O DÉCIMO PROBLEMA DE HILBERT

Grégory Duran Cunha
Universidade Federal de Uberlândia
gdurancunha@hotmail.com

Victor Gonzalo Lopez Neumann
Universidade Federal de Uberlândia
gonzalo@famat.ufu.br

RESUMO

Este trabalho trata do Décimo Problema de Hilbert, cujo enunciado é: Dada uma equação diofantina com coeficientes inteiros em um número qualquer de variáveis, é possível elaborar um processo que decida, através de um número finito de operações, se a equação tem soluções inteiras. O objetivo é demonstrar que não é possível elaborar tal processo, isto é, mostrar que o Décimo Problema de Hilbert é insolúvel. Este trabalho inicia-se com um estudo sobre Equações Diofantinas, Conjuntos Diofantinos e Funções Diofantinas, analisando suas propriedades, seguindo-se uma prova do Teorema da Sequência de Números. Um papel central nesse estudo é desempenhado pelas Equações de Pell, utilizadas com a finalidade de mostrar que a função exponencial é diofantina. Este resultado, juntamente com o conceito de função recursiva, permite mostrar que uma função ser recursiva é equivalente a ser diofantina. Finalmente, provamos o Teorema de Universalidade que é utilizado na demonstração do teorema principal que afirma a insolubilidade do Décimo Problema de Hilbert.

ABSTRACT

This work discusses the Hilbert's Tenth Problem, whose statement is: Given a Diophantine equation with any number of unknown quantities and with integer coefficients, it is possible to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers. The goal is to prove that it is impossible to develop such a process, ie, to show that the Hilbert's Tenth Problem is unsolvable. This work starts with a study of Diophantine equations, Diophantine Sets and Diophantine Functions, with an analysis of their properties, followed by a proof of the Sequence Number Theorem. An important role, in this study, is played by the Pell equations, which are used to show that the exponential function is Diophantine. This result, together with the concept of recursive function , allows us to show that there is an equivalence between recursive functions and Diophantine functions. Finally we prove the universality theorem which is used in the proof of the main theorem which asserts the insolubility of Hilbert's Tenth Problem.

Palavras-chave: Equações diofantinas, função recursiva, função diofantina.

1 INTRODUÇÃO

No ano de 1900, o matemático David Hilbert divulgou um documento contendo vinte e três problemas que deixaram o século XIX para serem resolvidos no século XX. O décimo

problema se trata de equações diofantinas e seu enunciado é: Dada uma equação diofantina com coeficientes inteiros em um número qualquer de variáveis, é possível elaborar um processo que decida, através de um número finito de operações, se a equação tem soluções inteiras. Hoje entendemos o termo "elaborar um processo" no sentido de encontrar um algoritmo. Mas, quando os problemas de Hilbert foram propostos, não havia nenhuma noção rigorosa para o conceito de algoritmo, e isso era um obstáculo para a solução desse problema.

A primeira grande contribuição foi dada em 1931 por Kurt Godel (ver [5]), além de outros lógicos como Alonzo Church [1] e Alan Turing [9], que contribuíram na formulação rigorosa para a noção de computabilidade. Isso possibilitou o estabelecimento do que seria um algoritmo insolúvel, isto é, a impossibilidade de existir um algoritmo com determinadas propriedades. Assim, os primeiros exemplos de algoritmos insolúveis foram encontrados inicialmente na lógica matemática para surgirem posteriormente em outros ramos da matemática.

A teoria da computabilidade forneceu diversas ferramentas para enfrentar o Décimo Problema de Hilbert. Na década de 1950, surgiram vários artigos relacionados ao problema, alguns deles escritos por Martin Daves [2] e Hilary Putnam [4].

A matemática Julia Robinson contribuiu fortemente na demonstração de que a função exponencial é diofantina (ver [7]). Mas, a peça chave na solução definitiva do problema foi o matemático Yuri Matiyasevich (ver [6]) que, apesar de não ter sido o primeiro a investigar o problema, soube habilmente juntar as peças deste grande quebra-cabeças e resolver, no ano de 1970, o Décimo Problema de Hilbert.

O artigo começa tratando das equações diofantinas com alguns exemplos e propriedades. Os resultados nesta seção são: o Teorema das Funções de Emparelhamento e o Teorema da Sequência de Números. Em seguida vem uma série de lemas sobre equações de Pell com a finalidade de provar que a função exponencial é diofantina. Como consequência desse fato obtemos novas funções diofantinas e novos conjuntos diofantinos. Na parte final do artigo definimos função recursiva e provamos que uma função ser recursiva é equivalente a ser diofantina. Após isso, provamos o Teorema da Universalidade e concluímos o artigo com o teorema que afirma a insolubilidade do Décimo Problema de Hilbert.

Neste artigo vamos denotar o conjunto dos números naturais por $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ e o conjunto dos números inteiros positivos por $\mathbb{N}^* = \{1, 2, 3, \dots\}$. Além disso, será necessário utilizar o Teorema de Lagrange, que afirma que todo número natural possui representação como soma de quatro quadrados. A demonstração deste teorema se encontra na referência [8].

2 EQUAÇÕES DIOFANTINAS

Vamos iniciar tratando das Equações Diofantinas com o objetivo de introduzir os conceitos de Conjuntos Diofantinos e Funções Diofantinas. Vamos definir tais conceitos, ver alguns exemplos e propriedades.

Definição 2.1: *Seja $D(x_1, \dots, x_n)$ um polinômio com coeficientes inteiros nas variáveis $x_1, \dots, x_n$. Dizemos que $D(x_1, \dots, x_n) = 0$ é uma equação diofantina.*

Observe que a equação diofantina $D(x_1, \dots, x_n) = 0$ pode ser escrita como

$$D_L(x_1, \dots, x_n) = D_R(x_1, \dots, x_n),$$

onde D_L e D_R são polinômios com coeficientes inteiros e positivos.

Vejamos agora um resultado que nos permite reduzir um sistema de equações diofantinas a uma única equação diofantina.

Proposição 2.1: *O sistema de equações diofantinas*

$$\begin{cases} D_1(x_1,\ldots,x_n)=0 \\ \vdots \\ D_m(x_1,\ldots,x_n)=0 \end{cases}$$

tem solução se, e somente se, a equação diofantina

$$D_1^2(x_1,\ldots,x_n)+\cdots+D_m^2(x_1,\ldots,x_n)=0$$

tem a mesma solução.

Demonstração. Suponha que o sistema dado tenha como solução os inteiros $x_1,\ldots x_n$, então

$$D_i(x_1,\ldots,x_n)=0, \quad 1\leq i\leq m.$$

Assim, $D_i^2(x_1,\ldots,x_n)=0$ para $1\leq i\leq m$. Portanto,

$$D_1^2(x_1,\ldots,x_n)+\cdots+D_m^2(x_1,\ldots,x_n)=0.$$

Reciprocamente, sejam $x_1,\ldots x_n\in\mathbb{Z}$ tais que

$$D_1^2(x_1,\ldots,x_n)+\cdots+D_m^2(x_1,\ldots,x_n)=0.$$

Como $D_i^2(x_1,\ldots,x_n)\geq 0$, para $1\leq i\leq m$, segue que $D_i^2(x_1,\ldots,x_n)=0$, para $1\leq i\leq m$, logo, $D_i(x_1,\ldots,x_n)=0$, para $1\leq i\leq m$. □

Dada uma equação diofantina $D(x_1,\ldots,x_n)=0$, vejamos quando esta equação possui solução no conjunto dos números naturais.

Proposição 2.2: *A equação diofantina $D(x_1,\ldots,x_n)=0$ tem uma solução nos naturais se, e somente se, o sistema*

$$\begin{cases} D(x_1,\ldots,x_n)=0 \\ x_1=y_{1,1}^2+y_{1,2}^2+y_{1,3}^2+y_{1,4}^2 \\ x_2=y_{2,1}^2+y_{2,2}^2+y_{2,3}^2+y_{2,4}^2 \\ \vdots \\ x_n=y_{n,1}^2+y_{n,2}^2+y_{n,3}^2+y_{n,4}^2 \end{cases} \tag{1}$$

tem uma solução nos inteiros.

Demonstração. Suponha que $D(x_1,\ldots,x_n)=0$ tenha uma solução nos naturais, digamos que seja ela $(x_1,\ldots,x_n)$. Pelo Teorema de Lagrange, x_i pode ser escrito como soma de quatro quadrados, para $1\leq i\leq n$. Logo, existe uma solução para o sistema.
Reciprocamente, uma solução do sistema em números inteiros inclui a solução $(x_1,\ldots,x_n)$ em números naturais da equação $D(x_1,\ldots,x_n)=0$. □

Observe que o sistema (1) pode ser escrito como uma única equação da forma

$$E(x_1,\ldots,x_n,y_{1,1},\ldots,y_{n,4})=0,$$

que tem solução nos inteiros se, e somente se, a equação $D(x_1,\ldots,x_n)=0$ tem solução nos naturais. Desse modo, utilizaremos este resultado para provar a insolubilidade do Décimo Problema de Hilbert no conjunto dos números inteiros depois de provar a sua insolubilidade no conjunto dos números inteiros positivos.

Definição 2.2 (Conjunto Diofantino): *Seja $M \subseteq (\mathbb{N}^*)^n$. O conjunto M será chamado de conjunto diofantino quando existe um polinômio $D(a_1, \ldots, a_n, x_1, \ldots, x_m)$ a coeficientes inteiros tal que*

$$(a_1, \ldots, a_n) \in M \Longleftrightarrow \exists x_1, \ldots, x_m \in \mathbb{N}^* \text{ tais que } D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0.$$

O número n é chamado de dimensão de M.

Vejamos alguns exemplos de conjuntos diofantinos:

1. O conjunto C dos números compostos é diofantino. Observe que, $x \in C \Longleftrightarrow \exists y, z \in \mathbb{N}^*$ tais que $x = (y+1)(z+1)$. De fato, seja $x \in C$. Então existem $1 < a, b < x$ tais que $x = ab$. Como $a, b > 1$, existem $y, z \in \mathbb{N}^*$ tais que $a = y + 1$ e $b = z + 1$. Logo,

   $$x = (y+1)(z+1).$$

   Reciprocamente, suponha que $\exists y, z \in \mathbb{N}^*$ tais que

   $$x = (y+1)(z+1).$$

   Como $(y+1), (z+1) > 1$, segue que x é composto. Portanto, $x \in C$.

2. O conjunto S dos números que não são potências de 2 é diofantino, pois

   $$x \in S \Longleftrightarrow \exists y, z \in \mathbb{N}^* \text{ tais que } x = y(2z+1).$$

3. O conjunto $M = \{(x, y) \in (\mathbb{N}^*)^2 : x < y\}$ é diofantino, pois

   $$(x, y) \in M \Longleftrightarrow \exists z \in \mathbb{N}^* \text{ tal que } x + z = y.$$

4. O conjunto $N = \{(x, y) \in (\mathbb{N}^*)^2 : x \leq y\}$ é diofantino, pois

   $$(x, y) \in N \Longleftrightarrow \exists z \in \mathbb{N}^* \text{ tal que } x + z - 1 = y.$$

5. O conjunto $D = \{(x, y) \in (\mathbb{N}^*)^2 : x \mid y\}$ é diofantino, pois

   $$(x, y) \in D \Longleftrightarrow \exists z \in \mathbb{N}^* \text{ tal que } y = zx.$$

Vejamos agora, que a união e a interseção de dois conjuntos diofantinos de mesma dimensão são também conjuntos diofantinos.

Proposição 2.3: *Sejam os conjuntos*

$$M_1 = \{(a_1, \ldots, a_n) \in (\mathbb{N}^*)^n : \exists x_1, \ldots, x_m \in \mathbb{N}^* \text{ tais que } D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\},$$

$$M_2 = \{(a_1, \ldots, a_n) \in (\mathbb{N}^*)^n : \exists y_1, \ldots, y_t \in \mathbb{N}^* \text{ tais que } D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0\}.$$

Então,

$$(a_1, \ldots, a_n) \in M_1 \cup M_2 \Longleftrightarrow \exists x_1, \ldots, x_m, y_1, \ldots, y_t \in \mathbb{N}^* \text{ tais que}$$
$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Demonstração. Seja $(a_1, \ldots, a_n) \in M_1 \cup M_2$. Caso $(a_1, \ldots, a_n) \in M_1$, então,

$$\exists x_1, \ldots, x_m \in \mathbb{N}^* \text{ tais que } D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0.$$

Logo,

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0,$$

para quaisquer $y_1, \ldots, y_t \in \mathbb{N}^*$. Caso $(a_1, \ldots, a_n) \in M_2$, então, existem $y_1, \ldots, y_t \in \mathbb{N}^*$ tais que $D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0$. Logo,

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0,$$

para quaisquer $x_1, \ldots, x_m \in \mathbb{N}^*$.
Reciprocamente, suponha que $\exists x_1, \ldots, x_m, y_1, \ldots, y_t \in \mathbb{N}^*$ tais que

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Caso $D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ então, $(a_1, \ldots, a_n) \in M_1$, logo, $(a_1, \ldots, a_n) \in M_1 \cup M_2$. Caso $D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0$, então $(a_1, \ldots, a_n) \in M_2$, logo, $(a_1, \ldots, a_n) \in M_1 \cup M_2$. □

Proposição 2.4: *Sejam os conjuntos*

$$M_1 = \{(a_1, \ldots, a_n) \in (\mathbb{N}^*)^n : \exists x_1, \ldots, x_m \in \mathbb{N}^* \textit{ tais que } D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}$$

$$M_2 = \{(a_1, \ldots, a_n) \in (\mathbb{N}^*)^n : \exists y_1, \ldots, y_t \in \mathbb{N}^* \textit{ tais que } D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0\}.$$

Então,

$$(a_1, \ldots, a_n) \in M_1 \cap M_2 \iff \exists x_1, \ldots, x_m, y_1, \ldots, y_t \in \mathbb{N}^* \textit{ tais que}$$

$$D_1^2(a_1, \ldots, a_n, x_1, \ldots, x_m) + D_2^2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Demonstração. Seja $(a_1, \ldots, a_n) \in M_1 \cap M_2$, então $\exists x_1, \ldots, x_m, y_1, \ldots, y_t \in \mathbb{N}^*$ tais que $D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ e $D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0$. Portanto,

$$D_1^2(a_1, \ldots, a_n, x_1, \ldots, x_m) + D_2^2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Reciprocamente, suponha que $\exists x_1, \ldots, x_m, y_1, \ldots, y_t \in \mathbb{N}^*$ tais que

$$D_1^2(a_1, \ldots, a_n, x_1, \ldots, x_m) + D_2^2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Então,

$$D_1(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \text{ e } D_2(a_1, \ldots, a_n, y_1, \ldots, y_t) = 0.$$

Logo, $(a_1, \ldots, a_n) \in M_1 \cap M_2$. □

3 FUNÇÕES DIOFANTINAS

Definição 3.1: *Seja $f : (\mathbb{N}^*)^n \longrightarrow \mathbb{N}^*$. Chamamos de gráfico de f o conjunto*

$$\text{graf}(f) = \{(a_1, \ldots, a_n, b) \in (\mathbb{N}^*)^{n+1} : b = f(a_1, \ldots, a_n)\}.$$

Definição 3.2 (Função Diofantina)**:** *Seja $f : (\mathbb{N}^*)^n \longrightarrow \mathbb{N}^*$. Dizemos que f é uma função diofantina quando $\text{graf}(f)$ é um conjunto diofantino.*

Considere a função $T : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ definida por

$$T(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Observe que T é uma função diofantina, de fato, como

$$\text{graf}(T) = \{(m, n) \in (\mathbb{N}^*)^2 : n = T(m)\},$$

então

$$(m, n) \in \text{graf}(T) \iff n = \frac{m(m+1)}{2} \iff 2n = m(m+1).$$

Logo, $\text{graf}(T)$ é um conjunto diofantino e, portanto, T é uma função diofantina.

Lema 3.1: *Considere a função $T : \mathbb{N} \longrightarrow \mathbb{N}$ definida por*

$$T(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ se } n > 0$$

e $T(0) = 0$. Então, para cada $z \in \mathbb{N}^*$, existe um único $n \in \mathbb{N}$ tal que

$$T(n) < z \leq T(n+1).$$

Demonstração. Seja $z \in \mathbb{N}^*$. Como $z \geq 1$, temos que $\frac{z+1}{2} \geq 1$, então $\frac{z(z+1)}{2} \geq z$, e portanto, $T(z) \geq z$. Agora, defina o conjunto

$$S_z = \{n \in \mathbb{N} : T(n) \geq z\}.$$

Veja que $S_z \neq \emptyset$, pois $z \in S_z$. Além disso, $S_z \subset \mathbb{N}^*$, pois $0 \notin S_z$. Pelo Princípio da Boa Ordem, existe um único $m \in S_z$ tal que $m = \min S_z$, e consequentemente, existe um único $n = m - 1 \in \mathbb{N}$. Como $n < m = \min S_z$, temos que $n \notin S_z$, logo, $T(n) < z$, e como $m \in S_z$, temos que $z \leq T(m)$. Portanto,

$$T(n) < z \leq T(n+1).$$

□

No próximo resultado veremos que é possível encontrar uma bijeção diofantina entre $\mathbb{N}^* \times \mathbb{N}^*$ e $\mathbb{N}^*$.

Teorema 3.1 (Teorema das Funções de Emparelhamento): *Existem funções diofantinas $P(x, y)$, $L(z)$ e $R(z)$ tais que*

(i) $\forall x, y \in \mathbb{N}^*$ *temos* $L(P(x, y)) = x$ *e* $R(P(x, y)) = y$.

(ii) $\forall z \in \mathbb{N}^*$ *temos* $P(L(z), R(z)) = z$, $L(z) \leq z$ *e* $R(z) \leq z$.

Demonstração. Considere a função

$$T(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}, \ \ n \in \mathbb{N}.$$

Seja $z \in \mathbb{N}^*$, então, pelo lema anterior, existe um único $n \in \mathbb{N}$ tal que

$$T(n) < z \leq T(n+1).$$

Como $T(n) < z$, segue que $z - T(n) > 0$, então

$$y := z - T(n) \in \mathbb{N}^*.$$

Por outro lado, como

$$z \leq T(n+1) = T(n) + n + 1,$$

temos que

$$y + T(n) \leq T(n) + n + 1,$$

então, $y \leq n + 1$, ou seja, $n + 1 - y \geq 0$, logo,

$$(n+1) - y + 1 > 0.$$

Assim,

$$x := (n+1) - y + 1 \in \mathbb{N}^*.$$

Observe que x e y são únicos e dependem de z. Podemos então definir as funções:

$$L : \mathbb{N}^* \longrightarrow \mathbb{N}^*, \text{ com } L(z) = x;$$

$$R : \mathbb{N}^* \longrightarrow \mathbb{N}^*, \text{ com } R(z) = y.$$

Como $z = T(n) + y$ e $n = x + y - 2$, segue que

$$z = T(x + y - 2) + y.$$

Definimos assim,

$$P(x, y) = z = T(x + y - 2) + y.$$

Observe que

$$P(L(z), R(z)) = P(x, y) = z.$$

Como $z = T(x + y - 2) + y$ temos que $z \geq y$, ou seja, $z \geq R(z)$. Vejamos agora, que $L(z) \leq z$. Como

$$z = T(x + y - 2) + y,$$

segue que $z > T(x + y - 2)$, então

$$z \geq T(x + y - 2) + 1 \geq T(x - 1) + 1,$$

pois T é crescente. Se $x = 1$, então $z \geq x = L(z)$. Se $x = 2$, então

$$z \geq T(1) + 1 = 2 = x = L(z).$$

Se $x \geq 3$, então $x - 1 \geq 2$, logo,

$$T(x - 1) = 1 + 2 + \cdots + (x - 1) \geq 1 + (x - 1) = x$$

assim,

$$z \geq T(x - 1) + 1 > T(x - 1) \geq x.$$

Portanto, $z \geq x = L(z)$. Agora, sejam $x, y \in \mathbb{N}^*$. Como

$$P(x, y) = T(x + y - 2) + y = z$$

temos que, para $n = x + y - 2$,

$$T(n) < z \leq T(n + 1).$$

De fato, como $z = T(n) + y$, segue que $z > T(n)$. E, como $x - 1 \geq 0$, temos que

$$T(n) + y + (x - 1) \geq T(n) + y,$$

então,

$$T(n) + n + 1 \geq z,$$

logo, $T(n + 1) \geq z$. Agora, veja que

$$R(P(x, y)) = R(z) = z - T(n) = y$$

$$L(P(x, y)) = L(z) = (n - 1) - R(z) + 1 = (x + y - 1) - y + 1 = x.$$

Finalmente,

$$z = T(x + y - 2) + y = \frac{(x + y - 2)(x + y - 1)}{2} + y \iff 2z = (x + y - 2)(x + y - 1) + 2y.$$

Então,

$$z = P(x, y) \iff 2z = (x + y - 2)(x + y - 1) + 2y;$$

$$x = L(z) \iff \exists y \in \mathbb{N}^* \text{ tal que } 2z = (x + y - 2)(x + y - 1) + 2y;$$

$$y = R(z) \iff \exists x \in \mathbb{N}^* \text{ tal que } 2z = (x + y - 2)(x + y - 1) + 2y.$$

Portanto, as funções $L(z)$, $R(z)$ e $P(x, y)$ são diofantinas. □

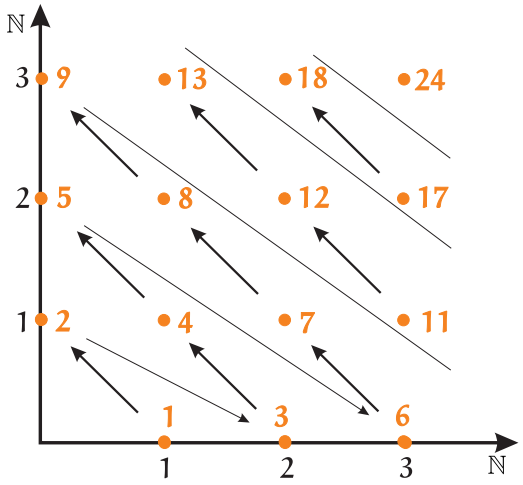

FIGURA 1

Veja na figura 1 abaixo como as funções de emparelhamento fazem a correspondência biunívoca entre $\mathbb{N}^* \times \mathbb{N}^*$ e $\mathbb{N}^*$.

Agora veremos que existe uma função $S(i,u)$, relacionada ao Teorema Chinês do Resto, que é capaz de decodificar qualquer sequência finita em $\mathbb{N}^*$.

Teorema 3.2 (Teorema da Sequência de Números): *Existe uma função diofantina $S(i,u)$ tal que*

(i) $S(i,u) \leq u$;

(ii) Para cada sequência $a_1, \ldots, a_n$, existe um número u tal que $S(i,u) = a_i$ para $1 \leq i \leq n$.

Demonstração. Defina a função $S : (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$ da seguinte forma: $S(i,u) = w$, onde w é o único inteiro positivo para o qual

$$w \equiv L(u) \pmod{1 + iR(u)}$$

$$w \leq 1 + iR(u).$$

Primeiramente vamos mostrar que $S(i,u)$ é uma função diofantina. Veja que $w = S(i,u) \iff \exists z \in \mathbb{N}^*$ tal que $L(u) = (z-1)(1+iR(u))+w$ e $0 < w \leq 1+iR(u) \iff \exists x,y,z,v \in \mathbb{N}^*$ tais que

$$\begin{cases} 2u = (x+y-2)(x+y-1)+2y \\ x = (z-1)(1+iy)+w \\ 1+iy = w+v-1 \end{cases}$$

$\iff \exists x,y,z,v \in \mathbb{N}^*$ tais que

$$(2u-(x+y-2)(x+y-1)-2y)^2 + (x-(z-1)(1+iy)-w)^2 + (1+iy-w-v+1)^2 = 0.$$

Portanto, $S(i,u)$ é uma função diofantina. Agora, veja que $S(i,u) \leq u$. De fato, como

$$L(u) = (z-1)(1+iR(u)) + w$$

temos que $w \leq L(u) \leq u$. Logo, $S(i,u) \leq u$.

Finalmente, seja $a_1, \ldots, a_n$ uma sequência de números. Escolha $y \in \mathbb{N}^*$ tal que $y > a_i$, $1 \leq i \leq n$, e $j \mid y$, $1 \leq j \leq n$. Observe que os números $1+y$, $1+2y$, $\ldots$, $1+ny$ são primos entre si. De fato, se $d \mid 1+iy$ e $d \mid 1+jy$, com $1 \leq i < j \leq n$, então

$$d \mid j(1+iy) - i(1+jy),$$

assim, $d \mid j-i$. Como $d \leq j-i \leq n$ temos que $d \mid y$. De $d \mid y$ e $d \mid 1+iy$, segue que $d=1$. Sendo assim, podemos aplicar o Teorema Chinês do Resto para obtermos um número x tal que

$$\begin{cases} x \equiv a_1 \pmod{1+y} \\ x \equiv a_2 \pmod{1+2y} \\ \vdots \\ x \equiv a_n \pmod{1+ny}. \end{cases}$$

Se definirmos $u = P(x,y)$, então $x = L(u)$ e $y = R(u)$. Logo, para $1 \leq i \leq n$ teremos que

$$a_i \equiv L(u) \pmod{1+iR(u)}$$

$$a_i < y = R(u) < 1+iR(u),$$

isto é, $a_i = S(i,u)$. □

Teorema 3.3: *Um conjunto S de inteiros positivos é diofantino se, e somente se, existe um polinômio p tal que S é precisamente o conjunto dos inteiros positivos na imagem da função definida por p.*

Demonstração. Suponha que S é diofantino, logo existe um polinômio q tal que:

$$x \in S \iff \exists x_1, \ldots, x_m \in \mathbb{N}^* \text{ tais que } q(x, x_1, \ldots, x_m) = 0.$$

Seja

$$p(x, x_1, \ldots, x_m) := x(1 - q^2(x, x_1, \ldots, x_m)).$$

Dado $x \in S$, escolha $x_1, \ldots, x_m \in \mathbb{N}^*$ tal que $q(x, x_1, \ldots, x_m) = 0$, logo $p(x, x_1, \ldots, x_m) = x$, e portanto, x está no conjunto imagem da função definida por p. Agora, seja $z \in \mathbb{N}^*$ tal que

$$z = p(x, x_1, \ldots, x_m).$$

Como $z = x(1 - q^2(x, x_1, \ldots, x_m))$ e $x > 0$, segue que

$$1 - q^2(x, x_1, \ldots, x_m) > 0,$$

então $q^2(x, x_1, \ldots, x_m) < 1$, ou seja, $q^2(x, x_1, \ldots, x_m) = 0$, assim, temos que

$$q(x, x_1, \ldots, x_m) = 0.$$

Como

$$z = x(1 - q^2(x, x_1, \ldots, x_m)) = x,$$

então $q(z, x_1, \ldots, x_m) = 0$. Portanto, $z \in S$.

Reciprocamente, seja S o conjunto dos inteiros positivos na imagem da função definida por p. Então, $x \in S \iff \exists x_1, \ldots, x_m \in \mathbb{N}^*$ tal que $p(x_1, \ldots, x_m) = x$. Defina

$$f(x, x_1, \ldots, x_m) = x - p(x_1, \ldots, x_m).$$

Então, $x \in S \iff \exists x_1, \ldots, x_m \in \mathbb{N}^*$ tal que $f(x, x_1, \ldots, x_m) = 0$. Portanto, S é diofantino. □

4 AS EQUAÇÕES DE PELL

A função exponencial $h : (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$, $h(n,k) = n^k$ é diofantina. Para provar este resultado será necessário utilizar diversos resultados sobre as Equações de Pell. Esse resultado servirá de base para mostrarmos que outras funções importantes também são diofantinas. As demonstrações para os próximos Lemas (4.1-4.14) encontram-se em [3]. O Lema 4.15 foi acrescentado, pois será necessário na demonstração do Teorema 5.1.

Definição 4.1: *A Equação de Pell é dada por:* $x^2 - dy^2 = 1$, *com* $x, y \in \mathbb{Z}$, *onde tomaremos* $d = a^2 - 1$, $a > 1$.

Observe que $(x,y) = (1,0)$ e $(x,y) = (a,1)$ são soluções triviais da Equação de Pell.

Definição 4.2: $x_n(a)$ *e* $y_n(a)$ *para* $n \geq 0$ *e* $a > 1$, *são definidos por*

$$x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n.$$

Lema 4.1: x_n *e* y_n *satisfazem a Equação de Pell, para todo* $n \in \mathbb{N}^*$. *E se* (x,y) *é uma solução não negativa da Equação de Pell. Então, existe* $n \in \mathbb{N}$ *tal que* $x = x_n$ *e* $y = y_n$.

Lema 4.2: $(x_n, y_n) = 1$.

Lema 4.3: *Sejam* $n, t \in \mathbb{N}^*$. *Então,* $y_n \mid y_t \iff n \mid t$.

Lema 4.4: $y_n^2 \mid y_{ny_n}$.

Lema 4.5: $y_n^2 \mid y_t \Longrightarrow y_n \mid t$.

Lema 4.6: $x_{n+1} = 2ax_n - x_{n-1}$ *e* $y_{n+1} = 2ay_n - y_{n-1}$, $\forall n \in \mathbb{N}^*$.

Observe que estas equações mais as condições iniciais $x_0 = 1$, $x_1 = a$, $y_0 = 0$ e $y_1 = 1$ determinam recursivamente todos os valores de x_n e y_n.

Lema 4.7: $y_n \equiv n \pmod{a-1}$, $\forall n \in \mathbb{N}$.

Lema 4.8: *Se* $a \equiv b \pmod{c}$, *então* $x_n(a) \equiv x_n(b) \pmod{c}$ *e* $y_n(a) \equiv y_n(b) \pmod{c}$, $\forall n \in \mathbb{N}$.

Lema 4.9: *Quando* n *é par,* y_n *é par e quando* n *é ímpar,* y_n *é ímpar.*

Lema 4.10: $x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$.

Lema 4.11: $y_{n+1} > y_n \geq n$, $\forall n \in \mathbb{N}$.

Lema 4.12: $a^n \leq x_n(a) < x_{n+1}(a)$ *e* $x_n(a) \leq (2a)^n$, $\forall n \in \mathbb{N}$.

Lema 4.13: *Seja* $0 < i \leq n$ *e* $x_j \equiv x_i \pmod{x_n}$, *então* $j \equiv \pm i \pmod{4n}$.

Lema 4.14: *Se* $a > y^k \geq 1$, *então* $2ay - y^2 - 1 > y^k$.

Lema 4.15: $b > a \Longrightarrow x_n(b) > x_n(a)$ *e* $y_n(b) \geq y_n(a)$.

Demonstração. (Indução sobre n) Para $n = 0$ o resultado se verifica. Suponha que o Lema seja verdadeiro para $n = k$. Então,

$$y_{k+1}(b) = by_k(b) + x_k(b) \geq ay_k(a) + x_k(a) = y_{k+1}(a).$$

Além disso,

$$x_{k+1}(b) = bx_k(b) + (b^2-1)y_k(b) > ax_k(a) + (a^2-1)y_k(a) = x_{k+1}(a).$$

□

5 A FUNÇÃO EXPONENCIAL É DIOFANTINA

Considere o seguinte sistema de equações diofantinas:

$$\begin{array}{ll}(i) & x^2-(a^2-1)y^2=1\\ (ii) & u^2-(a^2-1)v^2=1\\ (iii) & s^2-(b^2-1)t^2=1\\ (iv) & v=ry^2\\ (v) & b=1+4py=a+qu\\ (vi) & s=x+cu\\ (vii) & t=k+4(d-1)y\\ (viii) & y=k+e-1\end{array}$$

Teorema 5.1: *Dados a,x,k, com $a>1$, o sistema $(i)-(viii)$ tem solução nos argumentos restantes y,u,v,s,t,b,r,p,q,c,d,e se, e somente se, $x=x_k(a)$.*

Demonstração. Primeiramente, consideremos dada uma solução de $(i)-(viii)$. De (v) temos que $b>a>1$. Por (i), (ii), (iii) e pelo Lema 4.1, concluímos que existem $i,j,n>0$ tais que:

$$x=x_i(a),\quad y=y_i(a),\quad u=x_n(a),\quad v=y_n(a),\quad s=x_j(b),\quad t=y_j(b).$$

De (iv), temos $y\leq v$ e, portanto, $i\leq n$. As equações (v) e (vi) produzem as seguintes congruências:

$$b\equiv a \pmod{x_n(a)},$$

$$x_i(a)\equiv x_j(b) \pmod{x_n(a)},$$

e, pelo Lema 4.8,

$$x_j(b)\equiv x_j(a) \pmod{x_n(a)}.$$

Logo,

$$x_i(a)\equiv x_j(a) \pmod{x_n(a)}.$$

Do Lema 4.13, temos $j\equiv\pm i \pmod{4n}$. Da equação (iv), $(y_i(a))^2 \mid y_n(a)$ e, do Lema 4.5, $y_i(a)\mid n$. Daí (i) implica que

$$j\equiv\pm i \pmod{4y_i(a)}.$$

Da equação (vii),

$$y_j(b)\equiv k \pmod{4y_i(a)}.$$

Por transitividade,

$$k\equiv\pm i \pmod{4y_i(a)}.$$

Pela equação $(viii)$, $k\leq y_i(a)$ e, do Lema 4.11, $i\leq y_i(a)$. Assim, $-y_i(a)<k-i<y_i(a)$. Como

$$k\equiv\pm i \pmod{4y_i(a)},$$

temos que $4y_i(a)\mid k\pm i$ e $-y_i(a)<k-i<y_i(a)$, logo $k\pm i=0$. Como $k+i>0$, temos $k-i=0$, isto é, $k=i$. Portanto, $x=x_i(a)=x_k(a)$.

Reciprocamente, suponha que $x=x_k(a)$. Assim, $y=y_k(a)$ satisfaz (i). Considere

$$m=2ky_k(a)$$

e sejam $u=x_m(a)$ e $v=y_m(a)$, então (ii) é satisfeita. Pelo Lema 4.4, temos que $y_k^2\mid y_{ky_k}$, mas $ky_k\mid m$, pelo Lema 4.3, $y_{ky_k}\mid y_m$. Por transitividade, $y_k^2\mid y_m$, isto é, $y_k^2\mid v$. Com isso, podemos escolher r satisfazendo (iv). Além disso, como m é par, pelo Lema 4.9, temos que v é par, e como u e v satisfazem (ii) segue que u é ímpar. Pelo Lema 4.2, $(u,v)=1$. Afirmação:

$(u, 4y) = 1$. De fato, seja p um primo tal que $p \mid u$ e $p \mid 4y$. Como u é ímpar e $p \mid u$, temos que p é ímpar e por $p \mid 4y$ devemos ter que $p \mid y$. Como

$$m = 2ky_k(a)$$

temos que $k \mid m$ e, pelo Lema 4.3, $y_k \mid y_m$. Isto é, $y \mid v$, logo, $p \mid v$. Como $(u, v) = 1$, $p \mid u$ e $p \mid v$, temos que $p \mid 1$, absurdo. Portanto, $(u, 4y) = 1$. Pelo Teorema Chinês do Resto, podemos encontrar b_0 tal que:

$$b_0 \equiv 1 \pmod{4y}$$

$$b_0 \equiv a \pmod{u}.$$

Como $4jyu \equiv 0 \pmod{4y}$ e $4jyu \equiv 0 \pmod{u}$, então $b_0 + 4jyu$ também satisfaz as congruências e, portanto, podemos encontrar b, p, q satisfazendo a equação (v). Definindo $s = x_k(b)$ e $t = y_k(b)$, (iii) é satisfeita. Por (v), $b > a$ e pelo Lema 4.15,

$$x_k(b) > x_k(a).$$

Isto é, $s > x$. Pelo Lema 4.8 e utilizando (v),

$$s \equiv x \pmod{u}.$$

Assim, podemos escolher c de forma a satisfazer (vi). Do Lema 4.11, $y_k \geq k$, ou seja, $t \geq k$ e, pelo Lema 4.7,

$$y_k = t \equiv k \pmod{b - 1}.$$

Assim, usando (v),

$$t \equiv k \pmod{4y},$$

logo, podemos escolher d satisfazendo a equação (vii). Novamente, pelo Lema 4.11, $y \geq k$. Assim, $\exists e \in \mathbb{N}^*$ tal que

$$y = k + e - 1,$$

logo $(viii)$ é satisfeita. □

O Teorema 5.1 implica que o conjunto

$$M = \{(a, x, k) : x = x_k(a)\}$$

é diofantino. Isto é obtido aplicando a Proposição 2.1 para reduzir a só uma equação o sistema de equações diofantinas $(i) - (viii)$.

Corolário 5.1: *A função $g(z, k) = x_k(z + 1)$ é diofantina.*

Demonstração. Adicionando ao sistema $(i) - (viii)$ a equação $a = z + 1$, pelo Teorema 5.1,

$$M_0 = \{(z, k, x) : x = g(z, k)\}$$

é diofantino. Portanto, g é uma função diofantina. □

Agora, inclua ao sistema $(i) - (viii)$ as seguintes equações:

$$\begin{array}{ll} (ix) & (x - y(a - n) - m)^2 = (f - 1)^2(2an - n^2 - 1)^2 \\ (x) & m + g = 2an - n^2 - 1 \\ (xi) & w = n + h = k + l \\ (xii) & a^2 - (w^2 - 1)(w - 1)^2 z^2 = 1 \end{array}$$

Lema 5.1: *$m = n^k$ se, e somente se, as equações $(i) - (xii)$ tem uma solução nos argumentos restantes.*

Demonstração. Suponha que $(i)-(xii)$ é satisfeito. Por (xi), $w>1$, assim, $(w-1)z>0$, e por (xii), $a>1$. Aplicando o Teorema 5.1 segue que $x=x_k(a)$ e $y=y_k(a)$. Por (ix), temos

$$x_k - y_k(a-n) \equiv m \pmod{2an-n^2-1}$$

e pelo Lema 4.10,

$$x_k - y_k(a-n) \equiv n^k \pmod{2an-n^2-1}.$$

Por transitividade,

$$m \equiv n^k \pmod{2an-n^2-1}.$$

Da equação (xi) segue que $n,k<w$. De (xii) e do Lema 4.1, $\exists j \in \mathbb{N}^*$ tal que $a=x_j(w)$ e

$$(w-1)z = y_j(w).$$

Do Lema 4.7,

$$y_j(w) \equiv j \pmod{w-1}$$

e como

$$y_j(w) \equiv 0 \pmod{w-1},$$

temos que

$$j \equiv 0 \pmod{w-1}.$$

Como $w-1 \mid j$ e $j \neq 0$, segue que $w-1 \leq j$. Do Lema 4.12, $x_j(w) \geq w^j$, ou seja, $a \geq w^j$. Observe que

$$a \geq w^j \geq w^{w-1} > n^{w-1} \geq n^k;$$

logo, $a>n^k$. Por (x),

$$m < 2an-n^2-1$$

e pelo Lema 4.14,

$$n^k < 2an-n^2-1.$$

Como

$$m \equiv n^k \pmod{2an-n^2-1}$$
$$m, n^k < 2an-n^2-1$$

concluímos que $m=n^k$.

Reciprocamente, suponha que $m=n^k$. Devemos encontrar soluções para o sistema $(i)-(xii)$. Escolha algum w tal que $w>n,k$. Seja $a=x_{w-1}(w)$ tal que $a>1$. Pelo Lema 4.7,

$$y_{w-1}(w) \equiv w-1 \equiv 0 \pmod{w-1}.$$

Assim, $\exists z \in \mathbb{N}^*$ tal que

$$y_{w-1}(w) = z(w-1).$$

Tomando $a=x_{w-1}(w)$ e $z(w-1)=y_{w-1}(w)$, temos que (xii) é satisfeita. Definindo $h=w-n$ e $l=w-k$, temos que (xi) é satisfeita. Como anteriormente, $a>n^k$, e novamente pelo Lema 4.14,

$$m=n^k < 2an-n^2-1.$$

Daí, $\exists g \in \mathbb{N}^*$ tal que

$$m+g = 2an-n^2-1,$$

assim, (x) é satisfeita. Definindo $x=x_k(a)$ e $y=y_k(a)$, pelo Lema 4.10, podemos definir f tal que

$$x-y(a-n)-m = \pm(f-1)(2an-n^2-1)$$

de forma que (ix) é satisfeita. Finalmente, pelo Teorema 5.1, segue que $(i)-(viii)$ é satisfeito. □

Teorema 5.2: *A função exponencial $h(n,k) = n^k$ é diofantina.*

Demonstração. Pelo Lema 5.1, temos que o conjunto

$$N = \{(m,n,k) \in (\mathbb{N}^*)^3 : m = n^k\}$$

é diofantino. Portanto, a função exponencial $h(n,k) = n^k$ é diofantina. □

6 AS FUNÇÕES COMBINATORIAL E FATORIAL SÃO DIOFANTINAS

Agora que provamos que a função exponencial é diofantina, podemos mostrar que muitas outras funções e conjuntos também são. Por exemplo, a função

$$h(u,v,w) = u^{v^w}$$

é diofantina. De fato, $y = u^{v^w} \iff \exists z \in \mathbb{N}^*$ tal que $y = u^z$ e $z = v^w$. Pelo Teorema 5.2, existe um polinômio P tal que

$$\begin{aligned} y = u^z &\iff \exists r_1, \ldots, r_n \in \mathbb{N}^* \text{ tais que } P(y,u,z,r_1,\ldots,r_n) = 0; \\ z = v^w &\iff \exists s_1, \ldots, s_n \in \mathbb{N}^* \text{ tais que } P(z,v,w,s_1,\ldots,s_n) = 0. \end{aligned}$$

Logo, $y = u^{v^w} \iff \exists z, r_1, \ldots, r_n, s_1, \ldots, s_n \in \mathbb{N}^*$ tais que

$$P^2(y,u,z,r_1,\ldots,r_n) + P^2(z,v,w,s_1,\ldots,s_n) = 0.$$

Portanto, h é diofantina.

Definição 6.1: *Seja $\alpha \in \mathbb{R}$. Então, definimos $[\alpha]$ como sendo o único inteiro tal que*

$$[\alpha] \leq \alpha < [\alpha] + 1.$$

Lema 6.1: *Para $0 < k \leq n$ e $u > 2^n$, temos que*

$$\left[\frac{(u+1)^n}{u^k}\right] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}.$$

Demonstração. Pelo Binômio de Newton temos que

$$\frac{1}{u^k}(u+1)^n = \frac{1}{u^k}\sum_{i=0}^{n}\binom{n}{i}u^i = \sum_{i=0}^{n}\binom{n}{i}u^{i-k} = \sum_{i=0}^{k-1}\binom{n}{i}u^{i-k} + \sum_{i=k}^{n}\binom{n}{i}u^{i-k} = R + S,$$

onde

$$R = \sum_{i=0}^{k-1}\binom{n}{i}u^{i-k} \text{ e } S = \sum_{i=k}^{n}\binom{n}{i}u^{i-k}.$$

Observe que $S \in \mathbb{Z}$, pois $i \geq k$. Além disso,

$$R \leq u^{-1}\sum_{i=0}^{k-1}\binom{n}{i} < u^{-1}\sum_{i=0}^{n}\binom{n}{i} = u^{-1}(1+1)^n = \frac{2^n}{u} < 1.$$

Portanto,

$$S \leq S + R = \frac{(u+1)^n}{u^k} < S + 1,$$

ou seja, $S = [S+R]$. □

Lema 6.2: *Se $0 < k \leq n$ e $u > 2^n$, então* $\left[\frac{(u+1)^n}{u^k}\right] \equiv \binom{n}{k} \pmod{u}$.

Demonstração. Pelo Lema 6.1, temos que

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

$$\binom{n}{k} + \binom{n}{k+1}u + \binom{n}{k+2}u^2 + \cdots + \binom{n}{n}u^{n-k} \equiv \binom{n}{k} \pmod{u}.$$

□

Lema 6.3: *A função* $f(n,k) = \binom{n}{k}$ *é diofantina.*

Demonstração. Seja $u \in \mathbb{N}^*$ tal que $u > 2^n$. Então,

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

Pelo Lema 6.2, $\left[\frac{(u+1)^n}{u^k}\right] \equiv \binom{n}{k} \pmod{u}$ e sabemos que $0 < \binom{n}{k} < u$, então, temos que

$$z = \binom{n}{k} \iff \exists u, v, w \in \mathbb{N}^* \text{ tais que } v = 2^n \text{ e } u > v \text{ e}$$

$$w = \left[\frac{(u+1)^n}{u^k}\right] \text{ e } z \equiv w \pmod{u} \text{ e } z < u.$$

Como a função exponencial é diofantina, então $v = 2^n$ determina o conjunto diofantino

$$\{(n, v) \in (\mathbb{N}^*)^2 : v = 2^n\}.$$

A desigualdade $u > v$ também determina um conjunto diofantino. Além disso, $z \equiv w \pmod{u}$ e $z < u \iff \exists x, y \in \mathbb{N}^*$ tais que $w = z + (x-1)u$ e $u = z + y$. Finalmente,

$$w = \left[\frac{(u+1)^n}{u^k}\right] \iff \exists x, y, t \in \mathbb{N}^* \text{ tais que } t = u+1 \text{ e } x = t^n \text{ e } y = u^k \text{ e } w \leq \frac{x}{y} < w+1.$$

□

As funções combinatorial e exponencial serem diofantinas nos permite mostrar que a função fatorial é diofantina.

Lema 6.4: $r > (2x)^{x+1} \implies x! = \left[\frac{r^x}{\binom{r}{x}}\right]$.

Demonstração. Seja $r > (2x)^{x+1}$. Então,

$$\frac{r^x}{\binom{r}{x}} = r^x \frac{x!(r-x)!}{r!} = \frac{r^x x!}{r(r-1)\cdots(r-x+1)} = \frac{x!}{(1-\frac{1}{r})\cdots(1-\frac{x-1}{r})} < \frac{x!}{(1-\frac{x}{r})^{x-1}} < \frac{x!}{(1-\frac{x}{r})^x}.$$

Mas, como $r > (2x)^{x+1}$, temos que $\frac{x}{r} < \frac{x}{2x(2x)^x} < \frac{1}{2}$. Então,

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

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

Daí,

$$\left(1+\frac{2x}{r}\right)^x = \sum_{j=0}^{x}\binom{x}{j}\left(\frac{2x}{r}\right)^j < 1+\frac{2x}{r}\sum_{j=1}^{x}\binom{x}{j} = 1+\frac{2x}{r}(2^x-1) < 1+\frac{2x}{r}2^x.$$

Assim,

$$\frac{r^x}{\binom{r}{x}} < \frac{x!}{(1-\frac{x}{r})^x} < x!\left(1+\frac{2x}{r}\right)^x < x!\left(1+\frac{2x}{r}2^x\right) =$$

$$x! + \frac{2^{x+1}}{r}xx! < x! + \frac{2^{x+1}}{r}xx^x = x! + \frac{(2x)^{x+1}}{r}.$$

Por hipótese,

$$\frac{(2x)^{x+1}}{r} < 1,$$

logo,

$$\frac{r^x}{\binom{r}{x}} < x! + \frac{(2x)^{x+1}}{r} < x! + 1.$$

Como,

$$\frac{r^x}{r(r-1)\cdots(r-x+1)} \geq 1,$$

então

$$x! \leq \frac{r^x x!}{r(r-1)\cdots(r-x+1)} = \frac{r^x}{\binom{r}{x}} < x! + 1.$$

Portanto, $x! = \left[\dfrac{r^x}{\binom{r}{x}}\right]$. □

Lema 6.5: *$f(n) = n!$, $n \in \mathbb{N}^*$ é uma função diofantina.*

Demonstração.

$$m = n! \iff \exists r, s, t, u, v \in \mathbb{N}^* \text{ tais que } s = 2n+1 \text{ e } t = n+1 \text{ e}$$

$$r = s^t \text{ e } u = r^n \text{ e } v = \binom{r}{n} \text{ e } mv \leq u < (m+1)v.$$

De fato, suponha que $m = n!$. Defina $s = 2n+1$, $t = n+1$, $r = s^t$, $u = r^n$ e $v = \binom{r}{n}$. Como $m, n > 0$, temos que $s, t, r, u, v > 0$. Observe que

$$r = s^t = (2n+1)^{n+1} > (2n)^{n+1},$$

e pelo Lema 6.4,

$$m = n! = \left[\frac{r^n}{\binom{r}{n}}\right],$$

ou seja,

$$m \leq \frac{u}{v} < m+1,$$

logo,

$$mv \leq u < (m+1)v.$$

Reciprocamente, suponha que $\exists r, s, t, u, v \in \mathbb{N}^*$ tais que $s = 2n+1$ e $t = n+1$ e $r = s^t$ e $u = r^n$ e $v = \binom{r}{n}$ e $mv \leq u < (m+1)v$. Então, $\left[\dfrac{u}{v}\right] = m$, isto é,

$$\left[\frac{r^n}{\binom{r}{n}}\right] = m.$$

Como

$$r = s^t = (2n+1)^{n+1} > (2n)^{n+1},$$

pelo Lema 6.4,

$$n! = \left\lfloor \frac{r^n}{\binom{r}{n}} \right\rfloor = m.$$

□

Lema 6.6: $bq \equiv a \pmod{m} \Longrightarrow \prod_{k=1}^{y}(a+bk) \equiv b^y y! \binom{q+y}{y} \pmod{m}$.

Demonstração. Veja que

$$b^y y! \binom{q+y}{y} = b^y \frac{(q+y)!}{q!} =$$

$$b^y (q+y)(q+y-1)\cdots(q+1) = (bq+by)(bq+b(y-1))\cdots(bq+b).$$

Como,

$$bq \equiv a \pmod{m},$$

temos que

$$(bq+by)(bq+b(y-1))\cdots(bq+b) \equiv (a+by)(a+b(y-1))\cdots(a+b) \pmod{m}.$$

Portanto,

$$\prod_{k=1}^{y}(a+bk) \equiv b^y y! \binom{q+y}{y} \pmod{m}.$$

□

Como consequência do fato de que as funções exponencial, combinatorial e fatorial são diofantinas, obtemos uma nova função diofantina:

Lema 6.7: $h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ *é uma função diofantina.*

Demonstração. Considere $m = b(a+bk)^y + 1$. Então, $(m,b) = 1$ e

$$0 < \prod_{k=1}^{y}(a+bk) < m,$$

assim, a congruência

$$bx \equiv a \pmod{m}$$

possui uma única solução $x = q$ tal que $0 \leq q < m$. Como

$$bq \equiv a \pmod{m},$$

pelo Lema 6.6,

$$\prod_{k=1}^{y}(a+bk) \equiv b^y y! \binom{q+y}{y} \pmod{m}$$

e sabemos que

$$0 < \prod_{k=1}^{y}(a+bk) < m.$$

Então,

$$z = \prod_{k=1}^{y}(a+bk) \Longleftrightarrow \exists m,p,q,r,s,t,u,v,w,x \in \mathbb{N}^* \text{ tais que}$$

$$r = a + by \text{ e } s = r^y \text{ e } m = bs + 1 \text{ e } bq = a + mt \text{ e } u = b^y \text{ e } v = y!$$

$$\text{e } z < m \text{ e } w = q + y \text{ e } x = \binom{w}{y} \text{ e } z + mp = uvx.$$

Como as funções exponencial, combinatorial e fatorial são diofantinas, segue que h é uma função diofantina. □

7 NOVOS CONJUNTOS DIOFANTINOS

Com este Lema 6.7, combinado com os próximos Lemas 7.1 e 7.2, poderemos mostrar que é diofantino o seguinte conjunto:

$$S = \{(y, x_1, \ldots, x_n) \in (\mathbb{N}^*)^{n+1} : \forall z \in \mathbb{N}^* \text{ com } z \leq y, \ \exists y_1, \ldots, y_m \in \mathbb{N}^* \\ \text{tais que } P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\},$$

onde P é um polinômio qualquer.

Este conjunto S ser diofantino será fundamental para provar o Teorema da Universalidade e o Teorema que caracteriza as funções diofantinas.

Lema 7.1:

$$\forall k \in \mathbb{N}^* \textit{ com } k \leq y, \ \exists y_1, \ldots, y_m \in \mathbb{N}^* \textit{ tais que } P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$
$$\Updownarrow$$
$$\exists u \in \mathbb{N}^* \textit{ tal que } \forall k \in \mathbb{N}^* \textit{ com } k \leq y, \ \exists y_1, \ldots, y_m \in \mathbb{N}^* \textit{ com}$$
$$y_i \leq u, \ i = 1, \ldots, m \textit{ tais que } P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Demonstração. ($\Longrightarrow$) Por hipótese, para cada $k \in \{1, 2, \ldots, y\}$, $\exists y_1^k, \ldots, y_m^k \in \mathbb{N}^*$ para os quais

$$P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) = 0.$$

Tomando

$$u = \max\{y_j^k : j = 1, \ldots, m, \ \ k = 1, \ldots, y\},$$

segue que $\exists u \in \mathbb{N}^*$ tal que $\forall k \in \mathbb{N}^*$ com $k \leq y$, $\exists y_1, \ldots, y_m \in \mathbb{N}^*$ com $y_i \leq u$, $i = 1, \ldots, m$, tais que

$$P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

($\Longleftarrow$) É trivial. □

Lema 7.2: *Sejam $P(y, k, x_1, \ldots, x_n, a_1, \ldots, a_m)$ um polinômio qualquer e $Q(y, u, x_1, \ldots, x_n)$ um polinômio com as propriedades*

(1) $Q(y, u, x_1, \ldots, x_n) > u$,
(2) $Q(y, u, x_1, \ldots, x_n) > y$,
(3) $k \leq y$ *e* $y_1, \ldots, y_m \leq u \Longrightarrow |P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m)| \leq Q(y, u, x_1, \ldots, x_n)$.

Então,

$$\forall k \in \mathbb{N}^* \textit{ com } k \leq y, \ \exists y_1, \ldots, y_m \in \mathbb{N}^* \textit{ tais que } P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$
$$\Updownarrow$$
$$\exists c, t, a_1, \ldots, a_m \in \mathbb{N}^* \textit{ tais que } 1 + ct = \prod_{k=1}^{y}(1 + kt),$$
$$t = Q(y, u, x_1, \ldots, x_n)!, \ \ 1 + ct \mid \prod_{j=1}^{u}(a_1 - j), \ldots, 1 + ct \mid \prod_{j=1}^{u}(a_m - j) \textit{ e}$$
$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \pmod{1 + ct}.$$

Demonstração. ($\Longleftarrow$) Para cada $k \in \{1, 2, \ldots, y\}$ seja p_k um fator primo de $1 + kt$. Seja y_i^k o resto da divisão de a_i por p_k, $k = 1, \ldots, y$ e $i = 1, \ldots, m$. Daí, para cada k, i, segue que

$$(a) \quad 1 \leq y_i^k \leq u \quad (b) \quad P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) = 0.$$

Prova de (a): Note que $p_k \mid 1 + kt$, $1 + kt \mid 1 + ct$ e $1 + ct \mid \prod_{j=1}^{u}(a_i - j)$, por transitividade,

$$p_k \mid \prod_{j=1}^{u}(a_i - j).$$

Como p_k é primo, $p_k \mid a_i - j$, para algum $j \in \{1, \ldots, u\}$. Então,

$$j \equiv a_i \equiv y_i^k \pmod{p_k}.$$

Agora, observe que

$$p \mid 1 + kt \Longrightarrow p > Q(y, u, x_1, \ldots, x_n), \tag{2}$$

para todo primo p. Como $p_k \mid 1 + kt$, temos que

$$p_k > Q(y, u, x_1, \ldots, x_n) > u,$$

logo, $j \leq u < p_k$. Como y_i^k é o resto da divisão de a_i por p_k temos que $y_i^k < p_k$. Assim,

$$j \equiv y_i^k \pmod{p_k},$$

$j < p_k$ e $y_i^k < p_k$, então $j = y_i^k$. Como $1 \leq j \leq u$, segue que $1 \leq y_i^k \leq u$.

Prova de (b): Observe que $p_k \mid 1 + ct$ e $p_k \mid 1 + kt$, então,

$$p_k \mid k(1 + ct) - c(1 + kt),$$

isto é, $p_k \mid k - c$, então, $k \equiv c \pmod{p_k}$. Já sabemos que

$$y_i^k \equiv a_i \pmod{p_k},$$

desse modo,

$$P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) \equiv P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \pmod{p_k},$$

pois $p_k \mid (1 + ct)$. Assim, $P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k)$ é múltiplo de p_k e, por (3), temos que

$$|P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k)| \leq Q(y, u, x_1, \ldots, x_n) < p_k.$$

Portanto,

$$P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) = 0.$$

($\Longrightarrow$) Suponha que

$$P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) = 0,$$

para cada $k = 1, \ldots, y$ e cada $y_j^k \leq u$. Nós fixamos $t = Q(y, u, x_1, \ldots, x_n)!$ e uma vez que

$$\prod_{k=1}^{y}(1 + kt) \equiv 1 \pmod{t},$$

existe $c \in \mathbb{N}^*$ tal que

$$1 + ct = \prod_{k=1}^{y}(1 + kt).$$

Agora, para $1 \leq k < l \leq y$, devemos ter

$$(1+kt, 1+lt) = 1.$$

De fato, suponha que exista um primo p tal que $p \mid 1+kt$ e $p \mid 1+lt$, então $p \mid (l-k)t$. Se ocorresse $p \mid l-k$, teríamos que $p \leq l-k < y$ e, assim,

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

Mas por (2) temos que $p > Q(y, u, x_1, \ldots, x_n)$. Logo, p não divide $l-k$. Como p é primo, $p \mid t$, logo, $p \mid 1$, contradição. Portanto, $(1+kt, 1+lt) = 1$. Desse modo, os números $1+kt$ são primos entre si, e o Teorema Chinês do Resto pode ser aplicado para produzir, para cada $i = 1, \ldots, m$, um número a_i tal que

$$a_i \equiv y_i^k \pmod{1+kt}, \quad k = 1, \ldots, y.$$

Como $1+kt \mid 1+ct$, temos que

$$1+kt \mid k(1+ct) - c(1+kt),$$

ou seja, $1+kt \mid k-c$, logo,

$$k \equiv c \pmod{1+kt}.$$

Assim, para cada $k = 1, \ldots, y$, temos que

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) \pmod{1+kt}.$$

Como $P(y, k, x_1, \ldots, x_n, y_1^k, \ldots, y_m^k) = 0$, temos que

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \pmod{1+kt}.$$

Como os números $1+kt$ são primos entre si e cada um divide $P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m)$, temos que

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \pmod{1+ct},$$

pois

$$1+ct = \prod_{k=1}^{y}(1+kt) \mid P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m).$$

Finalmente,

$$a_i \equiv y_i^k \pmod{1+kt},$$

isto é,

$$1+kt \mid a_i - y_i^k,$$

e como $1 \leq y_i^k \leq u$, temos que

$$1+kt \mid \prod_{j=1}^{u}(a_i - j).$$

E novamente, como os números $1+kt$ são primos entre si, segue que

$$\prod_{k=1}^{y}(1+kt) \mid \prod_{j=1}^{u}(a_i - j),$$

isto é,

$$1+ct \mid \prod_{j=1}^{u}(a_i - j).$$

□

Teorema 7.1: *Se P é um polinômio a coeficientes inteiros, então são diofantinos os seguintes conjuntos:*

$$R = \{(y, x_1, \ldots, x_n) \in (\mathbb{N}^*)^{n+1} : \exists z \in \mathbb{N}^* \textit{ com } z \leq y \textit{ e } \exists y_1, \ldots, y_m \in \mathbb{N}^* \textit{ tais que } P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

$$S = \{(y, x_1, \ldots, x_n) \in (\mathbb{N}^*)^{n+1} : \forall z \in \mathbb{N}^* \textit{ com } z \leq y \textit{ e } \exists y_1, \ldots, y_m \in \mathbb{N}^* \textit{ tais que } P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

Demonstração. Como $(y, x_1, \ldots, x_n) \in R \iff \exists z, y_1, \ldots, y_m \in \mathbb{N}^*$ tais que $z \leq y$ e

$$P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0,$$

segue que R é um conjunto diofantino. Para mostrar que S é diofantino, primeiro encontre um polinômio Q satisfazendo (1), (2) e (3) do Lema 7.2. Para isso, escreva

$$P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{r=1}^{N} t_r,$$

onde cada t_r tem a seguinte forma

$$t_r = c_r y^a k^b x_1^{q_1} \cdots x_n^{q_n} y_1^{s_1} \cdots y_m^{s_m},$$

onde $c_r \in \mathbb{Z}$. Sejam

$$u_r = |c_r| y^{a+b} x_1^{q_1} \cdots x_n^{q_n} u^{s_1 + \cdots + s_m}$$

$$Q(y, u, x_1, \ldots, x_n) = u + y + \sum_{r=1}^{N} u_r.$$

Assim, (1), (2) e (3) são trivialmente satisfeitos. Desse modo,

$$\begin{gathered}
\forall k \in \{1, \ldots, y\}, \ \exists y_1, \ldots, y_m \in \mathbb{N}^* \text{ tais que } P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0 \\
\Updownarrow \\
\exists u, c, t, a_1, \ldots, a_m \in \mathbb{N}^* \text{ tais que } 1 + ct = \prod_{k=1}^{y} (1 + kt), \ t = Q(y, u, x_1, \ldots, x_n)!, \\
1 + ct \mid \prod_{j=1}^{u} (a_1 - j), \ldots, 1 + ct \mid \prod_{j=1}^{u} (a_m - j) \text{ e} \\
P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \pmod{1 + ct} \\
\Updownarrow \\
\exists u, c, t, a_1, \ldots, a_m, e, f, g_1, \ldots, g_m, h_1, \ldots, h_m, l \in \mathbb{N}^* \text{ tais que} \\
e = 1 + ct, \ e = \prod_{k=1}^{y} (1 + kt), \ f = Q(y, u, x_1, \ldots, x_n), \ t = f!, \ g_1 = a_1 - u - 1, \\
g_2 = a_2 - u - 1, \ldots, g_m = a_m - u - 1, \ h_1 = \prod_{k=1}^{u} (g_1 + k), \ldots, h_m = \prod_{k=1}^{u} (g_m + k), \\
e \mid h_1, \ldots, e \mid h_m, \ l = P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m), \ e \mid l.
\end{gathered}$$

□

8 FUNÇÕES RECURSIVAS

Para definir função recursiva considere a função $S(i, u)$ definida no Teorema 3.2.

Definição 8.1: *Funções Recursivas são aquelas que podem ser obtidas a partir das funções recursivas iniciais*

$$\begin{cases} c(x) = 1; \\ S(x) = x + 1; \\ U_i^n(x_1, \ldots, x_n) = x_i, \qquad 1 \leq i \leq n; \\ S(i, u), \end{cases}$$

aplicando iterativamente três operações básicas. Uma função recursiva h pode ser definida por:

Composição:

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)),$$

a partir das funções recursivas $g_1, \ldots, g_m$ e f dadas.

Recursão Primitiva:

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

a partir das funções recursivas f, g dadas.

Minimização:

$$h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)],$$

a partir das funções recursivas f, g dadas e assumindo que para cada $x_1, \ldots, x_n$ existe pelo menos um y satisfazendo a equação:

$$f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y).$$

Observe que a classe das funções recursivas nos dá todas as funções calculáveis.

Proposição 8.1: *A função $h(x, y) = x + y$ é recursiva.*

Demonstração. Defina

$$g(u, v, w) = S(U_2^3(u, v, w)) = S(v) = v + 1$$

$$f(x) = S(x) = x + 1,$$

então f e g são recursivas. Agora, considere a função $h(x, t)$ definida por

$$h(x, 1) = f(x) = x + 1,$$
$$h(x, t+1) = g(t, h(x, t), x).$$

Portanto, $h(x, t) = x + t$, e por recursão primitiva, h é recursiva. □

Proposição 8.2: *A função $h(x, y) = xy$ é recursiva.*

Demonstração. Defina

$$f(x) = U_1^1(x) = x$$

$$g(u, v, w) = S_s(U_2^3(u, v, w), U_3^3(u, v, w)),$$

onde $S_s(a, b) = a + b$. Então, f e g são recursivas. Agora, considere a função $h(x, t)$ definida por

$$h(x, 1) = f(x) = x \cdot 1,$$
$$h(x, t+1) = g(t, h(x, t), x).$$

Logo, $h(x, t) = xt$, e por recursão primitiva, h é recursiva. □

Proposição 8.3: *Para cada $k \in \mathbb{N}^*$, a função constante $c_k(x) = k$ é recursiva.*

Demonstração. (Indução sobre k) Para $k = 1$ vale o resultado. Suponha que $c_k(x) = k$ é recursiva, então

$$c_{k+1}(x) = k + 1 = c_k(x) + c(x)$$

é recursiva, pois,

$$c_{k+1}(x) = S_s(c_k(x), c(x)),$$

onde $S_s(a, b) = a + b$. □

Observe que todos os polinômios $P(x_1, \ldots, x_n)$ com coeficientes inteiros positivos são recursivos. Basta expressar estas funções por uma iteração finita de adição, multiplicação de variáveis e $c(x)$. Por exemplo

$$2x^2y + 3xz^3 + 5 = c_2(x)xxy + c_3(x)xzzz + c_5(x).$$

O próximo teorema nos fornecerá uma caracterização das funções diofantinas.

Teorema 8.1: *Uma função é diofantina se, e somente se, é recursiva.*

Demonstração. Seja f uma função diofantina, $y = f(x_1, \ldots, x_n) \iff \exists t_1, \ldots, t_m \in \mathbb{N}^*$ tais que

$$P(x_1, \ldots, x_n, y, t_1, \ldots, t_m) = Q(x_1, \ldots, x_n, y, t_1, \ldots, t_m),$$

onde P e Q são polinômios com coeficientes inteiros e positivos. Sejam $x_1, \ldots, x_n \in \mathbb{N}^*$ e

$$y = f(x_1, \ldots, x_n).$$

Então, $\exists r_1, \ldots, r_m \in \mathbb{N}^*$ tais que

$$P(x_1, \ldots, x_n, y, r_1, \ldots, r_m) = Q(x_1, \ldots, x_n, y, r_1, \ldots, r_m).$$

Pelo Teorema da Sequência de Números (ver Teorema 3.2), $\exists u \in \mathbb{N}^*$ tal que $S(1, u) = y$ e $S(i + 1, u) = r_i$, $1 \leq i \leq m$. Assim,

$$P(x_1, \ldots, x_n, S(1, u), \ldots, S(m + 1, u)) = Q(x_1, \ldots, x_n, S(1, u), \ldots, S(m + 1, u)).$$

Logo, o conjunto

$$A = \{u \in \mathbb{N}^* : P(x_1, \ldots, x_n, S(1, u), \ldots, S(m + 1, u)) = Q(x_1, \ldots, x_n, S(1, u), \ldots, S(m + 1, u))\}$$

é não vazio. Pelo Princípio da Boa Ordem, existe $u_0 = \min A$. Daí,

$$P(x_1, \ldots, x_n, S(1, u_0), \ldots, S(m + 1, u_0)) = Q(x_1, \ldots, x_n, S(1, u_0), \ldots, S(m + 1, u_0)).$$

Definindo $t_i = S(i + 1, u_0)$, $1 \leq i \leq m$, temos que

$$P(x_1, \ldots, x_n, S(1, u_0), t_1, \ldots, t_m) = Q(x_1, \ldots, x_n, S(1, u_0), t_1, \ldots, t_m).$$

Portanto,

$$f(x_1, \ldots, x_n) = S(1, u_0) = S(1, \min A).$$

Assim, por composição, P e Q são recursivas, por minimalidade, $\min A$ é recursiva e, novamente, por composição, f é recursiva.

Reciprocamente, como $c(x)$, $S(x)$, $U_i^m(x_1, \ldots, x_n)$ e $S(i, u)$ são funções diofantinas, basta mostrar que as funções diofantinas são fechadas para as operações de composição, recursão primitiva e minimização.

Composição: Se

$$h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)),$$

onde $f, g_1, \ldots, g_m$ são diofantinas, então h é diofantina, pois,

$$y = h(x_1, \ldots, x_n) \Longleftrightarrow \exists t_1, \ldots, t_m \in \mathbb{N}^* \text{ tais que}$$
$$t_1 = g_1(x_1, \ldots, x_n), \ldots, t_m = g_m(x_1, \ldots, x_n) \text{ e } y = f(t_1, \ldots, t_m).$$

Recursão primitiva: Se

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

onde f, g são funções diofantinas, então usando o Teorema da Sequência de Números para codificar os números

$$h(x_1, \ldots, x_n, 1), h(x_1, \ldots, x_n, 2), \ldots, h(x_1, \ldots, x_n, z)$$

temos que

$$y = h(x_1, \ldots, x_n, z) \Longleftrightarrow \exists u \in \mathbb{N}^* \text{ tal que } [\exists v \in \mathbb{N}^* \text{ tal que } v = S(1, u) \text{ e } v = f(x_1, \ldots, x_n)]$$
$$\text{e } [\forall t \in \{1, \ldots, z\} \text{ temos } t = z \text{ ou } [\exists v \in \mathbb{N}^* \text{ tal que } v = S(t+1, u) \text{ e}$$
$$v = g(t, S(t, u), x_1, \ldots, x_n)]]$$
$$\text{e } [y = S(z, u)].$$

Minimização: Se

$$h(x_1, \ldots, x_n) = \min_y [f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)],$$

onde f, g são funções diofantinas, então h é diofantina, pois,

$$y = h(x_1, \ldots, x_n) \Longleftrightarrow \exists z \in \mathbb{N}^* \text{ tal que } [z = f(x_1, \ldots, x_n, y) \text{ e } z = g(x_1, \ldots, x_n, y)]$$
$$\text{e } [\forall t \in \{1, \ldots, y\} \text{ temos } t = y \text{ ou } [\exists u, v \in \mathbb{N}^* \text{ tais que } u = f(x_1, \ldots, x_n, t)$$
$$\text{e } v = g(x_1, \ldots, x_n, t) \text{ e } (u < v \text{ ou } u > v)]].$$

□

9 O CONJUNTO DIOFANTINO UNIVERSAL

Seja S o conjunto de todos os polinômios a coeficientes inteiros e positivos. Fixado um alfabeto de variáveis $x_0, x_1, x_2, \ldots$ e considerando as funções de emparelhamento descritas no Teorema 3.1, temos que a função $P : \mathbb{N}^* \longrightarrow S$, definida por

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

é sobrejetora, isto é, a função P gera todos os polinômios de S.

Agora, defina o conjunto

$$D_n = \{x_0 \in \mathbb{N}^* : \exists x_1, \ldots, x_n \in \mathbb{N}^* \text{ tais que } P_{L(n)}(x_0, x_1, \ldots, x_n) = P_{R(n)}(x_0, x_1, \ldots, x_n)\}.$$

Observe que $P_{L(n)}$ e $P_{R(n)}$ não envolvem todas as variáveis $x_0, x_1, \ldots, x_n$, mas claramente não pode envolver qualquer outra, pois $L(n), R(n) \leq n$.

Proposição 9.1: *O conjunto $\{D_1, D_2, D_3, \ldots\}$ contém todos os conjuntos diofantinos de números inteiros positivos.*

Demonstração. Seja $A \subseteq \mathbb{N}^*$ um conjunto diofantino. Então, existe um polinômio D com coeficientes inteiros tal que

$$A = \{x_0 \in \mathbb{N}^* : \exists x_1, \ldots, x_n \in \mathbb{N}^* \text{ tais que } D(x_0, x_1, \ldots, x_n) = 0\}.$$

Podemos escrever $D = f - g$, onde f e g são polinômios com coeficientes inteiros e positivos. Como a função P definida anteriormente é sobrejetora, existem $x, y \in \mathbb{N}^*$ tais que $P_x = f$ e $P_y = g$. Como $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$, existe $n \in \mathbb{N}^*$ tal que $x = L(n)$ e $y = R(n)$. Logo,

$$D = f - g = P_x - P_y = P_{L(n)} - P_{R(n)}.$$

Portanto, $A = D_n$. □

Teorema 9.1 (Teorema da Universalidade): *O conjunto* $\{(n, x) \in (\mathbb{N}^*)^2 : x \in D_n\}$ *é diofantino.*

Demonstração. Basta mostrar que

$$x \in D_n \iff \exists u \in \mathbb{N}^* \text{ tal que } S(1, u) = 1 \text{ e } S(2, u) = x \text{ e}$$
$$\forall i \in \{1, \ldots, n\} \text{ temos que } S(3i, u) = S(L(i), u) + S(R(i), u) \text{ e}$$
$$\forall i \in \{1, \ldots, n\} \text{ temos que } S(3i + 1, u) = S(L(i), u) \cdot S(R(i), u) \text{ e } S(L(n), u) = S(R(n), u).$$

($\Longrightarrow$) Seja $x \in D_n$ para x e n dados, então $\exists t_1, \ldots, t_n \in \mathbb{N}^*$ tais que

$$P_{L(n)}(x, t_1, \ldots, t_n) = P_{R(n)}(x, t_1, \ldots, t_n).$$

Pelo Teorema da Sequência de Números, $\exists u \in \mathbb{N}^*$ tal que

$$S(j, u) = P_j(x, t_1, \ldots, t_n), \;\; j = 1, 2, \ldots, 3n + 2.$$

Então, $S(1, u) = P_1(x, t_1, \ldots, t_n) = 1$, $S(2, u) = P_2(x, t_1, \ldots, t_n) = x$, para $i \in \{1, \ldots, n\}$ temos que

$$S(3i, u) = P_{3i}(x, t_1, \ldots, t_n) = P_{L(i)}(x, t_1, \ldots, t_n) + P_{R(i)}(x, t_1, \ldots, t_n) = S(L(i), u) + S(R(i), u)$$

e $S(3i - 1, u) = P_{3i-1}(x, t_1, \ldots, t_n) = t_{i-1}$ para $1 = 2, 3, \ldots, n + 1$ e

$$S(3i + 1, u) = P_{3i+1}(x, t_1, \ldots, t_n) =$$

$$P_{L(i)}(x, t_1, \ldots, t_n) \cdot P_{R(i)}(x, t_1, \ldots, t_n) = S(L(i), u) \cdot S(R(i), u).$$

Como $x \in D_n$, sabemos que

$$P_{L(n)}(x, t_1, \ldots, t_n) = P_{R(n)}(x, t_1, \ldots, t_n).$$

Ou seja,

$$S(L(n), u) = S(R(n), u).$$

($\Longleftarrow$) Suponha o lado direito verdadeiro para x e n dados. Seja

$$t_j = S(3j + 2, u), \;\; j = 1, \ldots, n.$$

Então

$$t_1 = S(5, u), t_2 = S(8, u), \ldots, t_n = S(3n + 2, u).$$

Vejamos por indução que

$$S(j, u) = P_j(x, t_1, \ldots, t_n), \;\; j = 1, \ldots, 3n + 2.$$

Para $j = 1$, temos que

$$S(1, u) = 1 = P_1(x, t_1, \ldots, t_n).$$

Agora, suponha válido para valores até $j-1$, e vamos mostrar que vale para j. Se $j = 3i-1$, então

$$S(3i-1, u) = S(3(i-1)+2, u) = t_{i-1} = P_{3i-1}(x, t_1, \ldots, t_n).$$

Se $j = 3i$ então

$$S(3i, u) = S(L(i), u) + S(R(i), u) =$$

$$P_{L(i)}(x, t_1, \ldots, t_n) + P_{R(i)}(x, t_1, \ldots, t_n) = P_{3i}(x, t_1, \ldots, t_n).$$

Se $j = 3i+1$ então

$$S(3i+1, u) = S(L(i), u) \cdot S(R(i), u) =$$

$$P_{L(i)}(x, t_1, \ldots, t_n) \cdot P_{R(i)}(x, t_1, \ldots, t_n) = P_{3i+1}(x, t_1, \ldots, t_n).$$

Portanto,

$$S(j, u) = P_j(x, t_1, \ldots, t_n), \;\; j = 1, \ldots, 3n+2.$$

Como

$$S(L(n), u) = S(R(n), u),$$

segue que

$$P_{L(n)}(x, t_1, \ldots, t_n) = P_{R(n)}(x, t_1, \ldots, t_n).$$

Logo, $x \in D_n$. □

Sabemos que $D_1, D_2, D_3, \ldots$ fornecem uma enumeração de todos os conjuntos diofantinos, daí, é fácil construir um conjunto diferente de todos eles e portanto não diofantino. Basta definir

$$V = \{n \in \mathbb{N}^* : n \notin D_n\}.$$

Teorema 9.2: *O conjunto V não é diofantino.*

Demonstração. Suponha que V é diofantino, então existe $k \in \mathbb{N}^*$ tal que $V = D_k$. De $V = D_k$ temos

$$k \in V \iff k \in D_k$$

e da definição de V temos

$$k \in V \iff k \notin D_k,$$

absurdo. □

Teorema 9.3: *A função $g(n, x)$ definida por*

$$\begin{cases} g(n, x) = 1, & \textbf{se } x \notin D_n, \\ g(n, x) = 2, & \textbf{se } x \in D_n, \end{cases}$$

não é recursiva.

Demonstração. Suponha por absurdo que g é recursiva, então g é diofantina, isto é,

$$y = g(n, x) \iff \exists y_1, \ldots, y_m \in \mathbb{N}^* \text{ tais que } P(n, x, y, y_1, \ldots, y_m) = 0.$$

Observe que

$$V = \{x \in \mathbb{N}^* : x \notin D_x\} = \{x \in \mathbb{N}^* : g(x, x) = 1\} =$$

$$\{x \in \mathbb{N}^* : \exists y_1, \ldots, y_m \in \mathbb{N}^* \text{ tais que } P(x, x, 1, y_1, \ldots, y_m) = 0\}.$$

Logo, V é diofantino, absurdo. □

Teorema 9.4: *O Décimo Problema de Hilbert é insolúvel nos inteiros positivos.*

Demonstração. Pelo Teorema da Universalidade, sabemos que o conjunto

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

é diofantino, isto é,

$$x \in D_n \iff \exists z_1, \ldots, z_k \in \mathbb{N}^* \text{ tais que } P(n, x, z_1, \ldots, z_k) = 0.$$

Suponha por absurdo que o Décimo Problema de Hilbert seja solúvel nos inteiros positivos, ou seja, suponha que existe um algoritmo para testar se uma equação diofantina possui soluções inteiras positivas. Então, para x e n dados, este algoritmo poderia ser usado para testar se a equação

$$P(n, x, z_1, \ldots, z_k) = 0$$

tem solução, isto é, se $x \in D_n$ ou não. Desse modo, o algoritmo calcula a função $g(n,x)$, logo, $g(n,x)$ é recursiva, absurdo. □

Teorema 9.5: *O Décimo Problema de Hilbert é insolúvel nos naturais.*

Demonstração. Seja $P(x_1, \ldots, x_m) = 0$ uma equação diofantina. Defina o polinômio

$$Q(y_1, \ldots, y_m) = P(y_1 + 1, \ldots, y_m + 1).$$

Suponha por absurdo que o Décimo Problema de Hilbert seja solúvel nos naturais. Então, existe um algoritmo que testa se $\exists y_1, \ldots, y_m \in \mathbb{N}$ tais que

$$Q(y_1, \ldots, y_m) = 0.$$

Escrevendo $x_i = y_i + 1$, $1 \leq i \leq m$, esse algoritmo testa se $\exists x_1, \ldots, x_m \in \mathbb{N}^*$ tais que

$$P(x_1, \ldots, x_m) = 0,$$

logo o Décimo Problema de Hilbert é solúvel nos inteiros positivos, absurdo. □

Teorema 9.6: *O Décimo Problema de Hilbert é insolúvel.*

Demonstração. Seja $P(x_1, \ldots, x_m) = 0$ uma equação diofantina. Sabemos que o sistema

$$\begin{cases} P(x_1, \ldots, x_m) = 0 \\ x_1 = y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 \\ x_2 = y_{2,1}^2 + y_{2,2}^2 + y_{2,3}^2 + y_{2,4}^2 \\ \vdots \\ x_m = y_{m,1}^2 + y_{m,2}^2 + y_{m,3}^2 + y_{m,4}^2 \end{cases}$$

pode ser simplificado na equação

$$E(x_1, \ldots, x_m, y_{1,1}, \ldots, y_{m,4}) = 0.$$

Suponha por absurdo que o Décimo Problema de Hilbert seja solúvel, logo, existe um algoritmo que testa se a equação

$$E(x_1, \ldots, x_m, y_{1,1}, \ldots, y_{m,4}) = 0$$

possui solução inteira. Pela Proposição 2.2, isso equivale a dizer que esse algoritmo testa se

$$P(x_1, \ldots, x_m) = 0$$

possui solução nos naturais. Portanto, o Décimo Problema de Hilbert é solúvel nos naturais, absurdo. □

Note que este resultado se limita a garantir que não existe um algoritmo único para testar se uma equação diofantina tem ou não solução nos números inteiros. Isto não quer dizer que, dada uma equação diofantina em particular, não possamos achar um método para tentar descobrir se ela possui ou não soluções inteiras.

AGRADECIMENTOS

O primeiro autor agradece à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e o segundo autor agradece à Fundação de Amparo à Pesquisa do estado de Minas Gerais (FAPEMIG), pelo auxílio financeiro recebido.

REFERÊNCIAS

[1] A. Church: *An unsolvable problem of elementary number theory*. American Journal of Mathematics, 58:345–363, 1936.

[2] M. Davis: *Arithmetical problems and recursively enumerable predicates*. J. Symbolic Logic, 18:33–41, 1953.

[3] M. Davis: *Hilbert's Tenth Problem is Unsolvable*. The American Mathematical Monthly, 80(3):233–269, 1973.

[4] M. Davis e H. Putnam: *Reduction of Hilbert's tenth problem*. J. Symbolic Logic, 23(1958): 183-187, 1958.

[5] K. Godel: *Uber formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme*. Monatsh. Math. und Physik, 38:173–198, 1931.

[6] Y. Matiyasevich: *Hilbert's Tenth Problem*. The MIT Press, 1993.

[7] J. Robinson: *Existential definability in arithmetic*. Transactions of the American Mathematical Society, 72(3):437–449, 1952.

[8] J. P. Santos: *Introdução à Teoria dos Números*. Coleção Matemática Universitária, 2010.

[9] A. Turing: *On computable numbers, whith an application to the Entscheidungsproblem*. Proceedings of the London Mathematical Society, 42:230–265, 1936.