max\{y_i^{(k)} : 1 \leq i \leq m, 1 \leq k \leq y\}$ one may suppose those solutions to be bounded too, so that the goal is to find an equivalent expression which get rid of multiple solutions, so that it is natural to find a uniform bound $0 \leq |P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})| < Q(y,u,x_1,\ldots,x_n)\ \forall k \leq y$.
Then, to impose the vanishing of P on those $m-$tuples depending on k could be expressed as a divisibility condition $\alpha_k \mid P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})$ combined with a bound $0 \leq |P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})| < \alpha_k\ \forall k \leq y$, in particular it is sufficient to ask for $Q(y,u,x_1,\ldots,x_n) \leq \alpha_k\ \forall k \leq y$.
To do so, it is useful the diophantinity of the factorial, cause the following fact holds: α prime, $\alpha \mid 1 + d \cdot Q! \implies Q < \alpha\ \forall d \in \mathbb{N}^+$.
In particular, the second condition on those α_k could be expressed for a suitable choice of $d_k \in \mathbb{N}^+$ as $\alpha_k \mid 1 + d_k \cdot t$, where $t = Q(y,u,x_1,\ldots,x_n)!$, so that the multiple divisibility conditions $\alpha_k \mid P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})$ can be expressed just as $\prod_{k=1}^{y}(1+d_k \cdot t) \mid P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})$, which a diophantine condition thanks to 1.6.3.
Now, to avoid this dependence on k for collecting those conditions all together it is just needed to manipulate the dividend, so that one may try to replace the variables $y_i^{(k)}$ with constants a_i such that $a_i \equiv_{1+d_k \cdot t} y_i^{(k)}\ \forall k \leq y$ so as of a constant c such that $c \equiv_{1+d_k \cdot t} k\ \forall k \leq y$, thanks to which the condition will transform as $\prod_{k=1}^{y}(1+d_k \cdot t) \mid P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)$.
To hope for something like that, the most natural way is to apply the Chinese Remainder Theorem to the sequence $\{1+d_k \cdot t\}_{k=1}^{y}$, which leads to the natural choice $d_k = k$ that should insure $(1+i \cdot t, 1+j \cdot t) = 1\ \forall 1 \leq i < j \leq y$.
Indeed, to find how to fulfill this coprimality suppose $d \mid 1 + i \cdot t \wedge d \mid 1 + j \cdot t \implies d \mid [j(1+i \cdot t) - i(1+j \cdot t)] = j - i \leq y \implies d \leq y$, so that imposing $y < Q(y,u,x_1,\ldots,x_n)$ recalling that $t = Q(y,u,x_1,\ldots,x_n)!$, then

$d \leq y \implies d \mid t$, which combined with $d \mid 1 + i \cdot t \wedge 1 \leq i \implies d = 1$ as desired.

To sum up, the vanishing of $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)})\ \forall k \leq y$ was reduced to the existence of $Q(y, u, x_1, \ldots, x_n)$ such that $y < Q(y, u, x_1, \ldots, x_n)$ and $0 \leq |P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)})| < Q(y, u, x_1, \ldots, x_n)\ \forall k \leq y$, together with the existence of a tuple $a_1, \ldots, a_m$ satisfying the divisibility conditions $a_i \equiv_{1+k\cdot t} y_i^{(k)}\ \forall k \leq y$ and $\prod_{k=1}^{y}(1 + k \cdot t) \mid P(y, k, x_1, \ldots, x_n, a_1, \ldots, a_m)$. So that, to conclude this reduction is just needed to observe the usefulness of the bound u on the solutions: indeed, one has $1 \leq y_i^{(k) \leq u}$ and $Q(y, u, x_1, \ldots, x_n) < Q(y, u, x_1, \ldots, x_n)! = t < 1 + kt\ \forall k \leq y$, so that adding the trivial condition $u < Q(y, u, x_1, \ldots, x_n)$, one will have that $y_i^{(k)}$ would be the residue dividing a_i by $1 + kt$, so that the congruence conditions could be resumed in $\prod_{k=1}^{y}(1 + k \cdot t) \mid \prod_{j=1}^{u}(a_i - j)\ \forall 1 \leq i \leq m$.
In particular, it was intuitively deduced the following key lemma:

Lemma 1.6.4. *Suppose* $\exists Q(y, u, x_1, \ldots, x_n)$ *s.t.*

i. $0 \leq |P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)| < Q(y, u, x_1, \ldots, x_n)\ \forall k \leq y\ \forall y_i \leq u$

ii. $y < Q(y, u, x_1, \ldots, x_n)$

iii. $u < Q(y, u, x_1, \ldots, x_n)$

Then the existence of $t, c, a_1, \ldots, a_m$ *satisfying the system:*

$$S = \begin{cases} I : t = Q(y, u, x_1, \ldots, x_n)! \\ II : 1 + ct = \prod_{k=1}^{y}(1 + kt) \\ III : 1 + ct \mid P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \\ IV : 1 + ct \mid \prod_{j=1}^{u}(a_i - j)\ \forall 1 \leq i \leq m \end{cases}$$

is equivalent to $(\forall k)_{\leq y} \exists (y_1, \ldots, y_m)_{\leq u} : P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$.

Proof. $(\implies) : \forall k \leq y$, let α_k be a prime divisor of $1 + kt$, then by I it must happen $\alpha_k > Q(y, u, x_1, \ldots, x_n)$.
Define $y_i^{(k)}$ as the remainder $a_i \equiv_{\alpha_k} y_i^{(k)}$, then by IV $\forall 1 \leq i \leq m\ \exists 1 \leq j_k^i \leq u$ such that $a_i \equiv_{\alpha_k} j_k^i$, but being $1 \leq y_i^{(k)} \leq \alpha_k$ and $1 \leq j_k^i \leq u$ and as one knows $u \leq Q(y, u, x_1, \ldots, x_n) \leq \alpha_k$ it must be $y_i^{(k)} = j_k^i \leq u$.
Also, by II $\forall k \leq y : 1 + kt \equiv_{\alpha_k} 1 + ct \equiv_{\alpha_k} 0 \implies kt \equiv_{\alpha_k} ct$, but being α_k

prime and $\alpha_k > Q(y,u,x_1,\dots,x_n) \implies (\alpha_k,t)=1$, so that $c \equiv_{\alpha_k} k$, which combined with the congruences $a_i \equiv_{\alpha_k} y_i^{(k)}$ leads to:

$$P(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}) \equiv_{\alpha_k} P(y,c,x_1,\dots,x_n,a_1,\dots,a_m)$$

So that by III $\alpha_k \mid P(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)})$, but also being $y_i^{(k)} \leq u$ one has $0 \leq |P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)| < Q(y,u,x_1,\dots,x_n) < \alpha_k$, so that $P(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}) = 0$ as desired.
$(\impliedby)$: define $t = Q(y,u,x_1,\dots,x_n)!$ satisfying I.
Then, the congruence $\prod_{k=1}^{y}(1+kt) \equiv_t 1$ gives the definition of c satisfying II.
As remarked above, the numbers $\{1+kt : 1 \leq k \leq y\}$ are pairwise coprime, then by the Chinese Remainder Theorem $\forall 1 \leq i \leq m\ \exists a_i : a_i \equiv_{1+kt} y_i^{(k)}\ \forall k \leq y$ and by $1+kt \mid (1+ct)-(1+kt) = (c-k)t \wedge (1+kt,t) = 1 \implies c \equiv_{1+kt} k\ \forall k \leq y$, so that:

$$P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv_{1+kt} P(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}) = 0$$

$\forall k \leq y$, so that III is satisfied too again by coprimality.
Finally, IV is given by $a_i \equiv_{1+kt} y_i^{(k)}\ \forall k \leq y$, coprimality and $y_i^{(k)} \leq u$. □

It is easy to check the existence of such polynomial $Q(y,u,x_1,\dots,x_n)$ satisfying the conditions of 1.6.4, which is the task of next lemma:

Lemma 1.6.5. *$\forall P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)\ \exists Q(y,u,x_1,\dots,x_n)$ s.t.*

i. $0 \leq |P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)| < Q(y,u,x_1,\dots,x_n)\ \forall k \leq y\ \forall y_i \leq u$

ii. $y < Q(y,u,x_1,\dots,x_n)$

iii. $u < Q(y,u,x_1,\dots,x_n)$

Proof. Expressing $P(y,k,x_1,\dots,x_n,y_1,\dots,y_m) = \sum_r t_r$, of terms of the form $t_r = dy^a k^b x_1^{q_1}\dots x_n^{q_n} y_1^{s_1}\dots y_m^{s_m}$, then defining $Q(y,u,x_1,\dots,x_n) = y+u+\sum_r u_r$ where $u_r = |d| y^{a+b} x_1^{q_1}\dots x_n^{q_n} u^{\sum_{i=1}^m s_i}$ the claim follows. □

Finally, it is a trivial remark that 1.6.1 is just a corollary of 1.6.4 and 1.6.5, cause the expressions in 1.6.4 are all diophantine thanks to 1.6.3.

1.7 Universal Diophantine Set and Recorsive Sets

It is simple Set Theory the fact that $\mathbb{N}[x_n : n \in \mathbb{N}] = \bigcup_{n\in\mathbb{N}} \mathbb{N}[x_0, \dots, x_n]$ is countable, being countable union of countable sets (recalling that $\#A[x] = \#P_F(A) = \#A$ for any set A thanks to the axiom of choice, where $P_F(A)$ is the set of finite subsets of A).
In particular, one could choose a way to enumerate those polynomials, let's fix it this way thanks to 1.5.5:

$$P_1 = 1,\ P_{3i-1} = x_{i-1},\ P_{3i} = P_{L(i)} + P_{R(i)},\ P_{3i+1} = P_{L(i)} \cdot P_{R(i)}$$

So that it is now possible to enumerate all the diophantine sets (of positive integers, from which all the others could be built) of dimension one (contained in $\mathbb{N}$), in the following way:

$$D_n = \{x_0 \in \mathbb{N} : \exists (x_1, \dots, x_n) \in \mathbb{N} : P_{L(n)}(x_0, x_1, \dots, x_n) = P_{R(n)}(x_0, x_1, \dots, x_n)\}$$

which is well-defined on the number of variables being $L(n), R(n) \leq n$ by 1.5.5.
Also this definition leads to a Universal Set defined as:

$$U = \{(x, n) \in \mathbb{N}^2 : x \in D_n\}$$

which next result shows to be diophantine too:

Theorem 1.7.1. *$U = \{(x, n) \in \mathbb{N}^2 : x \in D_n\}$ is diophantine.*

Proof. The thesis, thanks to 1.6.1, will follow from the claim: $x \in D_n \iff \exists u : \phi_1(u) \wedge \phi_2(u) \wedge \phi_3(u) \wedge \phi_4(u)$, where:

$$\phi_1(u) : S(1, u) = 1 \wedge S(2, u) = x$$

$$\phi_2(u) : (\forall i)_{\leq n} : (S(3i, u) = S(L(i), u) + S(R(i), u))$$
$$\phi_3(u) : (\forall i)_{\leq n} : (S(3i + 1, u) = S(L(i), u) \cdot S(R(i), u))$$
$$\phi_4(u) : S(L(n), u) = S(R(n), u))$$

Indeed, here the proof of the claim:
$(\implies)$ Let $x \in D_n \implies \exists x_1, \dots, x_n \in \mathbb{N}$:

$$P_{L(n)}(x, x_1, \dots, x_n) = P_{R(n)}(x, x_1, \dots, x_n)$$

In particular, using 1.5.6, one can find $u \in \mathbb{N}$ such that $S(i, u) = P_i(x, x_1, \dots, x_n)$ $\forall 1 \leq i \leq 3n+2$, so that by definition of the enumeration the claim is checked.

($\Longleftarrow$) Vice versa, defining $x_i = S(3i+2,u)$, then by induction it must happen $S(i,u) = P_i(x,x_1,\ldots,x_n)$ $\forall 1 \leq i \leq 3n+2$, so that in particular by $\phi_4(u)$ one has $P_{L(n)}(x,x_1,\ldots,x_n) = S(L(n),u) = S(R(n),u)) = P_{R(n)}(x,x_1,\ldots,x_n)$, which means $x \in D_n$. □

The previous result suggests a way to find an explicit non-diophantine set:

Theorem 1.7.2. *$V = \{n \in \mathbb{N} : n \notin D_n\}$ is not diophantine.*

Proof. By a Cantor argument, suppose by absurd V diophantine, then by 1.5.5 $\exists i \in \mathbb{N}$ such that $V = D_i$, so that $i \in V \iff i \notin V$ the contradiction. □

The previous result will also naturally give a non recursive function:

Theorem 1.7.3. *The function*

$$g(n,x) = \begin{cases} 1 \; if \; x \notin D_n \\ 2 \; if \; x \in D_n \end{cases}$$

is not diophantine.

Proof. Suppose by absurd g is diophantine, then let $P(n,x,y,y_1,\ldots,y_m)$ such that $y = g(n,x) \iff \exists y_1,\ldots,y_m : P(n,x,y,y_1,\ldots,y_m) = 0$, then it would be:

$$V = \{n \in \mathbb{N} : \exists y_1,\ldots,y_m : P(n,n,1,y_1,\ldots,y_m) = 0\}$$

So that V would be diophantine, contradicting 1.7.2. □

Finally, to prove the unsolvability of Hilbert's Tenth Problem, one has to formalize the notion of algorithm needed to theoretically establish the solvability of diophantine equations, and to do that the main point of reference is the famous "Church-Turing Thesis":

Theorem 1.7.4. *Every effectively calculable function is a computable function.*

Indeed, it is known that recursive functions are a model of computation for the theory of computability, so that they must incarnate the notion of algorithm needed (for alternative models see Turing Machines or Lamba Calculus).
In particular, supposing Hilbert's Tenth Problem would be solved by a recursive procedure h, then $\forall n \in \mathbb{N}$ let P_n a polynomial associated to D_n (diophantine set) so that $D_n = \{x \in \mathbb{N} : \exists y_1,\ldots,y_{m(n)} : P_n(x,y_1,\ldots,y_{m(n)}) = 0\}$, so

that h can be applied, $\forall n \in \mathbb{N}$, to the polynomial P_n to establish if $x \in D_n$ or not, which would make the function $g(n,x)$ computable, i.e. recursive by 1.7.4, i.e. diophantine by 1.5.2, contradicting 1.7.3.
In particular, the main result of the chapter follows:

Theorem 1.7.5. *Hilbert's Tenth Problem is unsolvable.*

As a corollary, it could be proved a strengthened version of Godel's Incompleteness Theorem:

Corollary 1.7.6. *Corresponding to any given axiomatization of number theory, there is a Diophantine equation which has no positive integer solutions, but such that this fact cannot be proved within the given axiomatization*

Finally, a theorem characterizing diophantine sets in an analogous way to 1.5.2:

Definition 1.7.7. $S \subseteq \mathbb{N}^n$ is called *recursively enumerable* if $\exists f(x, x_1, \dots, x_n)$, $g(x, x_1, \dots, x_n)$ recursive functions such that:

$$S = \{(x_1, \dots, x_n) \in \mathbb{N}^n : \exists x : f(x, x_1, \dots, x_n) = g(x, x_1, \dots, x_n)\}$$

Theorem 1.7.8. *$S \subseteq \mathbb{N}^n$ is recursively enumerable $\iff$ it is diophantine.*

Proof. ($\Longleftarrow$): By being diophantine $\exists P(x_1, \dots, x_n, y_1, \dots, y_m)$ such that:

$$S = \{(x_1, \dots, x_n) \in \mathbb{N}^n : \exists (y_1, \dots, y_m) \in \mathbb{N}^m : P(x_1, \dots, x_n, y_1, \dots, y_m) = 0\}$$

In particular, the equation $P(x_1, \dots, x_n, y_1, \dots, y_m) = 0$ might be espressed as $Q(x_1, \dots, x_n, y_1, \dots, y_m) = T(x_1, \dots, x_n, y_1, \dots, y_m)$ for polynomials Q, T with positive coeffients, which are recursive functions according to 1.5.3.
Using then 1.5.6, one can find a $u \in \mathbb{N}$ such that $S(i,u) = y_i \ \forall 1 \leq i \leq m$, so the claim follows with $f(u, x_1, \dots, x_n) = Q(x_1, \dots, x_n, S(1,u), \dots, S(m,u))$ and $g(u, x_1, \dots, x_n) = T(x_1, \dots, x_n, S(1,u), \dots, S(m,u))$.
($\Longrightarrow$): By being recursively enumerable $\exists f(x, x_1, \dots, x_n)$, $g(x, x_1, \dots, x_n)$ recursive functions such that:

$$S = \{(x_1, \dots, x_n) \in \mathbb{N}^n : \exists x : f(x, x_1, \dots, x_n) = g(x, x_1, \dots, x_n)\}$$

In particular:

$$S = \{(x_1, \dots, x_n) \in \mathbb{N}^n : \exists x, z : z = f(x, x_1, \dots, x_n) \wedge z = g(x, x_1, \dots, x_n)\}$$

which is diophantine being f, g diophantine by 1.5.2. □

Chapter 2

The work of Denef, Lipshitz and Pheidas

2.1 Generalizations of H10

Investigating the question of solvability of diophantine equation, right after the answer of Matiyasevich to Hilbert's tenth problem it was natural to try to extend the result to other rings, starting from the most natural ones: the rings of integers of number fields.
The classical case of Hilbert's tenth problem was mainly focused on producing as much diophantine subsets of $\mathbb{Z}$ as possible, so that finally it was sufficient to describe them as the recursively enumerable subsets.
In this case, finding all the diophantine subsets of the ring of integers of a number field will be just a corollary of establishing exactly one of those subsets, which is indeed $\mathbb{Z}$ as shown in 2.1.2, but first a lemma about general properties of diophantine sets inside rings of integers of number fields:

Proposition 2.1.1. *$K \subseteq L$ number fields:*

i. $S_1, S_2 \subseteq \mathcal{O}_L$ *diophantine* $\implies S_1 \cap S_2, S_1 \cup S_2 \subseteq \mathcal{O}_L$ *diophantine.*

ii. $\mathcal{O}_L \setminus \{0\} \subseteq \mathcal{O}_L$ *diophantine.*

iii. $\mathbb{Z} \subseteq \mathcal{O}_K$ *and* $\mathcal{O}_K \subseteq \mathcal{O}_L$ *diophantine* $\implies \mathbb{Z} \subseteq \mathcal{O}_L$ *diophantine.*

iv. $\mathbb{Z} \subseteq \mathcal{O}_L$ *diophantine* $\implies \mathbb{Z} \subseteq \mathcal{O}_K$ *diophantine.*

Proof. i. S_1 diophantine through the polynomial P_1, S_2 through P_2, then $S_1 \cup S_2$ is diophantine through $P_1 \cdot P_2$.
Let then $f(x) = x^n + a_1 x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with no roots in L (it exists being $L/\mathbb{Q}$ finite), then $S_1 \cap S_2$ is diophantine through $P_1^n + a_1 P_1^{n-1} P_2 + \cdots + a_0 P_2^n$.

ii. Since $1/2, 1/3 \notin \mathcal{O}_L$ then by the polynomial $P(x,y,v) = xy - (2v-1)(3v-1)$, one has immediately:

$$S := \{x \in \mathcal{O}_L : \exists y, v \in \mathcal{O}_L : P(x,y,v) = 0\} \subseteq \mathcal{O}_L \setminus \{0\}$$

Also, supposing $x \in \mathcal{O}_L \setminus \{0\}$, then by the decomposition of ideals in Dedekind domains $(x) = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = \mathfrak{p}_1^{e_1}\mathfrak{q}$ with $\mathfrak{p}_i$ prime ideals and $e_i, n \in \mathbb{N}^+$ since $x \neq 0$ and $x \in \mathcal{O}_L$.
Being $\mathfrak{p}_1^{e_1}$ and $\mathfrak{q}$ coprime ideals (trivially even in the limit case of $\mathfrak{q}= 1$) by the Chinese remainder theorem $\exists v \in \mathcal{O}_L : 3v \equiv_{\mathfrak{p}_1^{e_1}} 1 \wedge 2v \equiv_{\mathfrak{q}} 1$.
In particular, there are the ideals inclusions $(3v-1) \subseteq \mathfrak{p}_1^{e_1}$ and $(2v-1) \subseteq \mathfrak{q}$, which implies $((3v-1)\cdot(2v-1)) = (3v-1)\cdot(2v-1) \subseteq \mathfrak{p}_1^{e_1} \cdot \mathfrak{q} = (x)$, so that $\exists y \in \mathcal{O}_L : xy = (2v-1)(3v-1)$.
iii. By the hypothesis:

$$\mathbb{Z} = \{x \in \mathcal{O}_K : \exists y_1, \ldots, y_m : P(x, y_1, \ldots, y_m) = 0\}$$

$$\mathcal{O}_K = \{x \in \mathcal{O}_L : \exists z_1, \ldots, z_k : Q(x, z_1, \ldots, z_k) = 0\}$$

Then again choosing $f(x) = x^n + a_1 x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with no roots in L (it exists being $L/\mathbb{Q}$ finite), then:

$$\mathbb{Z} = \{x \in \mathcal{O}_L : \exists y_1, \ldots, y_m, z_1, \ldots, z_k \in \mathcal{O}_L : P^n + a_1 P^{n-1} Q + \cdots + a_0 Q^n = 0\}$$

iv. Supposing $P(x, y_1, \ldots, y_m)$ polynomial with coefficients in $\mathcal{O}_L$ such that $\mathbb{Z} = \{x \in \mathcal{O}_L : \exists y_1, \ldots, y_m \in \mathcal{O}_L : P(x, y_1, \ldots, y_m) = 0\}$, then since it is known $\mathcal{O}_L = \mathcal{O}_K\omega_1 + \cdots + \mathcal{O}_K\omega_n$ with $[L : K] = n$, one could write the unknowns $y_i = \sum_{j=1}^{n} x_{i,j}\omega_j$ so that with the new polynomial:

$$Q(x, x_{1,1}, \ldots, x_{m,n}) := R(x, \sum_{j=1}^{n} x_{1,j}\omega_j, \ldots, \sum_{j=1}^{n} x_{m,j}\omega_j)$$

where, recalling $Hom_K(L, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$:

$$R(x, y_1, \ldots, y_m) = \sum_{i=1}^{n} \sigma_i(P(x, y_1, \ldots, y_m))$$

So that $R(x, y_1, \ldots, y_m) \in \mathcal{O}_K[x, y_1, \ldots, y_m]$, and in particular $Q(x, x_{1,1}, \ldots, x_{m,n}) \in \mathcal{O}_K[x, x_{1,1}, \ldots, x_{m,n}]$, then it follows:

$$\mathbb{Z} = \{x \in \mathcal{O}_K : \exists x_{1,1}, \ldots, x_{m,n} \in \mathcal{O}_K : Q(x, x_{1,1}, \ldots, x_{m,n}) = 0\}$$

□

Lemma 2.1.2. *K number field: $\mathbb{Z} \subseteq \mathcal{O}_K$ diophantine $\implies$ H10 over $\mathcal{O}_K$ is unsolvable.*

Proof. Suppose by absurd the existence of a recursive procedure h that is able to test for any polynomial $P \in \mathcal{O}_K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ have solutions in the $y_i's$ variables for any given $x_1, \ldots, x_n \in \mathcal{O}_K$, for $n, m \in \mathbb{N}$ arbitrary.
Then, since $\mathbb{Z}$ is diophantine, for a certain polynomial $P_{\mathbb{Z}} \in \mathcal{O}_K[x, y_1, \ldots, y_t]$ one can describe it as:

$$\mathbb{Z} = \{x \in \mathcal{O}_K : \exists y_1, \ldots, y_t \in \mathcal{O}_K : P_{\mathbb{Z}}(x, y_1, \ldots, y_t) = 0\}$$

Also, there must exist a polynomial $Q = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with no roots in K, so that for any polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ one can apply h to the polynomial $R = P^n + a_{n-1}P^{n-1}P_{\mathbb{Z}} + \cdots + a_1 P P_{\mathbb{Z}}^{n-1} + a_0 P_{\mathbb{Z}}^n$, so that $R = 0 \iff P = P_{\mathbb{Z}} = 0$ ($\impliedby$ is obvious, for $\implies$ by absurd $R = 0$ and $P_{\mathbb{Z}} \neq 0$ (if $P \neq 0$ then it must also be $P_{\mathbb{Z}} \neq 0$), so that dividing by $P_{\mathbb{Z}}^n$ one will find $P/P_{\mathbb{Z}}$ as a solution for Q in K which is absurd).
This way, one would find a procedure to check for any polynomial with integral coefficients if it has integral solutions or not, contradicting the classical H10's unsolvability. □

With the same strategy, restricting to the totally real case since it's the protagonist of the main seminar and makes completely natural the extension of the definitio of recurively enumerable subsets, one can prove the analogue characterization of the classical case:

Lemma 2.1.3. *K totally real number field, $\mathbb{Z} \subseteq \mathcal{O}_K$ diophantine:*
$S \subseteq \mathcal{O}_K$ diophantine $\iff$ recursively enumerable.

Proof. ($\implies$): Always true as in [1].
($\impliedby$): Let $\omega_1, \ldots, \omega_n$ be an integral basis of K over $\mathbb{Q}$, in particular one has $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$, then since S is recursively enumerable $\exists f(x, x_1, \ldots, x_m)$, $g(x, x_1, \ldots, x_m)$ recursive functions such that:

$$S = \{(x_1, \ldots, x_m) \in \mathcal{O}_K^n : \exists x \in \mathcal{O}_K : f(x, x_1, \ldots, x_m) = g(x, x_1, \ldots, x_m)\}$$

But one could write $x = \sum_{j=1}^n \theta_j \omega_j$ and $x_i = \sum_{j=1}^n \lambda_{i,j}\omega_j$ for suitable $\lambda_{i,j} \in \mathbb{Z}$. In particular, defining the new functions:

$$h(\theta_1, \ldots, \theta_n, \lambda_{1,1}, \ldots, \lambda_{m,n}) := f(x, \sum_{j=1}^n \lambda_{1,j}\omega_j, \ldots, \sum_{j=1}^n \lambda_{m,j}\omega_j)$$

$$k(\theta_1, \ldots, \theta_n, \lambda_{1,1}, \ldots, \lambda_{m,n}) := g(x, \sum_{j=1}^n \lambda_{1,j}\omega_j, \ldots, \sum_{j=1}^n \lambda_{m,j}\omega_j)$$

which are going to be on each coordinate a classical recursive function, meaning diophantine by [1], so that each projection of S is diophantine in $\mathbb{Z}$, meaning diophantine in $\mathcal{O}_K$ too thanks to the hypothesis and the transitivity stated in 2.1.1 *iii.*, in particular S is diophantin in $\mathcal{O}_K$ since it's described as the solutions of the system of polynomials describing each coordinate of S and the linear polynomial given from the integral basis, and the intersection of diophantine sets is still diophantine by 2.1.1 *i.*. □

Finally, another useful tool to prove H10 for rings of integers of numbers fields is to make less restrictive the choice of the special subset one aims to be diophantine, which from 2.1.2 was just $\mathbb{Z}$:

Lemma 2.1.4. *$K \subseteq L$ number fields: $S \subseteq \mathcal{O}_L$ diophantine such that $\mathbb{N}^+ \subseteq S \subseteq \mathcal{O}_K \implies \mathcal{O}_K \subseteq \mathcal{O}_L$ diophantine.*

Proof. Choosing an integral base $\{\omega_1, \dots, \omega_n\}$ of $\mathcal{O}_K$, since $\mathbb{N}^+ \subseteq S \subseteq \mathcal{O}_K$, one could describe $\mathcal{O}_K$ as:

$$\mathcal{O}_K = \left\{ z \in \mathcal{O}_L : z = \sum_{i=1}^{n} \lambda_i \omega_i : \lambda_i \in S \vee -\lambda_i \in S \right\}$$

which is diophantine in $\mathcal{O}_L$ thanks to 2.1.1 *i.*. □

2.2 Quadratic number fields

The first and more natural case among all the number fields is the one of quadratic rings $\mathbb{Q}(\sqrt{D})$ for $D \in \mathbb{Z}$ square-free, which will be the main focus of this section.
In particular, thanks to 2.1.2 and 2.1.4 it is sufficient to prove the following lemma:

Lemma 2.2.1. *$D \in \mathbb{Z}$ square-free $\implies \exists\ \Sigma$ finite system of diophantine equations in variables $t, x, \dots, s$ such that:*

i. *$(t, x, \dots, s)$ solution to Σ in $\mathbb{Q}(\sqrt{D}) \implies t \in \mathbb{Z}$*

ii. *$k \in \mathbb{N} \setminus \{0\} \implies \exists (t, x, \dots, s)$ solution to Σ in $\mathbb{Q}(\sqrt{D})$ such that $t = k^2$*

Indeed, the set $S = \{t \in \mathbb{Q}(\sqrt{D}) : \Sigma(t, x, \dots, s) = 0\}$, by definition a diophantine set, will satisfy $\mathbb{N}^2 \subseteq S \subseteq \mathbb{Z}$ (with $\mathbb{N}^2$ the squares of natural numbers), so that by Lagrange's four-square theorem adding to Σ the equation $(a^2 + b^2 + c^2 + d^2)^2 = t$ (Actually $a^2 = t$ is sufficient since $\mathbb{Z}^2 = \mathbb{N}^2$) it is immediate that $\mathbb{N}^2$ is diophantine in $A(D) := \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, so trivially $\mathbb{N}$ is

diophantine and so $\mathbb{Z}$ too as required by 2.1.2.

To prove the main lemma 2.2.1 for quadratic rings the strategy will vary depending on the sign of D, so the real and imaginary cases will be separated, but still following a similar approach again based on the particular form of Pell's equation that was protagonist of the proof of the classical Hilbert's tenth problem. Indeed, recovering the notation from the previous chapter, here a useful property:

Lemma 2.2.2. *$a, n, k \in \mathbb{N}$ with $a > 1$: $y_{nk}(a)^2 \equiv_{y_n(a)^4} y_n(a)^2 k^2$*

Proof.

$$y_{nk}(a) = \sum_{i=0,\ i\equiv_2 1}^{k} \binom{k}{i} \cdot x_n(a)^{k-i} \cdot y_n(a)^i \cdot (a^2-1)^{\frac{i-1}{2}}$$

In particular $y_{nk}(a) \equiv_{y_n(a)^3} k x_n(a)^{k-1} y_n(a)$, so that $\frac{y_{nk}(a)}{y_n(a)} \equiv_{y_n(a)^2} k x_n(a)^{k-1}$, which, by using the Pell's equation in the form $x_n(a)^2 \equiv_{y_n(a)^2} 1$, implies:

$$\left(\frac{y_{nk}(a)}{y_n(a)}\right)^2 \equiv_{y_n(a)^2} k^2 (x_n(a)^2)^{k-1} \equiv_{y_n(a)^2} k^2$$

□

2.2.1 The Real case

For the real case one has $D > 1$ and the strategy will be based on next lemma:

Lemma 2.2.3. *$A, B \in \mathbb{N} \setminus \{0\}$ such that $A^2 - DB^2 = 1 \ \wedge\ x, y \in A(D)$ such that $x^2 - (A^2-1)y^2 = 1 \implies y^2 \in \mathbb{N}$.*

Proof. Clearly $a > 1$ and combining the two equations one obtains $x^2 - DB^2y^2 = (x - \sqrt{D}By)(x + \sqrt{D}By) = 1$, so the unit $u = x + \sqrt{D}By$ in $A(D)$ has inverse $u^{-1} = x - \sqrt{D}By$, in particular by squaring $u - u^{-1} = 2\sqrt{D}By$:

$$u^2 + u^{-2} = 4DB^2y^2 + 2$$

Noticing $u^{-1} = \pm\overline{u}$ it must be $4DB^2y^2 + 2 \in \mathbb{Z}$, so that $y^2 \in \mathbb{Q} \cap A(D) = \mathbb{Z}$, but for $D > 1$ then $y^2 \in \mathbb{N}$. □

Remark 2.2.4. A useful remark is that in $A(D)$ for $D > 1$ one could try to imitate the following property of integers:

$$n, m, k \in \mathbb{N} : 0 \le n, m < k \ \wedge\ n \equiv_k m \implies n = m$$

Indeed, analogously one can state:

$$x, y, z \in A(D) : x \equiv_z y \ \wedge\ 0 \le x, y < z \ \wedge\ 0 \le \overline{x}, \overline{y} < \overline{z} \implies x = y$$

Proof. By absurd $x \neq y \implies x - y = zw$ with $w \neq 0$, in particular $|x-y||\overline{x}-\overline{y}| = |z\overline{z}||N(w)|$, but $w \neq 0 \implies |N(w)| \geq 1$, so that $|x-y||\overline{x}-\overline{y}| \geq |z\overline{z}|$ which is a contradiction with the assumptions. □

Finally, the proof of the real case:

Theorem 2.2.5. *$D \in \mathbb{N} \setminus \{0,1\}$, $A, B \in \mathbb{N} \setminus \{0\}$ such that $A^2 - DB^2 = 1$, defining Σ as follows:*

$$\Sigma = \begin{cases} I : x^2 - (a^2-1)y^2 = 1 \\ II : u^2 - (a^2-1)v^2 = 1 \\ III : v^2 - y^2 t = zy^3 \\ IV : t = w^2 \\ V : y^2 - t = 1 + h^2 + q^2 + r^2 + s^2 \end{cases}$$

Then the conclusion of 2.2.1 holds.

Proof. i. Let $(t, x, \ldots, s) \in A(D)$ solution to Σ, by I and II and 2.2.3 one has $y^2, v^2 \in \mathbb{N}$, in particular by 2.2.2 $v^2/y^2 \equiv_{y^2} t$ and so $v^2/y^2 \equiv_{y^2} \overline{t}$, making $\overline{t} \equiv_{y^2} t$, but since by IV and V $0 \leq t, \overline{t} < y^2$, one has $t = \overline{t}$ by 2.2.4, and so $t \in \mathbb{Z}$ and $t \geq 0$ implies $t \in \mathbb{N}$ as claimed.
ii. Supposing $t = k^2$ for $k \in \mathbb{N}$ then IV is obviously satisfied.
By monotony on the index choosing $n \in \mathbb{N}$ such that $y_n(A) > k$ and setting $x = x_n(A), y = y_n(A), u = x_{nk}(A), v = y_{nk}(A)$ then I and II are also satisfied.
Finally, III can be satisfied thanks to 2.2.2 and V thanks to Lagrange's four-square theorem since $y, k \in \mathbb{N}$ and the choice $y^2 - k^2 > 0$. □

2.2.2 The Imaginary case

In this case, the previous strategy needs to be modified: with $D \leq -1$ square-free 2.2.3 no longer holds since there are no more non-trivial integral solution to the Pell's equation.
Next lemma is going to show a similar trick to 2.2.3 to guarantee the integrality using the characterization of the roots of unity in biquadratic fields:

Lemma 2.2.6. *$D \leq -1$, define $F = A^2 - 1$ where*

$$A = \begin{cases} 4 \text{ if } D = -1 \ \vee \ D = -3 \\ 3 \text{ otherwise} \end{cases}$$

Then for $x, y \in A(D) : x^2 - Fy^2 = 1 \implies y^2 \in \mathbb{Z}$.

Proof. $1 = x^2 - Fy^2 = (x - \sqrt{F}y)(x + \sqrt{F}y)$, so $u = x + \sqrt{F}y$ is a unit in $\mathbb{Q}(\sqrt{F}, \sqrt{D})$, which has invariants $r_1 = 0 \ \wedge \ r_2 = 2$ so that by Dirichlet's unit theorem one has $x + \sqrt{F}y = \rho\eta^m$ for ρ root of unity in $\mathbb{Q}(\sqrt{F}, \sqrt{D})$, η fundamental unity and $m \in \mathbb{Z}$.
In particular, $x - \sqrt{F}y = \rho^{-1}\eta^{-m}$ so that $4Fy^2 + 2 = \rho^2\eta^{2m} + \rho^{-2}\eta^{-2m}$. Again, from Dirichlet's theorem one has also a fundamental unit ϵ in $\mathbb{Q}(\sqrt{F})$, and also a unit in $\mathbb{Q}(\sqrt{F}, \sqrt{D})$ so it must happen $\epsilon = \rho_1\eta^k$, and recalling the Galois group $G_{\mathbb{Q}(\sqrt{F},\sqrt{D})/\mathbb{Q}} = \{1, \sigma_F, \sigma_D, \sigma_F \cdot \sigma_D\}$, with $\sigma_F(\sqrt{F}) = -\sqrt{F}$, $\sigma_F(\sqrt{D}) = \sqrt{D}$, $\sigma_D(\sqrt{D}) = -\sqrt{D}$, $\sigma_D(\sqrt{F}) = \sqrt{F}$:

$$\epsilon^2 = \epsilon\sigma_D(\epsilon) = (\rho_1\sigma_D(\rho_1))(\eta\sigma_D(\eta))^k = \rho' e^k$$

for certain ρ' root of unity of $\mathbb{Q}(\sqrt{F})$ and e unity of $\mathbb{Q}(\sqrt{F})$, so being ϵ fundamental in $\mathbb{Q}(\sqrt{F})$ then one can express $e = \pm\epsilon^{k'}$, so that finally $\epsilon^2 = \rho'(\pm\epsilon^{k'})^k$, in particular from $|\epsilon|^2 = |\epsilon|^{k'k}$ it must happen $k = \pm 1 \ \vee \ k = \pm 2$. Substituting $\eta^2 = \rho_2\epsilon^k$ in $4Fy^2 + 2 = \rho^2\eta^{2m} + \rho^{-2}\eta^{-2m}$:

$$4Fy^2 + 2 = \rho^2\rho_2^m\epsilon^{mk} + \rho^{-2}\rho_2^{-m}\epsilon^{-mk} = \rho_3\epsilon'^m + \rho_3\epsilon'^{-m}$$

For the choice of F one has $N_{\mathbb{Q}(\sqrt{F}/\mathbb{Q})}(\epsilon') = 1$, so that $\sigma_F(\epsilon') = \epsilon'^{-1}$, so considering the imaginary parts of both sides since $Im(\epsilon') = 0$ and $Im(\rho_3^{-1}) = -Im(\rho_3)$:

$$Im(4Fy^2 + 2) = (\epsilon'^m - \sigma_F(\epsilon'^m))Im(\rho_3)$$

But $y \in A(D)$ implies $Im(4Fy^2 + 2) = q_1\sqrt{-D}$ and $\epsilon' \in \mathbb{Q}(\sqrt{F})$ implies $(\epsilon'^m - \sigma_F(\epsilon'^m)) = q_2\sqrt{F}$, for $q_1, q_2 \in \mathbb{Q}$.
Since roots of unity in biquadratic imaginary fields could be just the ones in the set $U = \{\pm 1, \pm i, (\pm 1 \pm i\sqrt{3})/2, (\pm i \pm \sqrt{3})/2, (\pm\sqrt{2} \pm i\sqrt{2})/2\}$, then it must happen $Im(\rho_3) = q_3\sqrt{S}$ for $q_3 \in \mathbb{Q}$ and $S \in \{0, 1, 3\}$ ($S \neq 2$ since $F \in \{3, 15\}$).
In particular, $q_1\sqrt{-D} = q_2q_3\sqrt{FS}$, imposing $q_1 = q_2q_3 = 0$ for the choices of F, so that $4Fy^2 + 2 \in \mathbb{Q}$ giving $y^2 \in \mathbb{Q} \cap A(D) = \mathbb{Z}$.

□

Remark 2.2.7. To imitate the strategy of 2.2.4, one can notice the alternative statement:

$$D \leq -1, t \in A(D), n, m \in \mathbb{Z} : t \equiv_m n \ \wedge \ N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t) < m^2/4 \implies t \in \mathbb{Z}.$$

Proof. For certain $u, v \in \mathbb{Z}$ one has $t = n + (u + iv\sqrt{-D})m/2$, so that it follows $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t) = (n + um/2)^2 + |D|v^2m^2/4$, so if by absurd $v \neq 0$, then $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t) \geq m^2/4$ which is a contradiction, in particular being $v = 0$ it follows $t \in \mathbb{Z}$.

□

Theorem 2.2.8. *$D \in \mathbb{Z}$ with $D \leq -1$, $F = A^2 - 1$ where*

$$A = \begin{cases} 4 \text{ if } D = -1 \ \vee \ D = -3 \\ 3 \text{ otherwise} \end{cases}$$

Then defining Σ as follows:

$$\Sigma = \begin{cases} I : x^2 - Fy^2 = 1 \\ II : u^2 - Fv^2 = 1 \\ III : v^2 - y^2 t = zy^3 \\ IV : ry + s(5h + 2) = 1 \\ V : y = 2tw \end{cases}$$

Then the conclusion of 2.2.1 holds.

Proof. i. Let $(t, x, \ldots, s) \in A(D)$ solution to Σ, by I and II and 2.2.6 one has $y^2, v^2 \in \mathbb{Z}$, in particular by 2.2.2 $v^2/y^2 \equiv_{y^2} t$.
Supposing by absurd $y = 0$, then IV implies $s(5h + 2) = 1$, being $5h + 2$ a unity which having $h \in A(D)$ is impossible since it should be in the list $\{\pm 1, \pm i, (\pm 1 \pm i\sqrt{3})/2, (\pm i \pm \sqrt{3})/2\}$.
Thanks to V, $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(y^2) = 16(N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t))^2(N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(w))^2$ and the combined facts of $y \neq 0 \ \wedge \ y \in \mathbb{Z}$ give $y^4 = N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(y^2) \geq 16 N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t)$, in particular $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(t) < (y^2)^2/4$ so that since $y^2, v^2/y^2 \in \mathbb{Z}$ by 2.2.7 $t \in \mathbb{Z}$.
ii. Supposing $t = k^2$ for $k \in \mathbb{N} \setminus \{0\}$ then choosing solutions $X, Y \in \mathbb{N}$ with $Y \neq 0$ such that $X^2 - (F(2t)^2)Y^2 = 1$ and, seen that $F = A^2 - 1$, setting $x = x_n(A), y = y_n(A), u = x_{nk}(A), v = y_{nk}(A), w = Y$ then I, II and V are satisfied and $y \neq 0$.
Finally, III can be satisfied thanks to 2.2.2 and since $y \neq 0$ IV can be satisfied for any number of the sequence $\{5h + 2\}_{h \in \mathbb{N}}$ coprime to y (recalling Dirichlet's theorem on arithmetic progressions, infinitely many of them are primes, so all of those except the prime divisors of y, which are finitely many, will work).

□

In the end, putting all together:

Theorem 2.2.9. *$D \in \mathbb{Z}$ square-free:*

i. $\mathbb{Z}$ diophantine in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

ii. $S \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$: S diophantine $\iff$ recursively enumerable.

iii. H10 is unsolvable for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Proof. i. follows from 2.2.1, 2.2.5 and 2.2.8, then *ii.* follows from *i.* and 2.1.3, and *iii.* from *i.* and 2.1.2.

□

2.3 Refinements to other rings of integers

A similar reasoning with a more accurate argument will lead to the generalization of the previous result:

Theorem 2.3.1. *L number field satisfying one of the followings:*

i. $[L:\mathbb{Q}] = 2$.

ii. $[L:\mathbb{Q}] = 4$, *L not totally real and* $\exists K \subseteq L : [K:\mathbb{Q}] = 2$.

iii. $\exists K \subseteq L : [L:K] = 2$ *and K totally real and $\mathbb{Z}$ diophantine in* $\mathcal{O}_K$.

Then $\mathbb{Z}$ is diophantine in $\mathcal{O}_L$.

The main lemma on which the proof of 2.3.1 is the following:

Lemma 2.3.2. *L/K Galois extension of number fields,* $\exists d \in \mathcal{O}_L \setminus \{0\}$ *such that:*

i. $x^2 - dy^2 = 1$ *has infinitely many solutions in* $\mathcal{O}_L$.

ii. $\exists e \in \mathbb{N}^+$:

$$\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}} \in K$$

$\forall x, y \in \mathcal{O}_L$ *satisfying* $x^2 - dy^2 = 1$.

Then $\mathcal{O}_K$ diophantine over $\mathcal{O}_L$.

For this purpose, two preliminary lemmas trying to generalize the technique used in 2.2.3 and 2.2.6:

Lemma 2.3.3. *L/K Galois extension of number fields with* $[L:\mathbb{Q}] = n$: $\xi \in \mathcal{O}_L, z, w \in \mathcal{O}_K$ *such that:*

i. $\xi \equiv_z w$.

ii. $2^{n+1}\xi^n(\xi+1)^n \dots (\xi+n-1)^n \mid z$.

Then $\xi \in \mathcal{O}_K$.

Proof. If $z = 0$, then $\xi = w \in \mathcal{O}_K$.
Supposing $z \neq 0$, by *ii.* $|N_{L/\mathbb{Q}}(2^{n+1}(\xi+j)^n)| \leq |N_{L/\mathbb{Q}}(z)|$ $\forall j \in \{0, \dots, n-1\}$, in particular $|N_{L/\mathbb{Q}}(\xi+j)| \leq c := |N_{L/\mathbb{Q}}(z/2^{n+1})|^{1/n} (\geq 1$ since $z \neq 0)$.
In particular, for $Hom_{\mathbb{Q}}(L, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$ one has $\prod_{i=1}^n (\sigma_i(\xi) + j) \leq c$, which by next remark implies $|\sigma_i(\xi)| \leq 2^n c = \frac{1}{2}|N_{L/\mathbb{Q}}(z)|^{1/n}$ $\forall i \in \{1, \dots, n\}$.

Remark 2.3.4. $a_1, \ldots, a_n \in \mathbb{C}, c \in \mathbb{R}, c \geq 1 : \prod_{i=1}^{n} |a_i + j| \leq c \ \forall 0 \leq j \leq n-1 \implies |a_i| \leq 2^n c \ \forall 1 \leq i \leq n$

Furthermore, for any $\tau \in G_{L/K} : \tau(\xi) \equiv_{\tau(z)=z} \tau(w) = w \equiv_z \xi$ and $\sigma_i(\tau(\xi)) < \frac{1}{2}|N_{L/\mathbb{Q}}(z)|^{1/n}$, so that $\sigma_i(\xi - \tau(\xi)) < \frac{1}{2}|N_{L/\mathbb{Q}}(z)|^{1/n}$, in particular $\xi = \tau(\xi)$, giving $\xi \in \mathcal{O}_K$.

□

Remark 2.3.5. L number field, $t \in \mathcal{O}_L \setminus \{0\}$, $\epsilon \in \mathcal{O}_L$ unit $\implies \exists m \in \mathbb{N}^+ : t \mid \epsilon^m - \epsilon^{-m}$.
Indeed, for $m := \#(\mathcal{O}_L/(t))^*$, then $\epsilon^{\pm m} \equiv_t 1$.

Lemma 2.3.6. *L number field, $\epsilon \in \mathcal{O}_L$ unit, $k \in \mathbb{N}$ odd:*

$$\frac{\epsilon^k - \epsilon^{-k}}{\epsilon - \epsilon^{-1}} \equiv_{\epsilon - \epsilon^{-1}} k$$

Proof.

$$\frac{\epsilon^k - \epsilon^{-k}}{\epsilon - \epsilon^{-1}} = \sum_{i=0}^{k-1} \epsilon^{k-2i-1}$$

But since $\epsilon \equiv_{\epsilon-\epsilon^{-1}} \epsilon^{-1}$:

$$\sum_{i=0}^{k-1} \epsilon^{k-2i-1} \equiv_{\epsilon-\epsilon^{-1}} k\epsilon^{k-1}$$

But again $\epsilon^2 \equiv_{\epsilon-\epsilon^{-1}} 1$, since k is odd $\epsilon^{k-1} \equiv_{\epsilon-\epsilon^{-1}} 1$.

□

Following again the strategy of 2.2.1 the diophantinity of $\mathcal{O}_K$ over $\mathcal{O}_L$ will follow from next lemma:

Lemma 2.3.7. *L/K Galois extension of number fields with $d \in \mathcal{O}_L \setminus \{0\}$ and $e \in \mathbb{N} \setminus \{0\}$ such that:*

i. the equation $x^2 - dy^2 = 1$ has infinitely many solutions in $\mathcal{O}_L$.

ii. $\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}} \in K \ \forall x, y \in \mathcal{O}_L : x^2 - dy^2 = 1.$

Define Σ *as follows:*

$$\Sigma = \begin{cases} I : x^2 - dy^2 = 1 \\ II : u^2 - dv^2 = 1 \\ III : z = \frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}} \\ IV : z \neq 0 \\ V : zw = \frac{(u+v\sqrt{d})^e - (u-v\sqrt{d})^e}{2\sqrt{d}} \\ VI : w \equiv_z 2\xi + 1 \\ VII : 2^{n+1}(2\xi+1)^n \dots (2\xi+n)^n \mid z \end{cases}$$

Define $S \subseteq \mathcal{O}_L$ *by* $\xi \in S \iff \exists x, y, u, v, z, w \in \mathcal{O}_L$ *satisfying* Σ.
Then $S \subseteq \mathcal{O}_L$ *diophantine and* $\mathbb{N} \subseteq S \subseteq \mathcal{O}_K$.

Proof. $S \subseteq \mathcal{O}_L$ diophantine since 2.1.1 *i.* & *ii.* and hypothesis *ii.*.
Suppose first $\xi \in S$, then by hypothesis *ii.*, I and III one has $z \in \mathcal{O}_L \cap K = \mathcal{O}_K$, and with the same reasoning from II and V $zw \in \mathcal{O}_K$, but since IV it must be $w \in \mathcal{O}_K$ too.
In particular, by VI and VII $\xi \in \mathcal{O}_K$ by 2.3.3, so that $S \subseteq \mathcal{O}_K$.
Furthermore, supposing $\xi \in \mathbb{N}$, there must be found solutions in $\mathcal{O}_L$ to Σ.
First of all, choosing $x_0, y_0 \in \mathcal{O}_L$ satisfying I such that $\epsilon = x_0 + y_0\sqrt{d}$ is not a root of unity (possible by hypothesis *i.* and $L/\mathbb{Q}$ finite), then $\epsilon \in \mathcal{O}_{L'}^*$ where $L' = L(\sqrt{d})$.
By 2.3.5 $\exists m \in \mathbb{N}^+$ such that:

$$2^{n+1}(2\xi+1)^n \dots (2\xi+n)^n 2\sqrt{d} \mid \epsilon^m - \epsilon^{-m}$$

Defining $x, y : x + y\sqrt{d} = \epsilon^m \ \wedge \ x - y\sqrt{d} = \epsilon^{-m}$, then it must be $x, y \in \mathcal{O}_L$ (if $\sqrt{d} \notin L$, then $x = \sigma(x) \ \wedge \ y = \sigma(y)$, where $\sigma(\sqrt{d}) = -\sqrt{d}$), so that I is satisfied.
Setting $z = \frac{\epsilon^{me} - \epsilon^{-me}}{2\sqrt{d}}$ III is satisfied, but also IV since ϵ is not a root of unity, and of course by the choice of $m \in \mathbb{N}^*$ VII holds.
Finally, defining u, v unique satisfying $u + v\sqrt{d} = \epsilon^{m(2\xi+1)}$ and $u - v\sqrt{d} = \epsilon^{-m(2\xi+1)}$ II is satisfied, and then setting $w = \frac{\epsilon^{me(2\xi+1)} - \epsilon^{-me(2\xi+1)}}{\epsilon^{me} - \epsilon^{-me}}$, then $w \in \mathcal{O}_L$ and clearly V is satisfied, but by 2.3.7 VI is satisfied too which completes the construction of a solution to Σ, in particular $\mathbb{N} \subseteq S$. □

Lemma 2.3.8. *L number field,* $U_L := \mathcal{O}_L^*$ *group of units of L,* $d \in \mathcal{O}_L$ *such that* $L' := L(\sqrt{d}) \neq L$, *defining:*

$$V_L = \{x + y\sqrt{d} : x, y \in \mathcal{O}_L \ \wedge \ x^2 - dy^2 = 1\}$$

then $V_L \leq U_{L'}$ *and* $rk(U_L) = rk(U_{L'}) - rk(V_L)$

Proof. Considering the restriction of the norm map $x \in U_{L'} \mapsto N_{L'/L}(x) \in U_L$, then $V_L \leq Ker(N_{L'/L}|_{U_{L'}}) \leq U_{L'}$.
By 2.3.5 one has $[Ker(N_{L'/L}|_{U_{L'}}) : V_L] < +\infty \wedge [U_L : Im(N_{L'/L}|_{U_{L'}})] < +\infty$, so that:

$$rk(V_L) = rk(Ker(N_{L'/L}|_{U_{L'}})) = rk(U_{L'}) - rk(Im(N_{L'/L}|_{U_{L'}})) = rk(U_{L'}) - rk(U_L)$$

□

Remark 2.3.9. To prove 2.3.1 the strategy will be the following: proving for each case the existence of $d \in \mathcal{O}_L \setminus \{0\}$ and $e \in \mathbb{N} \setminus \{0\}$ satisfying 2.3.7, so that there must exist such a diophantine subset S, so that $\mathcal{O}_K \subseteq \mathcal{O}_L$ is diophantine from 2.1.4.
Notice that the assumption of 2.3.7 of the extension being Galois is checked in all of the cases since L/K is quadratic of $char(K) \neq 2$, so it must be Galois, then the result follows from the transitivity of being diophantine stated in 2.1.1 *iii.*.

Finally, according to the previous remark, the proof of 2.3.1:
Case *iii.*: Let $Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_h, \sigma_{h+1}, \dots, \sigma_k\}$, where $\{\sigma_1, \dots, \sigma_h\}$ do not extend to embeddings of L into $\mathbb{R}$ and $\{\sigma_{h+1}, \dots, \sigma_k\}$ extend to embeddings of L into $\mathbb{R}$, then by hypothesis $h \geq 1$.
Choosing $d \in \mathcal{O}_K$ such that $\sigma_i(d) > 0$ for $1 \leq i \leq h$ and $\sigma_i(d) < 0$ for $h+1 \leq i \leq k$.
Setting $K' = K(\sqrt{d})$ and $L' = L(\sqrt{d})$, then by Dirichlet theorem one has $rk(U_K) = k-1$, $rk(U_{K'}) = k+h-1$, $rk(U_L) = 2k-h-1$ and $rk(U_{L'}) = 2k-1$.
By 2.3.8 $rk(V_K) = h$ and $rk(V_L) = h$, so that $e := [V_L : V_K] < +\infty$.
Being $h \geq 1$ then $x^2 - dy^2 = 1$ has infinitely many solutions in $\mathcal{O}_L$ so *i.* is satisfied.
Furthermore, $\forall x, y \in \mathcal{O}_L : x^2 - dy^2 = 1$ one has $(x \pm y\sqrt{d})^e \in V_K \subseteq K'$, but the element $\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}}$ is invariant under the automorphism $\sqrt{d} \mapsto -\sqrt{d}$, so it is in L, in particular it is in $K' \cap L = K$ as desired.

Case *i.*: If L is imaginary, then it follows from Case *iii.* with $K = \mathbb{Q}$.
If L is real, then $L = \mathbb{Q}(\sqrt{d})$ for a certain $d \in \mathbb{N}^+$, and by the classical Pell's equation with infinitely many solutions in $\mathbb{Z}$, condition *i.* of 2.3.7 is satisfied.
The automorphism $\tau : \sqrt{d} \mapsto -\sqrt{d}$ is such that $\tau(x+y\sqrt{d}) = \pm(x+y\sqrt{d})^{-}1 = \pm(x-y\sqrt{d})$, so considering $e = 2$ the element $\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}}$ is τ-invariant, in particular it is in $\mathbb{Q}$, but also in $\mathcal{O}_L$, then it must be in $\mathbb{Z}$.

Case *ii.*: If K is real then the claim follows from Case *iii.* and Case *i.*.

Supposing K imaginary, then U_K is finite by Dirichlet theorem, defining then $e := \#U_K$ and choose $d \in \mathcal{O}_L : L = K(\sqrt{d})$, so that since $rk(V_K) = rk(U_L) \geq 1$ condition *i.* of 2.3.7 is satisfied.
Finally, condition *ii.* is satisfied being $N_{L/K}(x + y\sqrt{d}) \in U_K$, which by the definition of e gives $(x + y\sqrt{d})^e \tau(x + y\sqrt{d})^e = 1$ with the automorphism $\tau : \sqrt{d} \mapsto -\sqrt{d}$ fixing K.
In particular, $\tau(x + y\sqrt{d})^e = (x + y\sqrt{d})^{-e} = (x - y\sqrt{d})^e$, so that the element $\frac{(x+y\sqrt{d})^e - (x-y\sqrt{d})^e}{2\sqrt{d}}$ is τ-invariant, which means it is in K, but also in $\mathcal{O}_L$, then it must be in $\mathcal{O}_K$.

Remark 2.3.10. This generalization of the method of the first section cannot be improved since the conditions *i.* and *ii.* of the main tool used (2.3.7) can be both satisfied only with extension of number fields of the cases of 2.3.1.

2.4 Totally real number fields

The main goal of the last section of the article will be the following theorem:

Theorem 2.4.1. *Let K be a totally real number field: $\mathbb{Z} \subseteq \mathcal{O}_K$ is diophantine.*

For such purpose the strategy will follow ideas close to the ones for the diophantinity of the exponential function, which will work thanks to the order on $\mathbb{R}$ that will make possible using congruences and bounds to deduce equalities.
To procede this way, next lemma is the key point and makes clear the assumpion on the number field:

Lemma 2.4.2. *K number field, σ embedding of K into $\mathbb{R}$: $\{x \in \mathcal{O}_K : \sigma(x) \geq 0\}$ diophantine.*

Proof. Choosing $c \in \mathcal{O}_K : \sigma(c) > 0 \wedge \tau(c) < 0 \ \forall \tau \in Hom_{\mathbb{Q}}(K, \mathbb{C}) \setminus \{\sigma\}$, $\forall x \in \mathcal{O}_K$: $\sigma(x) \geq 0 \iff \exists x_0, x_1, x_2, x_3, x_4 \in \mathcal{O}_K : x_0 \neq 0 \wedge x_0^2 x = x_1^2 + x_2^2 + x_3^2 + c x_4^2$ by Hasse-Minkowski theorem on quadratic forms representation, and from 2.1.1 *i.* and *ii.* the claim follows. □

In particular, it turns out that to prove 2.4.1 thanks to 2.4.2 it is sufficient to show the existence of a more generic diophantine subset S of $\mathcal{O}_K$ satisfying next lemma:

Lemma 2.4.3. *K totally real number field, $S \subseteq \mathcal{O}_K$ diophantine such that $\mathbb{N}^+ \subseteq S \subseteq \mathbb{Z} \implies \mathbb{Z} \subseteq \mathcal{O}_K$ diophantine.*

Proof. Applying 2.1.4 with the number fields extension $K/\mathbb{Q}$ ($\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$). □

Pell's equation revisited

K number field, $a \in \mathcal{O}_K$, define $\delta(a) = \sqrt{a^2 - 1}$ and $\epsilon(a) = a + \delta(a)$.
Supposing $\delta(a) \notin K$, in analogy with the classical case define the sequences:

$$x_m(a) + y_m(a)\delta(a) = (\epsilon(a))^m$$

Lemma 2.4.4. *K number field, $a, b, c \in \mathcal{O}_K : \delta(a), \delta(b) \notin K$, $m, h, k, j \in \mathbb{N}$, then:*

i. $\epsilon(a) \in \mathcal{O}^*_{K(\delta(a))}$ *with* $\epsilon(a)^{-1} = a - \delta(a)$.

ii. $\{(x_m(a), y_m(a)) : m \in \mathbb{N}\} \subseteq \{(x, y) \in \mathcal{O}_K^2 : x^2 - (a^2 - 1)y^2 = 1\}$.

iii. $x_m(a) = \frac{\epsilon(a)^m + \epsilon(a)^{-m}}{2}$, $y_m(a) = \frac{\epsilon(a)^m - \epsilon(a)^{-m}}{2\delta(a)}$.

iv. $x_{m\pm k}(a) = x_m(a)x_k(a) + (a^2 - 1)y_m(a)y_k(a)$.
$y_{m\pm k}(a) = x_k(a)y_m(a) \pm x_m(a)y_k(a)$.

v. $h \mid m \implies y_h(a) \mid y_m(a)$.

vi. $y_{hk}(a) \equiv_{y_h(a)^3} k x_h(a)^{k-1} y_h(a)$.

vii. $x_{m+1}(a) = 2a x_m(a) - x_{m-1}(a)$, $y_{m+1}(a) = 2a y_m(a) - y_{m-1}(a)$.

viii. $y_m(a) \equiv_{a-1} m$.

ix. $a \equiv_c b \implies x_m(a) \equiv_c x_m(b) \ \wedge \ y_m(a) \equiv_c y_m(b)$.

x. $x_{2m\pm j}(a) \equiv_{x_m(a)} -x_j(a)$.

xi. $\eta \in \mathcal{O}_K \setminus \{0\} \implies \exists m \in \mathbb{N}^+ : \eta \mid y_m(a)$.

Proof. *i.-ix.* are equal to the classical case in Chapter I.
x.: Let $m := \#(\mathcal{O}_{K(\delta(a))}/(2\eta\delta(a)))^*$, then $\epsilon(a)^{\pm m} \equiv_{2\eta\delta(a)} 1$, in particular one has $\eta \mid \frac{\epsilon(a)^m - \epsilon(a)^{-m}}{2\delta(a)} = y_m(a)$. □

Suppose for the rest of the section K totally real number field with the real embeddings $Hom_{\mathbb{Q}}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_n\}$.
Suppose $a \in \mathcal{O}_K$ such that:

$$\sigma_1(a) \geq 2^{2n} \ \wedge \ |\sigma_i(a)| \leq 1/2 \ \forall i \in \{2,\dots,n\} \qquad (*)$$

so that $a \notin \mathbb{Z}$ and $\delta(a) \notin K$, define $L = K(\delta(a))$ with the embeddings $Hom_{\mathbb{Q}}(L,\mathbb{C}) = \{\sigma_{i,1},\sigma_{i,2} : i \in \{1,\dots,n\}\}$.
In particular, one has $\sigma_{i,1}(\delta(a)) = \pm\sqrt{\sigma_i(a)^2-1}$ and $\sigma_{i,2}(\delta(a)) = -\sigma_{i,1}(\delta(a))$, so for the assumptions on a, $\sigma_{1,1}$ and $\sigma_{1,2}$ are the only real embeddings of L.
Choosing $\sigma_{1,1}$ such that $0 < \sigma_{1,1}(\delta(a)) = +\sqrt{\sigma_i(a)^2-1}$, one can identify L as a subfield of $\mathbb{R}$ through this automorphism, and similarly for K with σ_1.
Next lemma will show trivial bounds that will help to reach the desired bounds similar to the one of $*$:

Lemma 2.4.5. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$, then $\forall m \in \mathbb{N}^+, \forall i \in \{2,\dots,n\}, \forall j \in \{1,2\}$:*

i. $a/2 < \delta(a) < a$, $\sigma_{i,j}(\delta(a)) \in \sqrt{-1}\mathbb{R}$, $1/2 < |\sigma_{i,j}(\delta(a))| < 1$.

ii. $a < \epsilon(a) < 2a$, $|\sigma_{i,j}(\epsilon(a))| = 1$.

iii. $\epsilon(a)^m/4a < y_m(a) < \epsilon(a)^m/a$, $|\sigma_i(y_m(a))| < 2$.

iv. $\epsilon(a)^m/2 < x_m(a) < \epsilon(a)^m$, $|\sigma_i(x_m(a))| < 1$.

Proof. i.: since $a = \sigma_1(a) \geq 2^{2n} \geq 16 > 2/\sqrt{3}$, then $a/2 < \delta(a) < a$ is obvious.
Since $i \geq 2$, $\sigma_{i,j}$ is not a real embedding, but being K totally real and $L = K(\delta(a))$, then it must be $\sigma_{i,j}(\delta(a)) \notin \mathbb{R}$, but $\delta(a)$ must then be purely imaginary and so $\sigma_{i,j}(\delta(a)) \in \sqrt{-1}\mathbb{R}$.
Finally, from $0 < |\sigma_i(a)| \leq 1/2$ one obtains $-1/2 \leq \sigma_i(a) \leq 1/2$, so that $0 < \sigma_i(a)^2 \leq 1/4$, equivalently $-1 < \sigma_i(a)^2 - 1 \leq -3/4$.
In particular, from $3/4 \leq |\sigma_i(a)^2 - 1| < 1$, one finally reaches the claim:

$$1/2 < \sqrt{3}/2 \leq \sqrt{|\sigma_i(a)^2-1|} = |\sigma_{i,j}(\delta(a))| < 1$$

ii.: By the previous $0 < a/2 < \delta(a) < a$ one has $a < a + \delta(a) = \epsilon(a) < a + a = 2a$.
Furthermore, $|\sigma_{i,j}(\epsilon(a))| = |(\sigma_i(a) \pm \sqrt{\sigma_i(a)^2-1})(\sigma_i(a) \mp \sqrt{\sigma_i(a)^2-1})| = 1$.
iii.: thanks to 2.4.4 *iii.* $y_m(a) = \frac{\epsilon(a)^m - \epsilon(a)^{-m}}{2\delta(a)}$, but since $a/2 < \delta(a) < a$, it holds $\frac{\epsilon(a)^m-\epsilon(a)^{-m}}{2a} < y_m(a) < \frac{\epsilon(a)^m-\epsilon(a)^{-m}}{a} \leq \frac{\epsilon(a)^m}{a}$.
But $16 \leq a < \epsilon(a)$, in particular $\epsilon(a)^{2m} > 2$, which means $\epsilon(a)^m/2 > \epsilon(a)^{-m}$, so that $\epsilon(a)^m - \epsilon(a)^{-m} \geq \epsilon(a)^m/2$, which also imply the other inequality.
iv.: Similar as *iii.*. □

Finally, the purpose of $*$ is clarified from next lemma: it will show that in this particular case the same property of the classical case holds, namely that all the solutions to the Pell's equation $x^2 - (a^2-1)y^2 = 1$ are of the form $(\pm x_m(a), \pm y_m(a))$, so generated by the solution $(a, 1)$:

Lemma 2.4.6. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$, then:*

$$\{(x,y) \in \mathcal{O}_K^2 : x^2 - (a^2-1)y^2 = 1\} = \{(\pm x_m(a), \pm y_m(a)) : m \in \mathbb{N}\}$$

Proof. Let $U_K := \mathcal{O}_K^*$ and $U_L := \mathcal{O}_L^*$, define:

$$S := \{x + \delta(a)y : x, y \in \mathcal{O}_K \ \wedge \ x^2 + (a^2-1)y^2 = 1\}$$

then $S \subseteq Ker := Ker(N_{L/K}|_{U_L} : U_L \to U_K)$.
Also $U_K^2 \subseteq Im := Im(N_{L/K}|_{U_L} : U_L \to U_K) \subseteq U_K$ and $[U_K : Im] < +\infty$, so that $1 \leq rk(S) \leq rk(U_L) - rk(U_K) = n - (n-1) = 1$ by Dirichlet theorem and $\epsilon \in S$.
But $S \subseteq \mathbb{R}$, so that $S_{tor} = \{\pm 1\}$, so choosing $\epsilon_0 = x_0 + \delta(a)y_0$ generator such that $\epsilon_0 > 1$, $\exists e \in \mathbb{N} : \epsilon = \epsilon_0^e$.
In particular, since $y_0 = (\epsilon_0 - \epsilon_0^{-1})/2\delta(a)$, one has $2\delta(a) \mid (\epsilon_0 - \epsilon_0^{-1})$, which implies:

$$|N_{L/\mathbb{Q}}(2\delta(a))| \leq |N_{L/\mathbb{Q}}(\epsilon_0 - \epsilon_0^{-1})|$$

By explicit computation:

$$|N_{L/\mathbb{Q}}(2\delta(a))| = 2^{[L:\mathbb{Q}]}\left|\delta(a)(-\delta(a)) \prod_{j=1}^{2}\prod_{i=2}^{n}(\sigma_{i,j}(\delta(a)))\right|$$

Being $[L : \mathbb{Q}] = 2n$ and using 2.4.5 *i.*:

$$|N_{L/\mathbb{Q}}(2\delta(a))| > 2^{2n}\delta(a)^2(1/2)^{2n-2} > a^2$$

Furthermore:

$$|N_{L/\mathbb{Q}}(\epsilon_0 - \epsilon_0^{-1})| = \left|(\epsilon_0 - \epsilon_0^{-1})(\epsilon_0^{-1} - \epsilon_0) \prod_{j=1}^{2}\prod_{i=2}^{n}(\sigma_{i,j}(\epsilon_0) - \sigma_{i,j}(\epsilon_0)^{-1})\right|$$

which by 2.4.5 *ii.* implies:

$$|N_{L/\mathbb{Q}}(\epsilon_0 - \epsilon_0^{-1})| \leq (\epsilon_0 - \epsilon_0^{-1})^2 2^{2n-2} < \epsilon_0^2 2^{2n-2}$$

and recollecting all together $a^2 < \epsilon_0^2 2^{2n-2}$, so supposing by absurd $e \neq 1$, then $\epsilon \geq \epsilon_0^2$, but since $2a > \epsilon$ by 2.4.5 *ii.*, then one has $a < 2^{2n-1}$ contradicting $*$. □

Furthermore, $*$ is important cause, as seen in the previous lemma, it guarantees many properties of the Pell's equation over $\mathbb{Z}$, and it is the case also for the main one that is used to control in a diophantine way the indexes of the canonical solutions $(\pm x_m(a), \pm y_m(a))$:

Lemma 2.4.7. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$, $h, m \in \mathbb{N}$ such that $|\sigma_i(y_h(a))| \geq 1/2 \ \forall i \in \{2, \dots, n\}$, then:*

i. $y_h(a) \mid y_m(a) \iff h \mid m$.

ii. $y_h(a)^2 \mid y_m(a) \implies h y_h(a) \mid m$.

Proof. *i.*: ($\Longleftarrow$) is given by 2.4.4 *v.*.
($\Longrightarrow$): by absurd suppose $h \nmid m$ so that $m = qh + k$ for certain $q, k \in \mathbb{N}$ such that $0 < k < h$.
From 2.4.4 *iv.* $y_m(a) = x_k(a)y_{qh}(a) + x_{qh}(a)y_k(a)$, but by 2.4.4 *v.* $y_h(a) \mid y_{qh}(a)$, so that thanks to the hypothesis it must be $y_h(a) \mid x_{qh}(a)y_k(a)$.
Since $x_{qh}(a)^2 - (a^2 - 1)y_{qh}(a)^2 = 1$, one has $(x_{qh}(a), y_{qh}(a)) = 1$, which also gives $(x_{qh}(a), y_h(a)) = 1$, in particular $y_h(a) \mid y_k(a)$ and so:

$$|N_{L/\mathbb{Q}}(y_h(a))| \leq |N_{L/\mathbb{Q}}(y_k(a))|$$

but, by explicit computation using the hypothesis $|\sigma_i(y_h(a))| \geq 1/2$ and 2.4.5 *iii.*:

$$|N_{L/\mathbb{Q}}(y_h(a))| = |y_h(a)| \prod_{i=2}^{n} |\sigma_i(y_h(a))| \geq |y_h(a)|(1/2)^{n-1} > \frac{\epsilon(a)^h}{4a} \left(\frac{1}{2}\right)^{n-1}$$

and similarly:

$$|N_{L/\mathbb{Q}}(y_k(a))| = |y_k(a)| \prod_{i=2}^{n} |\sigma_i(y_k(a))| \leq |y_k(a)|2^{n-1} < \frac{\epsilon(a)^h}{a} 2^{n-1}$$

and recollecting all the inequalities one obtains $\epsilon(a)^{h-k} < 2^{2n}$, in particular being $k < h$: $a < \epsilon < \epsilon^{h-k} < 2^{2n}$, contradicting $*$.
ii.: by $y_h(a)^2 \mid y_m(a)$ and *i.* one has $h \mid m$, so that $m = hk$.
In particular, by 2.4.4 *vi.*: $y_m(a) = y_{hk}(a) \equiv_{y_h(a)^3} k x_h(a)^{k-1} y_h(a)$, which gives $0 \equiv_{y_h(a)^2} k x_h(a)^{k-1} y_h(a)$, so that $y_h(a) \mid k x_h(a)^{k-1}$, and by $(x_h(a), y_h(a)) = 1$, it must be $y_h(a) \mid k$. □

Again another property that is inherited thanks to $*$.

Lemma 2.4.8. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$, $k, j \in \mathbb{N}$, $m \in \mathbb{N}^+$ such that $|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{2, \dots, n\}$, then:*

$$x_k(a) \equiv_{x_m(a)} \pm x_j(a) \implies k \equiv_m \pm j$$

Proof. By Euclid's algorithm $k = 2mq \pm k_0$ and $j = 2mh \pm j_0$ with $q, h, k_0, j_0 \in \mathbb{N}$ and $k_0, j_0 \leq m$.
By 2.4.4 *x.* $x_k(a) \equiv_{x_m(a)} x_{k_0}(a)$ and $x_j(a) \equiv_{x_m(a)} x_{j_0}(a)$, so without loss of generality one may suppose $1 \leq k, j \leq m$.
In this case, from $x_k(a) \equiv_{x_m(a)} \pm x_j(a)$ it will follow $x_k(a) = \pm x_j(a)$, supposing not, one notices $x_m(a) \mid x_k(a) \pm x_j(a)$ so that $|N_{L/\mathbb{Q}}(x_m(a))| \leq |N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))|$.
Furthermore, one may suppose $x_k(a) > x_j(a)$, so by explicit computation using the hypothesis $|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{2, \dots, n\}$ and 2.4.5 *iv.*:

$$|N_{L/\mathbb{Q}}(x_m(a))| = x_m(a) \prod_{i=2}^{n} |\sigma_i(x_m(a))| \geq x_m(a)(1/2)^{n-1} > \epsilon(a)^m (1/2)^n$$

and similarly:

$$|N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))| \leq (x_k(a) \pm x_j(a)) \prod_{i=2}^{n} (|\sigma_i(x_k(a))| + |\sigma_i(x_j(a))|)$$

so that:

$$|N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))| < 2x_k(a)2^{n-1} \leq \epsilon(a)^k 2^n$$

which recollecting all the inequalities leads to $\epsilon^{m-k} < 2^{2n}$, in particular from 2.4.5 *ii.* $a^{m-k} < 2^{2n}$, but by $*$ it must be $m = k$.
In particular, the congruence is translated in $x_m(a) \mid x_j(a)$, and with the exact same reasoning this leads to $a^{m-j} < 2^n$, and for $j \neq m = k$ this is contradicting $*$, so that it must happen $x_k(a) = \pm x_j(a)$ (if $j = k$ then this is obvious).
By 2.4.4 *vii.* the sequence is increasing in indexes, so it must be $k = j$. □

Finally, to use all the previous extensions of the classical properties of the Pell's equation $x^2 - (a^2 - 1)y^2 = 1$, one must find an algebraic integer $a \in \mathcal{O}_K$ satisfying all those hypotheses starting from $*$.
For this purpose, first it will be recalled a theorem of Kronecker:

Theorem 2.4.9. *$\theta_1, \dots, \theta_k, 1$ $\mathbb{Z}$-linearly independent, $\alpha_1, \dots, \alpha_k \in \mathbb{R}$, $N, \epsilon \in \mathbb{R}^+$, then $\exists n, p_1, \dots, p_k \in \mathbb{Z}$ such that $n > N$ and $|n\theta_m - p_m - \alpha_m| < \epsilon \ \forall m \in \{1, \dots, k\}$.*

Reformulating Kronecker's theorem in its multiplicative version with torus:

$$T \cong \mathbb{R}/\mathbb{Z}, e, k \in \mathbb{N}^+, \overline{v} = (v_1, \dots, v_e) \in T^e : v_1, \dots, v_e \textit{ linearly indipendent in } T$$
$$\implies \{m \cdot \overline{v} : k \mid m\} \textit{ everywhere dense in } T^e$$

one has now the key tool to make 2.4.7 and 2.4.8 concretely useful, as claimed in the following lemma:

Lemma 2.4.10. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$, $k \in \mathbb{N}^+$, then $\exists m, h \in k\mathbb{N}^+$ such that:*

$$|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{2, \dots, n\}$$

$$|\sigma_i(y_h(a))| \geq 1/2 \ \forall i \in \{2, \dots, n\}$$

Proof. With multiplicative notation $T = \{z \in \mathbb{C} : |z| = 1\}$, setting the vector $\overline{v} = (\sigma_{2,1}(\epsilon(a)), \dots, \sigma_{n,1}(\epsilon(a)))$, by 2.4.5 *ii.* one has $\overline{v} \in T^{n-1}$, and from 2.4.4 *iii.* one has $\sigma_i(x_m(a)) = \frac{1}{2}(\sigma_{i,1}(\epsilon(a))^m + \sigma_{i,1}(\epsilon(a))^{-m}) \ \forall i \in \{2, \dots, n\}$ and similarly $\sigma_i(y_m(a)) \geq \frac{1}{2}|(\sigma_{i,1}(\epsilon(a))^m - \sigma_{i,1}(\epsilon(a))^{-m})|$, so it is sufficient to check Kronecker hypothesis of linear independence.
Indeed, supposing $\prod_{i=2}^{n} \sigma_{i,1}(\epsilon(a))^{a_i} = 1$, let τ_j automorphism of $\mathbb{C}$ such that $\tau_j \sigma_{j,1} = \sigma_{1,1}$, then:

$$\epsilon(a)^{a_j} \prod_{i=2, i \neq j}^{n} \sigma_{i,1}(\epsilon(a))^{a_i} = \tau_j(1) = 1$$

but thanks to 2.4.5 *ii.* $|\sigma_{i,1}(\epsilon(a))| = 1$, so it must be $|\epsilon(a)^{a_j}| = 1$ too, in particular $a_j = 0$ and the desired independence is checked. □

In the exactly same way of the classical case in proving the diophantinity of the exponential, one has the need to control as desired the choice of the parameter a, in particular it is useful to combine the property *ix.* of 2.4.4 with the stability of satisfying $*$:

Lemma 2.4.11. *K totally real number field, $a \in \mathcal{O}_K$ satisfying $*$ and such that $|\sigma_i(a)| \leq 1/8 \ \forall i \in \{2, \dots, n\}$, $m \in \mathbb{N}^+$, then $\exists b \in \mathcal{O}_K$ such that:*

i. $b \equiv_{x_m(a)} a$.

ii. $b \equiv_{y_m(a)} 1$.

iii. *b satisfies $*$.*

Proof. For any $s \in \mathbb{N}$ *i.* and *ii.* trivially holds with $b = x_m(a)^{2s} + a(1 - x_m(a)^2)$ by using $x_m(a)^2 - (a^2 - 1)y_m(a)^2 = 1$.
Furthermore, by 2.4.5 *iv.* one has $x_m(a) > 1$ and $|\sigma_i(x_m(a))| < 1 \ \forall i \in \{2, \dots, n\}$, so one could choose any $s \in \mathbb{N}$ sufficiently large such that $b > 2^{2n}$ and also $|\sigma_i(x_m(a)^{2s})| \leq 1/4 \ \forall i \in \{2, \dots, n\}$. □

Lemma 2.4.12. *K number field, $[K : \mathbb{Q}] = n$, $Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, $\xi, z \in \mathcal{O}_K$ and $z \neq 0$:*
$2^{n+1}\xi^n(\xi + 1)^n \dots (\xi + n - 1)^n \mid z \implies |\sigma_i(\xi)| \leq 1/2|N_{L/\mathbb{Q}}(z)|^{1/n} \ \forall i \in \{1, \dots, n\}$.

Proof. Same as 2.3.3. □

Finally, recollecting all the pieces and following the already known system with the right adjustments:

Theorem 2.4.13. *K totally real number field, $Hom_{\mathbb{Q}}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_n\}$, $a \in \mathcal{O}_K$ satisfying:*

$$\sigma_1(a) \geq 2^{2n} \ \wedge \ |\sigma_i(a)| \leq 1/8 \ \forall i \in \{2,\dots,n\} \qquad (**)$$

Define Σ as follows:

$$\Sigma = \begin{cases} I : x^2 - (a^2-1)y^2 = 1 \\ II : w^2 - (a^2-1)z^2 = 1 \\ III : u^2 - (a^2-1)v^2 = 1 \\ IV : s^2 - (b^2-1)t^2 = 1 \\ V : \sigma_1(b) \geq 2^{2n} \\ VI : |\sigma_i(b)| \leq 1/2 \ \forall i \in \{2,\dots,n\} \\ VII : |\sigma_i(z)| \geq 1/2 \ \forall i \in \{2,\dots,n\} \\ VIII : |\sigma_i(u)| \geq 1/2 \ \forall i \in \{2,\dots,n\} \\ IX : v \neq 0 \\ X : z^2 \mid v \\ XI : b \equiv_z 1 \\ XII : b \equiv_u a \\ XIII : s \equiv_u x \\ XIV : t \equiv_z \xi \\ XV : 2^{n+1}\xi^n(\xi+1)^n \dots (\xi+n-1)^n \mid z \\ XVI : 2^{n+1}x^n(x+1)^n \dots (x+n-1)^n \mid z \end{cases}$$

Define $S \subseteq \mathcal{O}_K$ by $\xi \in S \iff \xi \in \mathcal{O}_K \wedge \exists x,y,w,z,u,v,s,t,b \in \mathcal{O}_K$ satisfying Σ.
Then $S \subseteq \mathcal{O}_K$ diophantine and $\mathbb{N}^+ \subseteq S \subseteq \mathbb{Z}$.

Proof. Thanks to 2.1.1 *i.* & *ii.* and to 2.4.2 $S \subseteq \mathcal{O}_K$ is diophantine.
First it will be shown $S \subseteq \mathbb{Z}$. Suppose first $\xi \in S$ so that $\xi \in \mathcal{O}_K$ and $\exists x,y,w,z,u,v,s,t,b \in \mathcal{O}_K$ satisfying Σ.
From $**$ a satisfies $*$, from V and VI b satisfies $*$ too, in particular by 2.4.6 and I-II-III-IV $\exists k,h,m,j \in \mathbb{N}$:

$$x = \pm x_k(a) \qquad y = \pm y_k(a)$$

$$w = \pm x_h(a) \qquad z = \pm y_h(a)$$

$$u = \pm x_m(a) \qquad v = \pm y_m(a)$$

$$s = \pm x_j(b) \qquad t = \pm y_j(b)$$

In particular, from 2.4.4 *viii.* $j \equiv_{b-1} y_j(b) = \pm t$ and by XI it holds $j \equiv_z \pm t$, which combined with XIV leads to $j \equiv_z \pm\xi$.
Furthermore, by 2.4.4 *ix.* and XII one has $x_j(a) \equiv_u x_j(b) = \pm s$ which combined with XIII gives $x_j(a) \equiv_u \pm x = \pm x_k(a)$ so that from 2.4.8 it must be $j \equiv_m \pm k$.
But thanks to X $z^2 = y_h(a)^2 \mid y_m(a) = v$ and so from 2.4.7 *ii.* one has $z = y_h(a) \mid m$, in particular it holds $j \equiv_z \pm k$, and so $k \equiv_z \pm\xi$.
One then notices that from XV and 2.4.10 one has $|\sigma_i(\xi)| \leq 1/2|N_{K/\mathbb{Q}}(z)|^{1/n}$ $\forall i \in \{1, \ldots, n\}$, similarly from XVI and 2.4.10 $k < |\sigma_i(x_k(a))| \leq 1/2|N_{K/\mathbb{Q}}(z)|^{1/n}$ $\forall i \in \{1, \ldots, n\}$, so that:

$$|\sigma_i(\xi \pm k)||\sigma_i(\xi) \pm k| \leq |N_{K/\mathbb{Q}}(z)|^{1/n} \ \forall i \in \{1, \ldots, n\}$$

giving finally $|N_{K/\mathbb{Q}}(\xi \pm k) = \prod_{i=1}^{n} \sigma_i(\xi \pm k)| \leq |N_{K/\mathbb{Q}}(z)|$, which combined with $k \equiv_z \pm\xi$ leads to $\xi = \pm k \in \mathbb{Z}$.
Then it will be shown $\mathbb{N}^+ \subseteq S$. Suppose $\xi \in \mathbb{N}^+$, then the previous part of the proof suggests to define $k = \xi$, $x = x_k(a)$, $y = y_k(a)$ so that I is satisfied.
Defining $\eta = 2^{n+1}\xi^n(\xi+1)^n \ldots (\xi+n-1)^n x^n (x+1)^n \ldots (x+n-1)^n$, by 2.4.4 *xi.* $\exists h_0 \in \mathbb{N}^+$ such that $\eta \mid y_{h_0}(a)$, but then from 2.4.10 $\exists h \in h_0\mathbb{N}^+$ such that $|\sigma_i(y_h(a))| \geq 1/2$ $\forall i \in \{2, \ldots, n\}$, and by 2.4.7 *i.* $y_{h_0}(a) \mid y_h(a)$ so that setting $z = y_h(a)$ VII, XV and XVI are satisfied.
Setting naturally $w = x_h(a)$ II is satisfied too.
Again using 2.4.4 *xi.* $\exists m_0 \in \mathbb{N}^+$ such that $z^2 \mid y_{m_0}(a)$ but then from 2.4.10 $\exists m \in m_0\mathbb{N}^+$ such that $|\sigma_i(y_m(a))| \geq 1/2$ $\forall i \in \{2, \ldots, n\}$, and by 2.4.7 *i.* $y_{m_0}(a) \mid y_m(a)$ so that setting $u = x_m(a)$ and $v = y_m(a)$ III, VIII, IX and X are satisfied.
By 2.4.11 thanks to ** $\exists b \in \mathcal{O}_K$ satisfying V,VI,XI and XII.
Finally, setting $s = x_k(b)$, $t = y_k(b)$ IV is satisfied and thanks to XII and 2.4.4 *ix.* XIII is satisfied too.
From XI combined with 2.4.4 *viii.* XIV follows, in particular $\xi, x, y, w, z, u, v, s, t, b \in \mathcal{O}_K$ are a solution to Σ, so that $\xi \in S$. □

Finally, the proof of the main theorem 2.4.1 is given combining 2.4.13 with 2.4.3.

In the end, putting all together:

Theorem 2.4.14. *K totally real number field or quadratic extension of a totally real number field:*

i. $\mathbb{Z}$ diophantine in $\mathcal{O}_K$.

ii. $S \subseteq \mathcal{O}_K$: S diophantine $\iff$ recursively enumerable.

iii. H10 is unsolvable for $\mathcal{O}_K$.

Proof. i. follows from 2.4.13 and 2.4.3 for the totally real case, and from 2.3.1 the other case, then *ii.* follows from *i.* and 2.1.3, and *iii.* from *i.* and 2.1.2. □

2.5 Pheidas strenghtened procedure

The main goal of the last section of the chapter will be the following theorem due to Pheidas:

Theorem 2.5.1. *Let* K *be a number field with exactly two non real embeddings:* $\mathbb{Z} \subseteq \mathcal{O}_K$ *is diophantine.*

In particular, an immediate corollary:

Corollary 2.5.2. K *number field with exactly two non real embeddings:*

i. $S \subseteq \mathcal{O}_K$*:* S *diophantine* $\iff$ *recursively enumerable.*

ii. H10 is unsolvable for $\mathcal{O}_K$.

Proof. i. follows from 2.5.1 and 2.1.3, and *ii.* from *i.* and 2.1.2. □

For such purpose the strategy will follow ideas close to the ones used by Denef and Lipshitz, but here an immediate example of a class of such new number fields:

Corollary 2.5.3. *Let* $K = \mathbb{Q}(d)$ *where* $d \notin \mathbb{Q}$ *and* $d^3 \in \mathbb{Q}$*, then* $\mathbb{Z} \subseteq \mathcal{O}_K$ *is diophantine.*

Suppose for the rest of the section K number field with exactly two non real embeddings, so that $[K : \mathbb{Q}] = n \geq 3$ and $Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_{n-1}, \sigma_n\}$ where σ_{n-1}, σ_n are the non real embeddings and σ_1 is the canonical inclusion. Noticing that the embedding $\sigma := \overline{\sigma_n}$ is non real, then it must be $\sigma = \sigma_{n-1}$. In particular, there could be only two different cases: $\sigma_{n-1}(K) = \sigma_n(K)$ or $\sigma_{n-1}(K) \neq \sigma_n(K)$.
In the first case, by the Primitive Element theorem let $b \in K$ such that $K = \mathbb{Q}(b)$, in particular $\sigma_n(K) = \mathbb{Q}(\sigma_n(b))$ so that thanks to the hypothesis one trivially has $[\sigma_n(K) : \sigma_n(K) \cap \mathbb{R}] = 2$, where $\sigma_n(K)$ is a non totally real quadratic extension of the totally real number field $\sigma_n(K) \cap \mathbb{R}$, in particular by Denef-Lipshitz result $\mathbb{Z} \subseteq \mathcal{O}_{\sigma_n(K)} = \sigma_n(\mathcal{O}_K)$ is diophantine, so as well $\mathbb{Z} \subseteq \mathcal{O}_K$.

By the previous reasoning, it will be considered just the case $\sigma_{n-1}(K) \neq \sigma_n(K)$, and supposing $a \in \mathcal{O}_K$ such that:

$$|\sigma_i(a)| \leq 1/2^{4n} \ \forall i \in \{1, \dots, n-2\} \qquad (***)$$

so that $a \notin \mathbb{Z}$ and $\delta(a) \notin K$, define $L = K(\delta(a))$ quadratic extension of K with the embeddings $Hom_{\mathbb{Q}}(L, \mathbb{C}) = \{\sigma_{i,1}, \sigma_{i,2} : i \in \{1, \dots, n\}\}$.
In particular, one has $\sigma_{i,1}(\delta(a)) = \pm\sqrt{\sigma_i(a)^2 - 1}$ and $\sigma_{i,2}(\delta(a)) = -\sigma_{i,1}(\delta(a))$.
Next lemma will play an analogous role as the trivial bounds in the path to obtain Denef-Lipshitz result using the strenghtened bounds in $***$:

Lemma 2.5.4. *$[K : \mathbb{Q}] = n \geq 3$ number field, $Hom_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_{n-1}, \sigma_n\}$ where σ_{n-1}, σ_n are the unique non real embeddings, $a \in \mathcal{O}_K$ satisfying $***$, then $\forall i \in \{1, \dots, n-2\}, \forall j \in \{1, 2\}$:*

i. $0 < |\sigma_i(a)| < 1/2^{4n}$, $|\sigma_{n-1}(a)| = |\sigma_n(a)| \geq 2^{2n}$.

ii. $|\sigma_{i,j}(\epsilon(a))| = 1$.

iii. $|\sigma_{n-1,j}(\epsilon(a))| \neq 1$, $|\sigma_{n,j}(\epsilon(a))| \neq 1$ *and*

$$max(|\sigma_{n-1,1}(\epsilon(a))|, |\sigma_{n-1,2}(\epsilon(a))|) = max(|\sigma_{n,1}(\epsilon(a))|, |\sigma_{n,2}(\epsilon(a))|) > 2^{2n}$$

Proof. *i.* Since $\sigma_{n-1} = \overline{\sigma_n}$ then $|\sigma_{n-1}(a)| = |\sigma_n(a)|$.
Furthermore, being $a \neq 0$, then $N_{K/\mathbb{Q}}(a) \in \mathbb{Z} \setminus \{0\}$, so that $|\prod_{i=1}^n \sigma_i(a)| \neq 0$, in particular using $***$ one has $0 < |\sigma_i(a)| < 1/2^{4n}$.
Finally, from $|\prod_{i=1}^n \sigma_i(a)| \geq 1$ and $0 < |\sigma_i(a)| < 1/2^{4n}$, one immediately obtains $|\sigma_{n-1}(a) \cdot \sigma_n(a)| = |\sigma_n(a)|^2 > 2^{4n(n-2)}$, and being $n \geq 3$ then $4n(n-2) \geq 4n$, so that $|\sigma_{n-1}(a)| = |\sigma_n(a)| \geq 2^{2n}$.
ii. $|\sigma_{i,j}(\epsilon(a))|^2 = |\sigma_i(a) + \sigma_{i,j}(\delta(a))|^2$, but since $\forall i \in \{1, \dots, n-2\} : |\sigma_i(a) < 1|$, then $\sigma_{i,j}(\delta(a)) \in i\mathbb{R}$, so that:

$$|\sigma_{i,j}(\epsilon(a))|^2 = |\sigma_i(a) + \sigma_{i,j}(\delta(a))|^2 = \sigma_i(a)^2 + |\sigma_{i,j}(\delta(a))|^2 = 1$$

iii. From $\sigma_{n,1}(\epsilon(a)) + \sigma_{n,2}(\epsilon(a)) = 2\sigma_n(a)$ so that:

$$|\sigma_{n,1}(\epsilon(a))| + |\sigma_{n,2}(\epsilon(a))| \geq |\sigma_{n,1}(\epsilon(a)) + \sigma_{n,2}(\epsilon(a))| = |2\sigma_n(a)| \geq 2^{2n+1}$$

Concluding by $2max(|\sigma_{n-1,1}(\epsilon(a))|, |\sigma_{n-1,2}(\epsilon(a))|) \geq |\sigma_{n,1}(\epsilon(a))| + |\sigma_{n,2}(\epsilon(a))|$ and $|\sigma_n| = |\sigma_{n-1}|$. □

Remark 2.5.5. Thanks to 2.5.4 *iii.* one may suppose for the rest of the section that $|\sigma_{n-1,1}(\epsilon(a))| > 2^{2n}$ and $|\sigma_{n,1}(\epsilon(a))| > 2^{2n}$.

Remark 2.5.6. Noticing that $\lim_{n\to\infty}\varphi(n)$, then it is well-defined:

$$d := lcm\{ord(\xi) : \xi \in \mu(\overline{\mathbb{Q}}) \wedge ord(\xi) \leq 2n\}$$

Lemma 2.5.7. *Let K number field with two non real embeddings, a satisfying $***$, $\delta(a) = \sqrt{a^2-1}$, d as in 2.5.6, defining the sets:*

$$S = \{(x,y) \in \mathcal{O}_K^2 : x^2 - (a^2-1)y^2 = 1\}$$

$$T = \{(\pm x_m(a), \pm y_m(a)) \in \mathcal{O}_K^2 : x_m(a) + y_m(a)\delta(a) = \epsilon(a)^m \wedge m \in \mathbb{N}\}$$

$$R = \{(x,y) \in S : \exists(\overline{x},\overline{y}) \in S : x + y\delta(a) = (\overline{x} + \overline{y}\delta(a))^{6d}\}$$

Then $R \subseteq T$.

Proof. By Dirichlet's theorem on units, K has $n-2$ fundamental units, and, being $[L:K] = 2$ and having L no real embeddings, L has $n-1$ fundamental units.
Considering the set $Q = \{x + y\delta(a) : (x,y) \in S\}$, then since $\forall u \in \mathcal{O}_K^* : N_{L/K}(u) = u^2$, the image of $N_{L/K_{|\mathcal{O}_L\setminus\{0\}}}$ has free rank at least $n-2$, in particular $Q = Ker(N_{L/K_{|\mathcal{O}_L\setminus\{0\}}} : \mathcal{O}_L \setminus \{0\} \to \mathcal{O}_K \setminus \{0\})$ has at most free rank 1,but $\epsilon(a) \in Q$ and torsion free, so that $rank(Q) = 1$.
Hence, there exists $\epsilon_0 = x_0 + y_0\delta(a) \in Q$ fundamental unit such that $\forall u \in Q : \exists J \in \mu(\mathcal{O}_L) \wedge \exists m \in \mathbb{Z} : u = J\epsilon_0^m$, in particular $\epsilon(a) = J_0\epsilon_0^e$ for a certain $J_0 \in \mu\mathcal{O}_L$ (so $J_0^d = 1$) and $e \in \mathbb{Z}\setminus\{0\}$ since $\epsilon(a) \notin \mu(\mathcal{O}_L)$, and without loss of generality one may suppose $e > 0$ (if necessary replacing the role of ϵ_0 with ϵ_0^{-1}).
By $\epsilon_0 - \epsilon_0^{-1} = 2y_o\delta(a)$, $2\delta(a) \mid (\epsilon_0 - \epsilon_0^{-1})$, so $|N_{L/K}(2\delta(a))| \leq |N_{L/K}(\epsilon_0 - \epsilon_0^{-1})|$.
Furthermore, recalling $\overline{\sigma_n(a)} = \sigma_{n-1}(a)$ and so $\overline{\sigma_{n-1}(a)^2 - 1} = \overline{\sigma_{n-1}(a)}^2 - 1 = \sigma_n(a)^2 - 1$, and by explicit computation:

$$N_{L/\mathbb{Q}}(2\delta(a)) = 2^{2n}N_{L/\mathbb{Q}}(\delta(a)) = 2^{2n}\left|\prod_{i=1}^{n-2}(\sigma_i(a)^2 - 1)\right||\sigma_n(a)^2 - 1|^2$$

So that:

$$N_{L/\mathbb{Q}}(2\delta(a)) \geq 2^{2n}(1 - 1/2^{8n})^{n-1}|\sigma_n(a)^2 - 1|^2 > 2^{2n}(1/2^2)^{n-1}|\sigma_n(a)^2 - 1|^2$$

$$N_{L/\mathbb{Q}}(2\delta(a)) > 2^4|\sigma_n(a)^2 - 1|^2 \geq 2^4|\sigma_n(a)^2 - 1| \geq 2^3|\sigma_n(a)|^2$$

Also, noticing that it holds $\sigma_{n-1,1}(\epsilon_0) = \sigma_{n-1}(x_0) + \sigma_{n-1}(y_0)\sigma_{n-1,1}(\delta(a))$ and $\sigma_{n-1,2}(\epsilon_0) = \sigma_{n-1}(x_0) - \sigma_{n-1}(y_0)\sigma_{n-1,1}(\delta(a)) = \sigma_{n-1,1}(\epsilon_0^{-1})$, then:

$$|\sigma_{n-1,1}(\epsilon_0) - \sigma_{n-1,1}(\epsilon_0^{-1})| \cdot |\sigma_{n-1,2}(\epsilon_0) - \sigma_{n-1,2}(\epsilon_0^{-1})| = |\sigma_{n-1,1}(\epsilon_0) - \sigma_{n-1,1}(\epsilon_0^{-1})|^2$$

and similarly for $\sigma_{n,1}, \sigma_{n,2}$.
Furthermore:

$$(\sigma_{j,1}(\epsilon_0) - \sigma_{j,1}(\epsilon_0^{-1}))^2 = 4(\sigma_j(a)^2 - 1)\sigma_j(y_0)^2$$

From the relation $|\sigma_{j,1}(\epsilon_0)|^e = \sigma_{j,1}(\epsilon(a)) > 1 \; \forall j \in \{n-1, n\}$, then since $e > 0$ also $\sigma_{j,1}(\epsilon_0) > 1 \; \forall j \in \{n-1, n\}$.
In particular, an explicit computation gives:

$$|N_{L/K}(\epsilon_0 - \epsilon_0^{-1})| = \Big| \prod_{\substack{i=1 \\ j=1,2}}^{n} |(\sigma_{i,j}(\epsilon_0) - \sigma_{i,j}(\epsilon_0^{-1}))| \Big|$$

But by 2.5.4 *ii.* $|(\sigma_{i,j}(\epsilon_0) - \sigma_{i,j}(\epsilon_0^{-1}))| \leq |(\sigma_{i,j}(\epsilon_0)| + |\sigma_{i,j}(\epsilon_0^{-1}))| \leq 1 + 1 = 2 \; \forall i \in \{1, \dots, n-2\}$:

$$|N_{L/K}(\epsilon_0 - \epsilon_0^{-1})| \leq 2^{2n-4} |(\sigma_{n,1}(\epsilon_0) - \sigma_{n,1}(\epsilon_0^{-1}))|^4$$

Also

$$|\sigma_{n,1}(\epsilon_0) - \sigma_{n,1}(\epsilon_0^{-1})|^2 = |\sigma_{n,1}(\epsilon_0)^2 + \sigma_{n,1}(\epsilon_0^{-1})^2 - 2|$$
$$\leq |\sigma_{n,1}(\epsilon_0)|^2 + |\sigma_{n,1}(\epsilon_0^{-1})|^2 - 2 \leq 2(|\sigma_{n,1}(\epsilon_0)|^2 + |\sigma_{n,1}(\epsilon_0^{-1})|^2)$$

So that $|(\sigma_{n,1}(\epsilon_0) - \sigma_{n,1}(\epsilon_0^{-1}))|^4 \leq 4(|\sigma_{n,1}(\epsilon_0)|^2 + |\sigma_{n,1}(\epsilon_0^{-1})|^2)^2$, and in particular with the same reasoning $|(\sigma_{n,1}(\epsilon_0) - \sigma_{n,1}(\epsilon_0^{-1}))|^4 \leq 8(|\sigma_{n,1}(\epsilon_0)|^4 + |\sigma_{n,1}(\epsilon_0^{-1})|^4)$.
Hence, $|N_{L/K}(\epsilon_0 - \epsilon_0^{-1})| \leq 2^{2n-1}(|\sigma_{n,1}(\epsilon_0)|^4 + |\sigma_{n,1}(\epsilon_0^{-1})|^4) \leq 2^{2n}|\sigma_{n,1}(\epsilon_0)|^4$ since $\sigma_{n,1}(\epsilon_0) > 1$.
Finally, supposing by absurd that $e \geq 4$, then:

$$|N_{L/K}(\epsilon_0 - \epsilon_0^{-1})| \leq 2^{2n}|\sigma_{n,1}(\epsilon_0)|^4 \leq 2^{2n}|\sigma_{n,1}(\epsilon(a))|$$

But:

$$|\sigma_{n,1}(\epsilon(a) = a + \delta(a))| \leq |\sigma_{n,1}(a)| + \sqrt{|\sigma_{n,1}(a)^2 - 1|} \leq 4|\sigma_{n,1}(a)|$$

reaching finally $|N_{L/K}(\epsilon_0 - \epsilon_0^{-1})| \leq 4|\sigma_{n,1}(a)|$, but combining this with the previous bounds $|N_{L/K}(2\delta(a))| \leq |N_{L/K}(\epsilon_0 - \epsilon_0^{-1})|$ and $N_{L/\mathbb{Q}}(2\delta(a)) > 2^2|\sigma_n(a)|^2$, it turns out $2^2|\sigma_n(a)|^2 < 2^{2n+2}|\sigma_{n,1}(a)|$, equivalently $|\sigma_n(a)| < 2^{2n}$ contradicting 2.5.4 *i.*.
In particular, $e \leq 3$, so that supposing $(x, y) \in R$, so that $\exists \overline{x}, \overline{y} \in S : x + y\delta(a) = (\overline{x} + \overline{y}\delta(a))^{6d}$, then $\exists m \in \mathbb{Z} \wedge \overline{J} \in \mu(\mathcal{O}_L) : \overline{x} + \overline{y}\delta(a) = \overline{J}\epsilon_0^m$, in particular, since $\overline{J}^d = 1$, defining $k = |6nd/e|$, then $k \in \mathbb{N}$ for $e \leq 3$ and so $x + y\delta(a) = \epsilon_0^{6md} = \epsilon(a)^{\pm k}$, so that $x = \pm x_k(a), y = \pm y_k(a)$, and $(x, y) \in T$. □

Lemma 2.5.8. *Let K number field with two non real embeddings, a satisfying* ∗∗∗, *$h, m \in \mathbb{N}$ such that $|\sigma_i(y_h(a))| \geq 1/2 \ \forall i \in \{1, \dots, n-2\}$, then:*

i. $|\sigma_n(y_h(a))| > |\sigma_{n,1}(\epsilon(a))|^h/4|\sigma_{n,1}(\delta(a))| \wedge |\sigma_{n,1}(\epsilon(a))| > 2^{2n}$.

ii. $y_h(a) \mid y_m(a) \iff h \mid m$.

iii. $y_h(a)^2 \mid y_m(a) \implies h y_h(a) \mid m$.

Proof. *i.*: $|\sigma_{n,1}(\epsilon(a))| > 2^{2n}$ follows from 2.5.4 *iii.* and the choice of indexing established in 2.5.5.
Thanks to this inequality, it trivially follows $|\sigma_{n,1}(\epsilon(a))|^h - |\sigma_{n,1}(\epsilon(a))|^{-h} \geq |\sigma_{n,1}(\epsilon(a))|^h/\sqrt{2} \ \forall h \in \mathbb{N}^+$, so that:

$$|\sigma_{n,1}(y_k(a))| = \frac{|\sigma_{n,1}(\epsilon(a))^h - \sigma_{n,1}(\epsilon(a))^{-h}|}{2|\sigma_{n,1}(\delta(a))|} \geq \frac{|\sigma_{n,1}(\epsilon(a))|^h}{2\sqrt{2}|\sigma_{n,1}(\delta(a))|} > \frac{|\sigma_{n,1}(\epsilon(a))|^h}{4|\sigma_{n,1}(\delta(a))|}$$

ii.: ($\Longleftarrow$) is given by the properties of Pell's equation 2.4.4 *v.*.
($\Longrightarrow$): by absurd suppose $h \nmid m$ so that $m = qh + k$ for certain $q, k \in \mathbb{N}$ such that $0 < k < h$.
From the addition formula 2.4.4 *iv.* $y_m(a) = x_k(a)y_{qh}(a) + x_{qh}(a)y_k(a)$, but by 2.4.4 *v.* $y_h(a) \mid y_{qh}(a)$, so that thanks to the hypothesis it must be $y_h(a) \mid x_{qh}(a)y_k(a)$.
Since $x_{qh}(a)^2 - (a^2-1)y_{qh}(a)^2 = 1$, one has $(x_{qh}(a), y_{qh}(a)) = 1$, which also gives $(x_{qh}(a), y_h(a)) = 1$, in particular $y_h(a) \mid y_k(a)$ and so:

$$|N_{L/\mathbb{Q}}(y_h(a))| \leq |N_{L/\mathbb{Q}}(y_k(a))|$$

but, by explicit computation using the hypothesis $|\sigma_i(y_h(a))| \geq 1/2$:

$$|N_{L/\mathbb{Q}}(y_h(a))| = \prod_{i=1}^{n-2} |\sigma_i(y_h(a))||\sigma_{n-1}(y_h(a))||\sigma_n(y_h(a))| \geq (1/2)^{n-2}|\sigma_n(y_h(a))|^2$$

Giving thanks to *i.*:

$$|N_{L/\mathbb{Q}}(y_h(a))| > \frac{|\sigma_{n,1}(\epsilon(a))|^{2h}}{4|\sigma_{n,1}(\delta(a))|^2}\left(\frac{1}{2}\right)^{n-1}$$

But from $\sigma_i(x_k(a))^2 - (\sigma_i(a)^2 - 1)\sigma_i(y_k(a))^2 = 1$ and $\forall i \in \{1, \dots, n-2\}$: $|\sigma_i(a)| < 1$, then also $\forall i \in \{1, \dots, n-2\} : |\sigma_i(y_k(a))| < 1$ and so:

$$|N_{L/\mathbb{Q}}(y_k(a))| = \prod_{i=1}^{n-2} |\sigma_i(y_k(a))||\sigma_{n-1}(y_k(a))||\sigma_n(y_k(a))| < |\sigma_n(y_k(a))|^2$$

But:

$$|\sigma_{n,1}(y_k(a))| = \frac{|\sigma_{n,1}(\epsilon(a))^k - \sigma_{n,1}(\epsilon(a))^{-k}|}{2|\sigma_{n,1}(\delta(a))|} \leq \frac{|\sigma_{n,1}(\epsilon(a))^k|}{|\sigma_{n,1}(\delta(a))|}$$

So that:

$$|N_{L/\mathbb{Q}}(y_k(a))| < \frac{|\sigma_{n,1}(\epsilon(a))|^{2k}}{|\sigma_{n,1}(\delta(a))|^2}$$

and recollecting all the inequalities one obtains:

$$\frac{|\sigma_{n,1}(\epsilon(a))|^{2h}}{4|\sigma_{n,1}(\delta(a))|^2}\left(\frac{1}{2}\right)^{n-1} < |N_{L/\mathbb{Q}}(y_h(a))| \leq |N_{L/\mathbb{Q}}(y_k(a))| < \frac{|\sigma_{n,1}(\epsilon(a))|^{2k}}{|\sigma_{n,1}(\delta(a))|^2}$$

$|\sigma_{n,1}(\epsilon(a))|^{h-k} < 2^n$, contradicting *i.* being $k < h$.
iii.: by $y_h(a)^2 \mid y_m(a)$ and *i.* one has $h \mid m$, so that $m = hk$.
By 2.4.4 *vi.*: $y_m(a) = y_{hk}(a) \equiv_{y_h(a)^3} kx_h(a)^{k-1}y_h(a)$, which gives $0 \equiv_{y_h(a)^2} kx_h(a)^{k-1}y_h(a)$, so that $y_h(a) \mid kx_h(a)^{k-1}$, and knowing that $(x_h(a), y_h(a)) = 1$, it must be $y_h(a) \mid k$. □

Lemma 2.5.9. *Let K number field with two non real embeddings, a satisfying* $***$, *$k, j \in \mathbb{N}$, $m \in \mathbb{N}^+$ such that $|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{1, \ldots, n-2\}$, then:*

$$x_k(a) \equiv_{x_m(a)} \pm x_j(a) \implies k \equiv_m \pm j$$

Proof. By Euclid's algorithm $k = 2mq \pm k_0$ and $j = 2mh \pm j_0$ with $q, h, k_0, j_0 \in \mathbb{N}$ and $k_0, j_0 \leq m$.
By 2.4.4 *x.* $x_k(a) \equiv_{x_m(a)} x_{k_0}(a) \wedge x_j(a) \equiv_{x_m(a)} x_{j_0}(a)$, so without loss of generality one may suppose $1 \leq k, j \leq m$.
In this case, from $x_k(a) \equiv_{x_m(a)} \pm x_j(a)$ it will follow $x_k(a) = \pm x_j(a)$, supposing not, by $x_m(a) \mid x_k(a) \pm x_j(a)$ one has $|N_{L/\mathbb{Q}}(x_m(a))| \leq |N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))|$.
Furthermore, one may suppose $|\sigma_n(x_k(a))| > |\sigma_n(x_j(a))|$, so by explicit computation using the hypothesis $|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{1, \ldots, n-2\}$:

$$|N_{L/\mathbb{Q}}(x_m(a))| = \prod_{i=1}^{n-2} |\sigma_i(x_m(a))| |\sigma_n(x_m(a))|^2 \geq |\sigma_n(x_m(a))|^2 \left(\frac{1}{2}\right)^{n-2}$$

But also $|\sigma_n(x_m(a))| = \frac{|\sigma_{n,1}(\epsilon(a))^m + \sigma_{n,1}(\epsilon(a))^{-m}|}{2}$ so that:

$$|\sigma_n(x_m(a))|^2 \geq \frac{(|\sigma_{n,1}(\epsilon(a))|^m - |\sigma_{n,1}(\epsilon(a))|^{-m})^2}{4} > \frac{|\sigma_{n,1}(\epsilon(a))|^{2m}}{8}$$

Hence, it follows $|N_{L/\mathbb{Q}}(x_m(a))| > \left(\frac{1}{2}\right)^{n+1} |\sigma_{n,1}(\epsilon(a))|^{2m}$.
Similarly:

$$|N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))| \leq \prod_{i=1}^{n-2} (|\sigma_i(x_k(a))| + |\sigma_i(x_j(a))|)(|\sigma_n(x_k(a))| + |\sigma_n(x_j(a))|)^2$$

$$< |2\sigma_n(x_k(a))|^2 2^{n-2} \leq 2^n |\sigma_{n,1}(\epsilon(a))|^{2k}$$

which recollecting all the inequalities leads to:

$$\frac{|\sigma_{n,1}(\epsilon(a))|^{2m}}{2^{n+1}} < |N_{L/\mathbb{Q}}(x_m(a))| \leq |N_{L/\mathbb{Q}}(x_k(a) \pm x_j(a))| < 2^n |\sigma_{n,1}(\epsilon(a))|^{2k}$$

In particular, $|\sigma_{n,1}(\epsilon(a))|^{2m-2k} < 2^{2n+1}$, so that $|\sigma_{n,1}(\epsilon(a))|^{m-k} < 2^{n+1}$, and if $m \neq k$, then the inequality would contradict 2.5.8 *i.*, so it must be $m = k$. In particular, the congruence is translated in $x_m(a) \mid x_j(a)$, and with the exact same reasoning this leads to $|\sigma_{n,1}(\epsilon(a))|^{m-k} < 2^{n+1}$, and for $j \neq m = k$ this is contradicting 2.5.8 *i.*, so that it must happen $x_k(a) = \pm x_j(a)$.
If $x_k(a) = x_j(a)$, then $\epsilon(a)^k + \epsilon(a)^{-k} = \epsilon(a)^j + \epsilon(a)^{-j}$, in particular it holds $\epsilon(a)^k - \epsilon(a)^j = \epsilon(a)^{-j} - \epsilon(a)^{-k}$, hence $\epsilon(a)^k(1-\epsilon(a)^{j-k}) = \epsilon(a)^{-j}(1-\epsilon(a)^{j-k})$, giving $(\epsilon(a)^k - \epsilon(a)^{-j})(1 - \epsilon(a)^{k-j}) = 0$, implying $(\epsilon(a)^k - \epsilon(a)^{-j}) = 0$ and so $k = -j$, or $(1 - \epsilon(a)^{k-j}) = 0$ and it must be $k = j$.
Similarly if $x_k(a) = -x_j(a)$. □

Lemma 2.5.10. *Let K number field with two non real embeddings, a satisfying* $***$ *and such that $\sigma_{n,1}(\epsilon(a))/\sigma_{n-1,1}(\epsilon(a)) \notin \mu(\overline{\mathbb{Q}})$, $k \in \mathbb{N}^+$, then $\exists m, h \in k\mathbb{N}^+$ such that:*

$$|\sigma_i(x_m(a))| \geq 1/2 \ \forall i \in \{1, \dots, n-2\}$$

$$|\sigma_i(y_h(a))| \geq 1/2 \ \forall i \in \{1, \dots, n-2\}$$

Proof. With multiplicative notation $T = \{z \in \mathbb{C} : |z| = 1\}$, setting the vector $\overline{v} = (\sigma_{2,1}(\epsilon(a)), \dots, \sigma_{n,1}(\epsilon(a)))$, by 2.5.4 *ii.* one has $\overline{v} \in T^{n-1}$, and from 2.4.4 *iii.* one has $\sigma_i(x_m(a)) = \frac{1}{2}(\sigma_{i,1}(\epsilon(a))^m + \sigma_{i,1}(\epsilon(a))^{-m}) \ \forall i \in \{1, \dots, n-2\}$ and similarly $\sigma_i(y_m(a)) \geq \frac{1}{2}|(\sigma_{i,1}(\epsilon(a))^m - \sigma_{i,1}(\epsilon(a))^{-m})|$, so it is sufficient to check Kronecker hypothesis of linear independence thanks to 2.4.1.
Indeed, supposing $\prod_{i=1}^{n-2} \sigma_{i,1}(\epsilon(a))^{a_i} = 1$, let K_1 normal closure of K and L_1 normal closure of L so that $K_1 \subseteq L_1$, suppose $\forall j \in \{1, \dots, n-2\} \exists \tau_j$ automorphism of K_1 such that $\tau_j \sigma_{n-1} = \sigma_j$ and $\tau_j \sigma_j = \sigma_{n-1}$ and $\tau_j \sigma_i = \sigma_i \ \forall i \in \{1, \dots, n\} \setminus \{j, n-1\}$, then applying to both sides an extension of τ_j in L_1:

$$\epsilon(a)^{a_j} \prod_{i=1, i \neq j}^{n-2} \sigma_{i,1}(\epsilon(a))^{a_i} = \tau_j(1) = 1$$

but thanks to 2.5.4 *ii.* $|\sigma_{i,1}(\epsilon(a))| = 1$, so it must be $|\epsilon(a)^{a_j}| = 1$ too, in particular $a_j = 0$ and the desired independence is checked.
To verify the existence of such automorphism τ_j, first it will be proved the following claim: $\sigma_{n-1}(K) \nsubseteq \sigma_1(K) \dots \sigma_{n-2}(K)\sigma_n(K)$.
Indeed, since $\sigma_{n-1}(K) \neq \sigma_n(K)$, there exists a non trivial extension of the

identity of $\sigma_n(K)$ to $\sigma_{n-1}(K)\sigma_n(K)$, which extends to a $\overline{\tau}$ automorphism of K_1.
Since $\overline{\tau}_{|_{\sigma_n(K)}} = 1_{|_{\sigma_n(K)}}$ and $\overline{\tau}_{|_{\sigma_{n-1}(K)}} \neq 1_{|_{\sigma_{n-1}(K)}}$, then $\overline{\tau}\sigma_{n-1} \neq \sigma_{n-1}$ so as $\overline{\tau}\sigma_{n-1} \neq \sigma_n$, in particular it follows that $\overline{\tau}\sigma_{n-1}$ is a real embedding σ_{i_0} for a certain $i_0 \in \{1, \dots, n-2\}$, and thanks to the conjunction $= (\sigma_{n-1}, \sigma_n)$, one obtains the transposition $\overline{\tau}(\sigma_{n-1}, \sigma_n)\overline{\tau}^{-1} = (\sigma_{i_0}, \sigma_n)$.
Finally, assuming by absurd $\sigma_{n-1}(K) \subseteq \sigma_1(K) \dots \sigma_{n-2}(K)\sigma_n(K)$, then applying the transposition it happens $\sigma_{n-1}(K) \subseteq \sigma_1(K) \dots \sigma_{n-2}(K)$, which is impossible being σ_{n-1} non real and σ_i real $\forall i \in \{1, \dots, n-2\}$, so the claim follows.
In particular, considering the extension E_j/F_j, where:

$$E_j = \sigma_{n-1}(K)\sigma_1(K) \dots \sigma_{j-1}(K)\sigma_{j+1}(K) \dots \sigma_{n-2}(K)\sigma_n(K)$$

$$F_j = \sigma_1(K) \dots \sigma_{j-1}(K)\sigma_{j+1}(K) \dots \sigma_{n-2}(K)\sigma_n(K)$$

then it cannot be a trivial extension thanks to the claim, so that there exists a non trivial extension of the identity of F_j to E_j, which extends to a τ_j automorphism of K_1.
Since $\tau_{j_{|_{F_j}}} = 1_{|_{F_j}}$, it happens that $\tau_j\sigma_i = \sigma_i \ \forall i \in \{1, \dots, n\} \setminus \{j, n-1\}$, but having also $\tau_{j_{|_{E_j}}} \neq 1_{|_{E_j}}$, then $\tau_j\sigma_{n-1} \neq \sigma_{n-1}$, so that it must be $\tau_j\sigma_{n-1} = \sigma_j$ and $\tau_j\sigma_j = \sigma_{n-1}$ as desired.

□

Lemma 2.5.11. *Let K number field with two non real embeddings, a satisfying* $***$, *and such that $|\sigma_i(a)| \leq 1/2^{8n}$ $\forall i \in \{1, \dots, n-2\}$, $m \in \mathbb{N}^+$, then $\exists b \in \mathcal{O}_K$ such that:*

i. $b \equiv_{x_m(a)} a$.

ii. $b \equiv_{y_m(a)} 1$.

iii. b *satisfies* $***$.

Proof. For any $s \in \mathbb{N}$ *i.* and *ii.* trivially holds with $b = x_m(a)^{2s} + a(1 - x_m(a)^2)$ by using $x_m(a)^2 - (a^2 - 1)y_m(a)^2 = 1$.
Furthermore, since $|\sigma_i(x_m(a))| < 1 \ \forall i \in \{1, \dots, n-2\}$ and $|\sigma_{n-1}(x_m(a))| \cdot |\sigma_n(x_m(a))| = |\sigma_n(x_m(a))|^2 \geq 1$, one could choose any $s \in \mathbb{N}$ sufficiently large such that $|\sigma_i(x_m(a)^{2s})| \leq 1/2^{8n}$ $\forall i \in \{1, \dots, n-2\}$.
In particular, $\forall i \in \{1, \dots, n-2\}$:

$$|\sigma_i(b)| \leq |\sigma_i(x_m(a)^{2s})| + |\sigma_i(a)| \cdot |1 - \sigma_i(x_m(a))^2| \leq 1/2^{8n} + 1/2^{8n} \leq 1/2^{4n}$$

□

Finally, recollecting everything:

Theorem 2.5.12. *K number field with two non real embeddings, $Hom_{\mathbb{Q}}(K,\mathbb{C}) = \{\sigma_1,\dots,\sigma_{n-1},\sigma_n\}$ with σ_{n-1},σ_n non real, $a \in \mathcal{O}_K$ satisfying:*

$$|\sigma_i(a)| \leq 1/2^{8n} \ \forall i \in \{1,\dots,n-2 \qquad (****)$$

Let d be as in 2.5.6, and define Σ as follows:

$$\Sigma = \begin{cases} I : \overline{x}^2 - (a^2-1)\overline{y}^2 = 1 \\ II : \overline{w}^2 - (a^2-1)\overline{z}^2 = 1 \\ III : \overline{u}^2 - (a^2-1)\overline{v}^2 = 1 \\ IV : \overline{s}^2 - (b^2-1)\overline{t}^2 = 1 \\ V : x + y\delta(a) = (\overline{x} + \overline{y}\delta(a))^{6d} \\ VI : w + z\delta(a) = (\overline{w} + \overline{z}\delta(a))^{6d} \\ VII : u + v\delta(a) = (\overline{u} + \overline{v}\delta(a))^{6d} \\ VIII : s + t\delta(b) = (\overline{s} + \overline{t}\delta(b))^{6d} \\ IX : |\sigma_i(b)| < 1/2^{4n} \ \forall i \in \{1,\dots,n-2\} \\ X : |\sigma_i(z)| \geq 1/2 \ \forall i \in \{1,\dots,n-2\} \\ XI : |\sigma_i(u)| \geq 1/2 \ \forall i \in \{2,\dots,n\} \\ XII : v \neq 0 \\ XIII : z^2 \mid v \\ XIV : b \equiv_z 1 \\ XV : b \equiv_u a \\ XVI : s \equiv_u x \\ XVII : t \equiv_z \xi \\ XVIII : 2^{n+1}\xi^n(\xi+1)^n \dots (\xi+n-1)^n \mid z \\ XIX : 2^{n+1}x^n(x+1)^n \dots (x+n-1)^n \mid z \end{cases}$$

Define $S \subseteq \mathcal{O}_K$ by $\xi \in S \iff \exists x,y,w,z,u,v,s,t,\overline{x},\overline{y},\overline{w},\overline{z},\overline{u},\overline{v},\overline{s},\overline{t},b \in \mathcal{O}_K$ satisfying Σ.
Then $S \subseteq \mathcal{O}_K$ diophantine and $\mathbb{N}^+ \subseteq S \subseteq \mathbb{Z}$.

Proof. Thanks to 2.1.1 *i.* & *ii.* and to 2.4.2 the diophantinity of the intersection and of the order $S \subseteq \mathcal{O}_K$ is diophantine.
First it will be shown $S \subseteq \mathbb{Z}$. Suppose first $\xi \in S$ so that $\xi \in \mathcal{O}_K \wedge \exists x,y,w,z,u,v,s,t,b \in \mathcal{O}_K$ satisfying Σ.
From $****$ a satisfies $***$, from IX b satisfies $***$ too, in particular by 2.5.7 and I-II-III-IV-V-VI-VII-VIII $\exists k,h,m,j \in \mathbb{N}$:

$$x = \pm x_k(a) \qquad y = \pm y_k(a)$$

$$w = \pm x_h(a) \qquad z = \pm y_h(a)$$

$$u = \pm x_m(a) \qquad v = \pm y_m(a)$$
$$s = \pm x_j(b) \qquad t = \pm y_j(b)$$

In particular, from 2.4.4 *viii.* $j \equiv_{b-1} y_j(b) = \pm t$ and by XIV it holds $j \equiv_z \pm t$, which combined with XVII leads to $j \equiv_z \pm\xi$.
Furthermore, by 2.4.4 *ix.* and XII one has $x_j(a) \equiv_u x_j(b) = \pm s$ which combined with XVI gives $x_j(a) \equiv_u \pm x = \pm x_k(a)$ so that from 2.5.9 it must be $j \equiv_m \pm k$.
But thanks to XIII $z^2 = y_h(a)^2 \mid y_m(a) = v$ and so from 2.5.8 *iii.* one has $z = y_h(a) \mid m$, in particular it holds $j \equiv_z \pm k$, and so $k \equiv_z \pm\xi$.
One then notices that from XVIII and 2.4.10 one has $|\sigma_i(\xi)| \leq 1/2|N_{K/\mathbb{Q}}(z)|^{1/n}$ $\forall i \in \{1, \dots, n\}$, similarly from XIX and 2.4.10 $k < |\sigma_i(x_k(a))| \leq 1/2|N_{K/\mathbb{Q}}(z)|^{1/n}$ $\forall i \in \{1, \dots, n\}$, so that:

$$|\sigma_i(\xi \pm k)||\sigma_i(\xi) \pm k| \leq |N_{K/\mathbb{Q}}(z)|^{1/n} \ \forall i \in \{1, \dots, n\}$$

giving finally $|N_{K/\mathbb{Q}}(\xi \pm k) = \prod_{i=1}^{n} \sigma_i(\xi \pm k)| \leq |N_{K/\mathbb{Q}}(z)|$, which combined with $k \equiv_z \pm\xi$ leads to $\xi = \pm k \in \mathbb{Z}$.
Then it will be shown $\mathbb{N}^+ \subseteq S$. Suppose $\xi \in \mathbb{N}^+$, then the previous part of the proof suggests to define $k = \xi$, $x = x_k(a)$, $y = y_k(a)$ so that I is satisfied and by 2.5.7 V is satisfied too.
Defining $\eta = 2^{n+1}\xi^n(\xi+1)^n \dots (\xi+n-1)^n x^n (x+1)^n \dots (x+n-1)^n$, by 2.4.4 *xi.* $\exists h_0 \in \mathbb{N}^+$ such that $\eta \mid y_{h_0}(a)$, but then from 2.5.10 $\exists h \in h_0\mathbb{N}^+$ such that $|\sigma_i(y_h(a))| \geq 1/2$ $\forall i \in \{2, \dots, n\}$, and by 2.5.8 *ii.* $y_{h_0}(a) \mid y_h(a)$ so that setting $z = y_h(a)$ X, XVIII and XIX are satisfied.
Setting naturally $w = x_h(a)$ II is satisfied and by 2.5.7 VI is satisfied too.
Again using 2.4.4 *xi.* $\exists m_0 \in \mathbb{N}^+$ such that $z^2 \mid y_{m_0}(a)$ but then from 2.5.10 $\exists m \in m_0\mathbb{N}^+$ such that $|\sigma_i(y_m(a))| \geq 1/2$ $\forall i \in \{1, \dots, n-2\}$, and by 2.5.8 *ii.* $y_{m_0}(a) \mid y_m(a)$ so that setting $u = x_m(a)$ and $v = y_m(a)$ III, XI, XII and XIII are satisfied and by 2.5.7 VII is satisfied too.
By 2.5.11 thanks to $****$ $\exists b \in \mathcal{O}_K$ satisfying IX, XIV and XV.
Finally, setting $s = x_k(b)$, $t = y_k(b)$ IV is satisfied and by 2.5.7 VIII is satisfied too, and thanks to XV and 2.4.4 *ix.* XVI is satisfied too.
From XIV combined with 2.4.4 *viii.* XVII follows, in particular the elements defined $\xi, x, y, w, z, u, v, s, t, b \in \mathcal{O}_K$ are a solution to Σ, so that $\xi \in S$. □

Chapter 3

Reductions with Elliptic Curves

3.1 Poonen's Theorem

The main goal of the section will be the following theorem:

Theorem 3.1.1. *Let $F \subseteq K$ extension of number fields: E elliptic curve over F such that $rkE(F) = rkE(K) = 1 \implies \mathcal{O}_F \subseteq \mathcal{O}_K$ is diophantine.*

An immediate corollary is the following:

Corollary 3.1.2. *Let $F \subseteq K$ extension of number fields: H10 unsolvable over $\mathcal{O}_F$ and E elliptic curve over F such that $rkE(F) = rkE(K) = 1 \implies$ H10 unsolvable over $\mathcal{O}_K$.*

Remark 3.1.3. Recalling that $\mathcal{O}_F \setminus \{0\} \subseteq \mathcal{O}_F$ is diophantine, then thanks to the surjective map $\varphi : \mathcal{O}_F \times \mathcal{O}_F \setminus \{0\} \twoheadrightarrow F$ such that $(a, b) \mapsto \frac{a}{b}$, then if $S \subseteq F^n$ diophantine over F, one has $(\varphi^{-1})^n(S) \subseteq \mathcal{O}_F^n$.
In particular, one may suppose some of the variables are taking values in $\mathcal{O}_F$ and some others in F.

Definition 3.1.4. F number field, $\mathcal{O}_F$ rings of integers of F, for $t \in F^\times$ define the *denominator ideal* of t as $den(t) := \{b \in \mathcal{O}_F : bt \in \mathcal{O}_F\}$ and the *numerator ideal* of t as $num(t) := den(t^{-1})$, with the convention $num(0) := (0)$.

Lemma 3.1.5. *Let F be a number field, $n, m \in \mathbb{N}^+$:*

- *i.* $S = \{(x_1, \dots, x_n, y_1, \dots, y_m) \in F^{n+m} : (x_1, \dots, x_n) \mid (y_1, \dots, y_m)\} \subseteq F^{n+m}$ *diophantine (meaning the division of fractional ideals).*
- *ii.* $S = \{(t, u) \in F^\times \times F^\times : den(t) \mid den(u)\} \subseteq F^2$ *diophantine.*

- *iii.* $S = \{(t,u) \in F^\times \times F^\times : den(t) \mid num(u)\} \subseteq F^2$ *diophantine.*
- *iv.* $S = \{(t,u) \in \mathcal{O}_F \times F^\times : t \mid den(u)\} \subseteq F^2$ *diophantine.*

Proof. *i.*: obvious.
ii.: trivially by *i.* considering that $den(t) \mid den(u) \iff (u,1) \mid (t,1)$.
iii.: noticing that $den(u^{-1}) = num(u)$ it follows that $den(t) \mid num(u) \iff u = 0 \vee (\exists v)(uv = 1 \wedge den(t) \mid den(v))$ concluding then from *ii.*.
iv.: analogously $t \mid den(u) \iff (\exists v)(tv = 1 \wedge den(v) \mid den(u))$ concluding then from *ii.*. □

Let for the rest of the section $n = [K : \mathbb{Q}]$ and $s = [F : \mathbb{Q}]$, $\alpha \in \mathcal{O}_K$ such that $B_\alpha = \{\alpha^i : i \in \{0, 1, \ldots, s-1\}\}$ integral basis of K over F.
Define $D_\alpha = Disc_{K/F}(1, \alpha, \ldots, \alpha^{s-1})$.

Lemma 3.1.6. *Let $F \subseteq K$ extension of number fields and α, D as above: $\exists c = c(F,K,\alpha) \in \mathbb{N}^+$ such that $\forall I \subsetneq \mathcal{O}_K$ non zero ideal, $\forall \mu \in \mathcal{O}_K$: $\mu = \sum_{i=0}^{s-1} a_i \alpha^i$ for $a_i \in F$: $(\mu(\mu+1)\cdots(\mu+n)) \mid I \implies N_{K/\mathbb{Q}}(D_\alpha a_i) \leq N_{K/\mathbb{Q}}(I)^c \ \forall i \in \{0, 1, \ldots, s-1\}$.*

Proof. See [8] Part 2 section 1.2. □

Lemma 3.1.7. *Let $F \subseteq K$ extension of number fields and α, D as above: $\exists c' = c(F,K) \in \mathbb{N}^+ : \forall I \subseteq \mathcal{O}_K$ non zero ideal, $\forall \mu \in \mathcal{O}_K, \forall \omega \in \mathcal{O}_F : \mu = \sum_{i=0}^{s-1} a_i \alpha^i$ for $a_i \in F$: $N_{K/\mathbb{Q}}(D_\alpha a_i) < c' N_{K/\mathbb{Q}}(I) \ \forall i \in \{0, 1, \ldots, s-1\} \wedge \mu \equiv_{I\mathcal{O}_K} \omega \implies \mu \in \mathcal{O}_F$.*

Proof. Choose $J_1, \ldots, J_h$ representative ideals generators of the class group of $\mathcal{O}_F$ and let $c' > 0 : c' N_{K/\mathbb{Q}}(J_i) < 1 \ \forall i \in \{1, \ldots, h\}$, then let $i_0 \in \{1, \ldots, h\}$: $J_{i_0} I^{-1} = (z)$ principal for a certain $z \in F^\times$, and since $\mu \equiv_{I\mathcal{O}_K} \omega$ one has:

$$z(\mu - \omega) = z(a_0 - \omega) + \sum_{i=1}^{s-1} (z a_i)\alpha^i \in (z) I \mathcal{O}_K = J_{i_0} \mathcal{O}_K$$

So that $Dz a_i \in \mathcal{O}_F \ \forall i \in \{1, \ldots, s-1\}$, but noticing:

$$|N_{K/\mathbb{Q}}(Dz a_i)| = |N_{K/\mathbb{Q}}(D a_i)||N_{K/\mathbb{Q}}(z)| < c' |N_{K/\mathbb{Q}}(I)| \frac{|N_{K/\mathbb{Q}}(J_{i_0})|}{|N_{K/\mathbb{Q}}(I)|} < 1$$

In particular, $Dz a_i = 0 \ \forall i \in \{1, \ldots, s-1\}$ and so $a_i = 0 \ \forall i \in \{1, \ldots, s-1\}$, in particular $\mu \in \mathcal{O}_K \cap F = \mathcal{O}_F$. □

Let $E : y^2 = x^3 + ax + b$ Elliptic curves in Weierstrass form for $a, b \in \mathcal{O}_F$ such that $rk(E(K)) = rk(E(F)) = 1$, and denote by O the point at infinity (identity of $E(F)$).
Let $\mathfrak{p}$ a non archimedean place of K, $K_{\mathfrak{p}}$ its completion, so that the reduction gives $E_{\mathfrak{p}}^{smooth}$ smooth part of $E_{\mathfrak{p}} = Proj\left(\frac{\mathbb{F}_{\mathfrak{p}}[X,Y,Z]}{(Y^2Z - X^3 - \bar{a}XZ^2 - \bar{b}Z^3)}\right)$, then defining $E_0(K_{\mathfrak{p}}) := \{P \in E_{\mathfrak{p}}(K_{\mathfrak{p}}) : \overline{P} \in E_{\mathfrak{p}}^{smooth}(\mathbb{F}_{\mathfrak{p}})\}$ ($\overline{P}$ meaning the reduction of $P \ mod \mathfrak{p}$).

Lemma 3.1.8. *The followings hold:*

i. $E_0(K_{\mathfrak{p}}) \leq E_{\mathfrak{p}}(K_{\mathfrak{p}})$ *(as a subgroup).*

ii. $red_{\mathfrak{p}} : E_0(K_{\mathfrak{p}}) \longrightarrow E_{\mathfrak{p}}^{smooth}(\mathbb{F}_{\mathfrak{p}})$ *epimorphism.*

iii. $[E_{\mathfrak{p}}(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})] < \infty \wedge [E_{\mathfrak{p}}(K_{\mathfrak{p}}) : E_1(K_{\mathfrak{p}})]$, *where* $E_1(K_{\mathfrak{p}}) := Ker(red_{\mathfrak{p}})$.

Proof. i. and *ii.* are from [12], and *iii.* follows noticing that both are open subgroups of the compact topological group $E_{\mathfrak{p}}(K_{\mathfrak{p}})$ with respect to the $\mathfrak{p}$-adic topology. □

Let $r \in \mathbb{N}^+ : \#E(K)_{tors} \mid r \ \wedge \ [E(K) : E(F)] \mid r \ \wedge \ [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})] \mid r$. For Ω_K the set of places of K, recalling the definition of height: $h(a) = \sum_{v \in \Omega_K} log(max\{\|a\|_v, 1\})$, then:

Lemma 3.1.9. *Let X be a smooth, projective, geometrically integral curve over K of genus $g \geq 1$, $v \in \Omega_K$, ϕ a non constant rational function on X, $\{P_n\}_{n \in \mathbb{N}} \subseteq X(K)$ sequence of distinct points such that $\exists m_0 \in \mathbb{N}^+ \ \forall m \in \mathbb{N} : m \geq m_0 \implies P_m$ not a pole of ϕ, so that $z_m := \phi(P_m) \in K$:*

$$\lim_{m \to +\infty} \frac{log(\|z_m\|_v)}{h(z_m)} = 0$$

Proof. See [13], Section 7.4. □

Lemma 3.1.10. $\exists r_0 \in \mathbb{N}^+ \ \forall r \in \mathbb{N} : r \geq r_0, P \in rE(K) \setminus \{O\}, m \in \mathbb{Z} \setminus \{0, \pm 1\}$:

$$log(N_{K/\mathbb{Q}}(den(x(mP)))) \geq \frac{9}{10} m^2 log(N_{K/\mathbb{Q}}(den(x(P)))) > 0$$

In particular, $den(x(mP)) \neq den(x(P)) \wedge den(x(P)) \neq (1)$.

Proof. By hypothesis $rk(E(K)) = 1$, implying $rk(rE(K)) = 1$ too, so that one can fix a generator P_1 of $rE(K)$, by results in Chapter 8 of [12] $\exists \hat{h}(P_1) \in \mathbb{R}^+$ such that $h(x(mP_1)) = m^2\hat{h}(P_1) + O(1)\ \forall m \in \mathbb{Z}$.
Applying 3.1.9 with $X = E$, $\phi = x$, to each $v \in \Omega_K$ archimedean for r sufficiently large the result follows from:

$$log(N_{K/\mathbb{Q}}(den(x(mP)))) = (1 + o(1))h(x(mP_1)) = (1 - o(1))m^2\hat{h}(P_1) + O(1)$$

□

Let from now on $r \in \mathbb{N}^+$ satisfying the hypothesis of 3.1.10 and the divisibility conditions above, equivalently such that $\forall P \in rE(K) \setminus \{O\}, \forall m \in \mathbb{Z} \setminus \{0, \pm 1\}$:

$$\Sigma = \begin{cases} I : log(N_{K/\mathbb{Q}}(den(x(mP)))) \geq \frac{9}{10}m^2 log(N_{K/\mathbb{Q}}(den(x(P)))) > 0 \\ II : \#E(K)_{tors} \mid r \\ III : [E(K) : E(F)] \mid r \\ VI : [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})] \mid r \end{cases}$$

Lemma 3.1.11. *Let $r \in \mathbb{N}^+$ satisfying the conditions of Σ, $P, P' \in rE(K) \setminus \{O\}$ then: $den(x(P)) \mid den(x(P')) \iff P'$ integral multiple of P.*

Proof. First it will be shown the claim: $\forall I \subseteq \mathcal{O}_K$ non zero ideal the set $G_I := \{Q \in rE(K) : I \mid den(x(Q))\}$ is a subgroup of $rE(K)$.
Indeed, by convention $den(O) = 0$, so $O \in G_I$, and since intersections of subgroups are still subgroups, using the decomposition of ideals in Dedekind domains and noticing I, J coprime ideals $\implies G_{IJ} = G_I \cap G_J$, then it is sufficient to check the claim for $I = \mathfrak{p}^n$ for $n \in \mathbb{N}, \mathfrak{p}$ prime ideal.
As in Chapter 4 of [12], denote $\mathcal{F} \in \mathcal{O}_K[[z_1, z_2]]$, then, letting $\mathcal{O}_{\mathfrak{p}}$ denote the $\mathfrak{p}$-adic completion of $\mathcal{O}_K$, one has the isomorphism $\mathcal{F}(\mathfrak{p}\mathcal{O}_{\mathfrak{p}}) \cong E_1(K_{\mathfrak{p}})$ explicitely given by $z \mapsto (x(z), y(z))$ pair of Laurent series with coefficients in $\mathcal{O}_K$.
Through this isomorphism, it is clear that $G_{\mathfrak{p}^n} \cong \mathcal{F}(\mathfrak{p}^{\lceil n/2 \rceil}\mathcal{O}_{\mathfrak{p}})$, so that it is a subgroup as claimed.
In particular, ($\impliedby$) is immediate since $G_{den(x(P))}$ is a subgroup and so integral multiples of its elements are still in it and trivially $P \in G_{den(x(P))}$.
For the other implication ($\implies$), since $G_{den(x(P))} \leq rE(K) \cong \mathbb{Z}$, then it is an abelian free group of rank 1, let Q be a generator of $G_{den(x(P))}$, but clearly $P \in G_{den(x(P))}$ so that P is an integral multiple of Q, and by the ($\impliedby$) part it follows that $den(x(Q)) \mid den(x(P))$, but by definition of $G_{den(x(P))}$ also $den(x(P)) \mid den(x(Q))$, so that $den(x(Q)) = den(x(P))$, which from 3.1.10 implies $Q = \pm P$, and the hypothesis $den(x(P)) \mid den(x(P'))$ gives immediately $P' \in G_{den(x(P))} \cong \mathbb{Z}Q \cong \mathbb{Z}P$. □

Remark 3.1.12. Let $r \in \mathbb{N}^+$ satisfying the conditions of Σ, $I \subseteq \mathcal{O}_K$ non-zero ideal, then $\exists P \in rE(K) \setminus \{O\}$ such that $I \mid den(x(P))$.
Indeed, as in 3.1.11 it is sufficient to check it for $I = \mathfrak{p}^n$ for $n \in \mathbb{N}$ and $\mathfrak{p}$ prime ideal, in which case, thanks to the isomorphism $E_1(K_\mathfrak{p}) \cong \mathcal{F}(\mathfrak{p}\mathcal{O}_\mathfrak{p})$ which gives the correspondence $G_{\mathfrak{p}^n} \cong \mathcal{F}(\mathfrak{p}^{\lceil n/2 \rceil}\mathcal{O}_\mathfrak{p})$, one has that $\mathcal{F}(\mathfrak{p}^{\lceil n/2 \rceil}\mathcal{O}_\mathfrak{p})$ is an open subgroup of $E(K_\mathfrak{p})$, in particular it has finite index and can't be trivial.

Lemma 3.1.13. *Let $r \in \mathbb{N}^+$ satisfying the conditions of Σ, $P \in rE(K)\setminus\{O\}$, $m \in \mathbb{Z} \setminus \{0\}$, $t = x(P), t' = x(mP)$, then $den(t) \mid num((t/t' - m^2)^2)$*

Proof. Supposing $\mathfrak{p}$ prime ideal such that $\mathfrak{p}^n \mid den(t)$ for a certain $n \in \mathbb{N}^+$, then $k = v_\mathfrak{p}(z(P)) \in \mathbb{N}^+$ since $n = 2k$ and thanks to the Laurent series $x(P) \in z(P)^{-2}(1 + \mathfrak{p}^k\mathcal{O}_K)$.
Furthermore, with the formal group law it follows $z(mP) \in mz(P) + \mathfrak{p}^{2k}\mathcal{O}_K$, in particular $v_\mathfrak{p}(z(mP)) \geq k$ so that also $x(mP) \in z(mP)^{-2}(1+\mathfrak{p}^k\mathcal{O}_K)$, which leads to:

$$\frac{t}{t'} = \frac{x(P)}{x(mP)} \in \left(\frac{z(P)}{z(mP)}\right)^{-2} (1 + \mathfrak{p}^k\mathcal{O}_K)$$

But since $\frac{z(P)}{z(mP)} \in m + \mathfrak{p}^k\mathcal{O}_K$, then $t/t' \in m^2 + \mathfrak{p}^k\mathcal{O}_K$, so that $\mathfrak{p}^k \mid num(t/t' - m^2)$, and the thesis follows since $n = 2k$. □

Theorem 3.1.14. *Let $F \subseteq K$ extension of number fields, E elliptic curve over F such that $rkE(F) = rkE(K) = 1$, Let $r \in \mathbb{N}^+$ satisfying the conditions of Σ, c constant of 3.1.6, c' constant of 3.1.7, $\ell \in \mathbb{N}^+$ sufficiently large such that thanks to 3.1.10:*

$$c' N_{K/\mathbb{Q}}(den(x(\ell P_0))^{1/2}) > N_{K/\mathbb{Q}}(den(x(P_0))^c) \qquad (\overline{*})$$

Define Π as follows:

$$\Pi = \begin{cases} I : P = \ell P_0 \\ II : t_0 = x(P_0), t = x(P), t' = x(P') \\ III : (\mu+1)(\mu+2)\cdot(\mu+n) \mid den(t_0) \\ IV : den(t) \mid den(t') \\ V : den(t) \mid num((t/t' - \mu)^2) \end{cases}$$

Define S by $\mu \in S \iff \mu \in \mathcal{O}_K \wedge \exists P_0, P, P' \in rE(K) \setminus \{O\}, \exists t_0, t, t' \in F$ satisfying Π.
Then $S \subseteq \mathcal{O}_K$ diophantine and $N = \{k^2 : k \in \mathbb{N}^+\} \subseteq S \subseteq \mathcal{O}_F$.

Proof. $S \subseteq \mathcal{O}_K$ is diophantine thanks to 3.1.5.
First it will be shown $N \subseteq S$: let $k \in \mathbb{N}^+$, define $\mu = k^2$ and let by 3.1.12

$P_0 \in rE(K) \setminus \{O\}$ such that $(\mu+1)(\mu+2)\cdot(\mu+n) \mid den(t_0)$, and III holds. Define $P = \ell P_0$ and $P' = mP$, so as $t_0 = x(P_0), t = x(P), t' = x(P')$, in particular I and II hold too.
Thanks to 3.1.11 IV holds, and by 3.1.13 V holds, so that $\mu \in S$ and $N \subseteq S$. Finally, it will be checked $S \subseteq \mathcal{O}_F$: let $\mu \in S$, by IV and 3.1.11 one has $P' = mP$ for a certain $m \in \mathbb{Z} \setminus \{0\}$, combining 3.1.13 with V one obtains that $den(t)^{1/2} \mid num(\mu - m^2)$ ($den(t)^{1/2}$ well-defined since as in 3.1.13 all primes dividing $den(t)$ must occur to an even power since $t = x(P) \in E(K)$, i.e. $y(P)^2 = t^3 + at + b$).
Noticing $t, t', m^2 \in \mathcal{O}_F$, then $num(\mu - m^2) = (\mu - m^2)$, so that $\mu \equiv_{den(t)^{1/2}} m^2$. Finally, writing $\mu = \sum_{i=0}^{s-1} a_i \alpha^i$ for $a_i \in F$, thanks to III and 3.1.6 one obtains $N_{K/\mathbb{Q}}(Da_i) \leq N_{K/\mathbb{Q}}(den(t_0))^c$ and by the definition of ℓ it holds $N_{K/\mathbb{Q}}(Da_i) \leq c' N_{K/\mathbb{Q}}(den(t)^{1/2})$, in particular applying 3.1.7 with $I = den(t))^{1/2}$ and $\omega = m^2$ the thesis follows. □

Finally, with the usual trick it is easy to prove 3.1.1:

Proof. Using the usual argument in 2.1.4 with the set S given by 3.1.14. □

3.2 Main Theorem

In a paper (see [10]) of Cornelissen, Pheidas and Zahidi, the assumptions of Poonen's theorem have been weakened somewhat. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the larger field and an abelian variety over the smaller field retaining its rank in the extension (which are now known to hold).
However, using a strengthened version of Poonen's method, Shlapentokh was able to extend his result to the following criterion ([7], Theorem 1.9):

Theorem 3.2.1. *Let $F \subseteq K$ extension of number fields: E elliptic curve over F such that $rkE(F) = rkE(K) > 0 \implies \mathcal{O}_F \subseteq \mathcal{O}_K$ is diophantine.*

The importance of the theorem, as for the one of Poonen of the previous section, is that gives another way to find diophantine sets in a less explicit way as it was done during both the first two chapters.
Furthermore, recently thanks to additive combinatorics P. Koymans and C. Pagano ([9]) were able to check Shlapentokh's condition in a specific situation, that turns out to actually be sufficient to solve Hilbert's Tenth Problem for rings of integers of number fields:

Theorem 3.2.2. *K number field, $L = K(i)$:*

i. L *Galois.*

ii. $K = L^{<\sigma>}$ *is the fixed field of the decomposition group of an infinite place (in* L/Q*), so* L/K *is a quadratic extension ramified at some infinite place.*

iii. $\mathbb{Q}(i, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19}) \subseteq K$.

$\exists E$ *elliptic curve such that* $rk(E(K)) = rk(E(K(i)) > 0$.

Indeed, thanks to this theorem and the whole discussion of the thesis, one is finally able to prove the main theorem:

Theorem 3.2.3. *F number field: $\mathbb{Z} \subseteq \mathcal{O}_F$ diophantine, in particular $H10$ over $\mathcal{O}_F$ is unsolvable.*

Proof. Define $L = \overline{F \cdot \mathbb{Q}(i, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \sqrt{17}, \sqrt{19})}$ normal closure of the composite field, so that $K_\sigma := L^{<\sigma>}$ has satisfies the hypotheses of 3.2.2 $\forall \sigma \in G_{L/\mathbb{Q}}$ such that $< \sigma >= D_{v,L/\mathbb{Q}}$ decomposition group of an infinite place v.
In particular, $\mathcal{O}_{K_\sigma} \subseteq \mathcal{O}_L$ is diophantine $\forall \sigma \in G_{L/\mathbb{Q}}$ considered before, so that from 2.1.1 *i.*, also $\mathcal{O}_M \subseteq \mathcal{O}_L$ is diophantine, where $M := \cap_\sigma K_\sigma$.
Finally, thanks to 2.4.14 *i* $\mathbb{Z} \subseteq \mathcal{O}_M$ diophantine since M must be totally real, and so by 2.1.1 *iii.* $\mathbb{Z} \subseteq \mathcal{O}_L$ diophantine too, so as from 2.1.1 *iv.* $\mathbb{Z} \subseteq \mathcal{O}_F$ diophantine, and the rest of the claim follows from 2.1.2. □

Bibliography

[1] M. Davis, *Hilbert's Tenth Problem is Unsolvable.*

[2] J. Denef, *Hilbert's tenth problem for quadratic rings.*

[3] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers.*

[4] J. Denef, *Diophantine sets of algebraic integers, II.*

[5] T. Pheidas, *Hilbert's Tenth Problem for a class of rings of algebraic integers.*

[6] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers.*

[7] A. Shlapentokh, *Elliptic Curves retaining their rank in finite extensions and Hilbert's Tenth Problem for rings of algebraic numbers*

[8] A. Shlapentokh, *Hilbert's Tenth Problem over number fields, a survey*

[9] P. Koymans, C. Pagano, *Hilbert's tenth problem via additive combinatorics*

[10] Gunther Cornelissen, Thanases Pheidas, Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers.*

[11] G. Hardy and E. Wright, *An introduction to the theory of numbers.*

[12] J.H. Silverman, *The Arithmetic of the Elliptic Curves*

[13] J. Serre, *Lectures on the Mordell-Weil Theorem*