UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

EDNEY FREITAS GREGÓRIO

O DÉCIMO PROBLEMA DE HILBERT E UMA APLICAÇÃO

FORTALEZA

2018

EDNEY FREITAS GREGÓRIO

O DÉCIMO PROBLEMA DE HILBERT
E UMA APLICAÇÃO

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional, Universidade Federal do Ceará, como requisito para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. Marcos Ferreira de Melo.

FORTALEZA

2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

G833d Gregório, Edney Freitas.
O décimo problema de Hilbert e uma aplicação / Edney Freitas Gregório. – 2018.
60 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2018.
Orientação: Prof. Dr. Marcos Ferreira de Melo.

1. Equações diofantinas. 2. Funções recursivas. I. Título.

CDD 510

EDNEY FREITAS GREGÓRIO

O DÉCIMO PROBLEMA DE HILBERT E UMA APLICAÇÃO

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional, Universidade Federal do Ceará, como requisito para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. Marcos Ferreira de Melo.

Aprovada em: 11/06/2018

BANCA EXAMINADORA

Prof. Dr. Marcos Ferreira de Melo (orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Marcelo Ferreira de Melo
Universidade Federal do Ceará (UFC)

Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

A todos os colegas do PROFMAT,
pelo companheirismo durante o curso.

AGRADECIMENTOS

A Deus em primeiro lugar, por me abençoar com a vida. A minha familia que me ajudou do começo ao fim, minha querida esposa, amigos e professores.

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 possivel elaborar um processo que decida, atráves de um número finito de operações, se a equação tem soluções inteiras. O objetivo é demonstrar que não é possivel 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 dos 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 a 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 e no ultimo capitulo é dada uma aplicação desse resultado para a demonstração do Teorema de Incompletude de Gödel.

Palavras-chave: Equações Diofantinas. Funções Recursivas. Função Exponencial.

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 Hibert’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 Number Sequence 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 and not last chapter and given application of result for a demonstration of Gödel's Incompletude Theorem.

Key words: Diophantine Equations. Recursive Functions. Exponential Function.

SUMÁRIO

1 INTRODUÇÃO..... 9
2 EQUAÇÕES DIOFANTINAS..... 11
2.1 Sistemas de equações diofantinas..... 11
2.2 Soluções nos números naturais..... 12
2.3 Conjuntos diofantinos..... 13
3 O 10º PROBLEMA DE HILBERT É INSOLÚVEL..... 21
3.1 A função exponencial é diofantina..... 21
3.2 A linguagem dos predicados diofantinos..... 38
3.3 Novos conjuntos diofantinos..... 43
3.4 Conceito de algoritmo e modelos de computabilidade..... 49
3.5 Funções recursivas..... 50
3.6 O conjunto diofantino universal..... 54
4 UMA APLICAÇÃO PARA O 10º PROBLEMA DE HILBERT..... 59
4.1 Teorema de incompletude de Godel..... 59
5 CONCLUSÃO..... 60
REFERÊNCIAS..... 61

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 trata-se 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 solução inteira. 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 , além de outros lógicos como Alonzo Church e Alan Turing , que contribuiram na formulação rigorosa para a noção de computabilidade. Isso possibilitou o estabelecimento do que seria um algoritmo insóluvel, 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 posteriomente em outros ramos da matemática.

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

A matemática Julia Robinson contribuiu fortemente na demonstração de que a função exponencial é diofantina . Mas, a peça chave na solução definitiva do problema foi o matemático Yuri Matiyasevich 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.

A dissertação 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 25 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 da dissertação definimos função recursiva e provamos que uma função ser recursiva é equivalente a ser diofantina. Após isso, demonstramos o Teorema da Universalidade e concluimos a dissertação com o Teorema que afirma a insolubilidade do Décimo Problema de Hilbert e usamos esse resultado para provar o Teorema de Incompletude de Gödel.

Nessa dissertação 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 e tambem usaremos o teorema chinês sobre restos. As demonstrações desses teoremas se encontram na referência bibliográfica (Introdução a Teoria dos números.

2 EQUAÇÕES DIOFANTINAS

O objetivo principal desse capítulo é introduzir dois conceitos, o de conjunto Diofantino e o de função Diofantina bem como suas propriedades e exemplos que elucidarão estes conceitos.

Uma equação Diofantina é uma equação da forma:

$$D(x_1, \dots, x_m) = 0$$

Onde D é um polinômio com coeficientes inteiros. Esta equação também pode ser escrita da seguinte forma:

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

Onde D_L e D_R são polinômios com coeficientes inteiros positivos. Para obter tal forma basta transpor para o lado direito os termos com coeficientes negativos.

2.1 Sistema de equações diofantinas

Lema 1.1. um sistema constituido de k equações Diofantinas

$$\begin{cases} D_1(x_1, \dots, x_m) = 0 \\ \dots \\ D_k(x_1, \dots, x_m) = 0 \end{cases}$$

Tem como solução os inteiros $x_1, \dots, x_m$ se, e somente se, a equação Diofantina

$$E(x_1, \dots, x_m) = \sum_{i=1}^{k} D_i^2(x_1, \dots, x_m) = 0$$

tem a mesma solução.

Demonstração.

Primeiramente, suponha que o sistema é satisfeito, ou seja , $D_i(x_1, \dots, x_m) = 0$ para $1 \leq i \leq k$ daí $D_i^2(x_1, \dots, x_m) = 0$ para $1 \leq i \leq k$, e então $\sum_{i=1}^{k} D_i^2(x_1, \dots, x_m) = 0$.

Reciprocamente, se $\sum_{i=1}^{k} D_i^2(x_1, \dots, x_m) = 0$, como $D_i^2(x_1, \dots, x_m) \geq 0$ para $1 \leq i \leq k$, segue que $D_i(x_1, \dots, x_m) = 0$ para $1 \leq i \leq k$. Portanto um sistema de equações Diofantinas pode ser reduzido a uma única equação Diofantina. ■

A transformação inversa também é possivel, isto é , transformar a equação $D(x_1, \dots, x_m) = 0$ em um sistema

$$\begin{cases} D_1(x_1, \dots, x_m, y_1, \dots, y_n) = 0 \\ \dots \\ D_k(x_1, \dots, x_m, y_1, \dots, y_n) = 0 \end{cases}$$

Onde $y_1, \dots, y_n$ são novas variáveis no sistema.

Um possível motivo para transformar uma equação Diofantina em um sistema pode ser a obtenção de um sistema constituído de equações de grau menor. É interessante perceber que qualquer equação Diofantina pode ser transformada num sistema de equações constituído de equações de dois tipos:

I) $\boldsymbol{\alpha = \beta + \gamma}$ **II)** $\boldsymbol{\alpha = \beta\gamma}$

Onde α, β e γ são números particulares ou dependem das variáveis $x_1, \dots, x_m, y_1, \dots, y_n$.

Exemplo 1.1 : Considere a seguinte equação Diofantina que envolve três variáveis (x, y, z) , $D(x, y, z) = 4x^3y - 2x^2z^3 - 3y^2x + 5z = 0$ transpondo os termos negativos obtemos $4x^3y + 5z = 2x^2z^3 + 3y^2x$. Agora introduziremos 15 novas variáveis $p_1, \dots, p_4, q_1, r_1, \dots r_5, s_1, .., s_3, t_1, u_1$ $(p_4p_3p_2p_1$, $r_5r_4r_3r_2r_1$, $s_3s_2s_1 \neq 0)$ e obtemos o sistema equivalente:

$$\begin{cases} p_1 = 4x\,, \quad p_2 = p_1x\,, \quad p_3 = p_2x\,, \quad p_4 = p_3y; \\ q_1 = 5z; \\ r_1 = 2x\,, \quad r_2 = r_1x\,, \quad r_3 = r_2z\,, \quad r_4 = r_3z, \quad r_5 = r_4z; \\ s_1 = 3y\,, \quad s_2 = s_1y\,, \quad s_3 = s_2x\,; \\ t_1 = p_4 + q_1\,, \ u_1 = r_5 + s_3\,, \quad t_1 = u_1. \end{cases}$$

Veja que $p_4 = 4x^3y$, $q_1 = 5z$, $r_5 = 2x^2z^3$, $s_3 = 3y^2x$.

Finalmente, utilizando o Lema 1.1, obtemos uma equação de grau 4 independentemente do grau da equação inicial. Então para resolver o 10º problema de Hilbert será suficiente decidir se uma equação de grau 4 tem ou não solução.

2.2 Soluções nos números naturais

Em seu 10° problema, Hilbert falou sobre as soluções nos inteiros. Algumas vezes uma solução nos inteiros é evidente. Por exemplo , a equação $(x + 1)^3 + (y + 1)^3 = (z + 1)^3$ tem infinitas soluções da forma $x = z$ e $y = -1$. Por outro lado, a obtenção de soluções não-negativas x , y e z para tal equação não é trivial. Desse modo, para uma equação Diofantina particular , o problema de dicidir se esta tem uma solução inteira e o problema de decidir se esta tem uma solução inteira não-negativa são em geral dois problemas distintos.

Lema 1.2. A equação Diofantina $D(x_1, \dots, x_n) = 0$ tem uma solução nos naturais se, e somente se, o sistema

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

tem uma solução nos inteiros.

Demonstração.

Considere $(x_1, \dots, x_n)$ uma solução nos naturais da equação $D(x_1, \dots, x_n) = 0$. Pelo teorema de Lagrange todo natural pode ser escrito como soma de quatro quadrados portanto,podemos expressar cada x_i com

$1 \leq i \leq n$ como soma de quatro quadrados, dando uma solução ao sistema. Reciprocamente, qualquer solução do sistema em números inteiros inclui a solução $(x_1, \dots, x_n)$ em naturais da equação $D(x_1, \dots, x_n) = 0$.

■

Pelo Lema 1.1 podemos reduzir o sistema a uma única equação $E(x_1, \dots, x_n, y_{1,1}, \dots, y_{n,4}) = 0$ do resultado acima ela tem solução inteira se , e somente se $D(x_1, \dots, x_n) = 0$ tem solução natural , onde as equações D e E são diferentes.

Desse modo, foi mostrado que o problema de decisão de determinar a existência ou não-existência de soluções não-negativas é reduzido ao problema de determinar a existência ou não-existência de soluções inteiras. Assim , para provar que o Décimo Problema de Hilbert é insolúvel na sua forma original é suficiente mostrar que o mesmo é insolúvel nos inteiros não-negativos.

2.3 Conjunto diofantino

Definição 1.1: Seja $M \subseteq (\mathbb{N}^*)^n$. O Conjunto M será chamado de conjunto Diofantino quando existir um polinômio $D(a_1, \dots, a_n, x_1, \dots, x_m)$ a coeficientes inteiros tal que $(a_1, \dots, a_n) \in M \Leftrightarrow \exists\, x_1, \dots, x_m \in \mathbb{N}^*$ tais que $D(a_1, \dots, a_n, x_1, \dots, x_m) = 0$. O número n é chamado de dimensão de M.

Exemplo 1.2. O conjunto C dos números compostos positivos é Diofantino. Observe que, $x \in C \Leftrightarrow \exists y, z \in \mathbb{N}^*$ tais que $x = (y + 1)(z + 1)$.

Demonstração.

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 $x = (y + 1)(z + 1)$ e $(y + 1), (z + 1) > 1$ segue que x é composto. Portanto, $x \in C$. Veja que a dimensão de C é $n = 1$ e $x \in C \Leftrightarrow (\exists\, y, z \in \mathbb{N}^*)[\, D(x, y, z) = x - (y + 1)(z + 1)]$. ■

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

Proposição 1.1: Considere os conjuntos Diofantinos M_1 e M_2 de mesma dimensão então $M_1 \cup M_2$ também é um conjunto diofantino.

Demontração.

Por hipótese $M_1 = \{(a_1, \dots, a_n) \in (\mathbb{N}^*)^n : \exists x_1, \dots, x_m \in \mathbb{N}^* \mid D_1(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$ e

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

Devemos mostrar que ,

$(a_1, \dots, a_n) \in M_1 \cup M_2 \Leftrightarrow \exists z_1, z_2, \dots, z_{m+t} \in \mathbb{N}^* \mid [D(a_1, \dots, a_n, z_1, z_2, \dots, z_{m+t}) = 0]$.

Para isso definimos , $D(a_1, \dots, a_n, z_1, z_2, \dots, z_{m+t}) =$ $D_1(a_1, \dots, a_n, x_1, \dots, x_m) D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$ e $x_1 = z_1, \dots x_m = z_m$ e $y_1 = z_{m+1}, \dots y_t = z_{m+t}$.

Seja $(a_1, \dots, a_n) \in M_1 \cup M_2$. Se $(a_1, \dots, a_n) \in M_1$, então , $\exists\, x_1, \dots, x_m \in \mathbb{N}^*$ tal que $D_1(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ daí $D_1(a_1, \dots, a_n, x_1, \dots, x_m) D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$, Para quaisquer $y_1, \dots, y_t \in \mathbb{N}^*$. Se $(a_1, \dots, a_n) \in M_2$, então , existem $y_1, \dots, y_t \in \mathbb{N}^*$ tais que $D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$. Logo, $D_1(a_1, \dots, a_n, x_1, \dots, x_m) D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$, Para quaisquer $x_1, \dots, x_m \in \mathbb{N}^*$.

Reciprocamente , suponha que $\exists x_1, \dots, x_m, y_1, \dots, y_t \in \mathbb{N}^*$ tais que o produto seja zero, ou seja , $D_1(a_1, \dots, a_n, x_1, \dots, x_m)D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$.Caso $D_1(a_1, \dots, a_n, x_1, \dots, x_m) = 0$ então, $(a_1, \dots, a_n) \in M_1$, logo, $(a_1, \dots, a_n) \in M_1 \cup M_2$. Agora, Caso $D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$, então $(a_1, \dots, a_n) \in M_2$. Logo, $(a_1, \dots, a_n) \in M_1 \cup M_2$. ■

Proposição 1.2: Considere os conjuntos Diofantinos M_1 e M_2 de mesma dimensão então $M_1 \cap M_2$ também é um conjunto diofantino.

Demonstração.

Por hipótese, $M_1 = \{(a_1, \dots, a_n) \in (\mathbb{N}^*)^n : \exists x_1, \dots, x_m \in \mathbb{N}^* \mid D_1(a_1, \dots, a_n, x_1, \dots, x_m) = 0\}$ e $M_2 = \{(a_1, \dots, a_n) \in (\mathbb{N}^*)^n : \exists y_1, \dots, y_t \in \mathbb{N}^* \mid D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0\}$.

Devemos mostrar que

$$(a_1, \dots, a_n) \in M_1 \cap M_2 \Leftrightarrow \exists z_1, z_2, \dots, z_{m+t} \in \mathbb{N}^* \mid \left[D\left(a_1, \dots, a_n, z_1, z_2, \dots, z_{m+t}\right) = 0\right].$$

Para isso definimos

$D\left(a_1, \dots, a_n, z_1, z_2, \dots, z_{m+t}\right) = D_1^2(a_1, \dots, a_n, x_1, \dots, x_m) + D_2^2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$

onde ,

$$x_1 = z_1 \, , \dots x_m = z_m \text{ e } y_1 = z_{m+1} \, , \dots y_t = z_{m+t} \, .$$

Seja $(a_1, \dots, a_n) \in M_1 \cap M_2$, então $\exists x_1, .., x_m, y_1, .., y_t \in \mathbb{N}^* \mid D_1(a_1, .., a_n, x_1, .., x_m) = 0$ e $D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$. Portanto, $D_1^2(a_1, \dots, a_n, x_1, \dots, x_m) + D_2^2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$.

Reciprocamente, suponha que $\exists x_1, \dots, x_m, y_1, \dots, y_t \in \mathbb{N}^*$ tais que $D_1^2(a_1, .., a_n, x_1, .., x_m) + D_2^2(a_1, .., a_n, y_1, .., y_t) = 0$. Então, $D_1(a_1, .., a_n, x_1, \dots, x_m) = 0$ e $D_2(a_1, \dots, a_n, y_1, \dots, y_t) = 0$. Logo, $(a_1, \dots, a_n) \in M_1$ e $(a_1, \dots, a_n) \in M_2$, ou seja , $(a_1, \dots, a_n) \in M_1 \cap M_2$. ■

Vejamos alguns exemplos de conjuntos Diofantinos:

Exemplo 1.3. O conjunto E dos números positivos que não são potências de 2 é Diofantino com dimensão 1, pois,

$$x \in E \Leftrightarrow (\exists \, y, z \in \mathbb{N}^*)[x = y(2z + 1)].$$

Exemplo 1.4. O conjunto $D = \{(x, y) \in (\mathbb{N}^*)^2 : x < y\}$ é Diofantino com dimensão 2, pois

$$(x, y) \in D \iff (\exists z \in \mathbb{N}^*)\ [\, x + z = y].$$

Exemplo 1.5. (Relação de Ordem) O conjunto $N = \{(x, y) \in (\mathbb{N}^*)^2 : x \leq y\}$ é Diofantino com dimensão 2, pois

$$(x, y) \in N \iff (\exists z \in \mathbb{N}^*)[\, x + z - 1 = y].$$

Exemplo 1.6. (Relação de Divisibilidade) O conjunto $\boldsymbol{E} = \{(x, y) \in (\mathbb{N}^*)^2 : x \mid y\}$ é Diofantino com dimensão 2, pois

$$(x, y) \in \boldsymbol{E} \iff (\exists z \in \mathbb{N}^*)[\ y = zx].$$

Exemplo 1.7. (Relação de Interseção) O conjunto $Y = \{(x, y, z) \in (\mathbb{N}^*)^3 : x \mid y \text{ e } x < z\}$ é Diofantino com dimensão 3.

Demonstração.

Como $x \mid y \iff (\exists a \in \mathbb{N}^*)\ [y = ax]$ e $x < z \iff (\exists b \in \mathbb{N}^*)[z = x + b]$, Podemos ver Y como a união de dois conjuntos $Y_1 \cap Y_2 = Y$ onde $Y_1 = \{(x, y, z) \in (\mathbb{N}^*)^3 : x \mid y\}$ e $Y_1 = \{(x, y, z) \in (\mathbb{N}^*)^3 \mid x < y\}$

pela propriedade (1.2) , $(x, y, z) \in Y \iff (\exists a, b \in (\mathbb{N}^*)^2)\ [(y - ax\ )^2 + (z - x - b\ )^2 = 0]$, ou seja, Y é diofantino.

■

Exemplo 1.8. (Relação de Congruência) Sejam $a, b, c \in \mathbb{N}^*$ definimos a relação de congruência sobre $\mathbb{N}^*$ como:

$$a \equiv b\ (mod\ c) \Leftrightarrow c \mid a - b$$

Mas isso é equivalente a :

$$a \equiv b\ (mod\ c) \Leftrightarrow \exists\ x \in \mathbb{N}^* \text{ tal que } a = b + cx$$

Pela propriedade 1.1 temos que :

$$a \equiv b\ (mod\ c) \Leftrightarrow \exists\ x \in \mathbb{N}^* \text{ tal que } a - b - cx = 0.$$

Assim pela definição 1.1 , a relação de congruência é diofantina.

■

1.4 Função diofantina

Definição 1.2: Seja $f: (\mathbb{N}^*)^n \longrightarrow \mathbb{N}^*$. Chamamos de gráfico de f o conjunto

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

Definição 1.3. (Função Diofantina): Seja $f: (\mathbb{N}^*)^n \longrightarrow \mathbb{N}^*$. Dizemos que f é uma função diofantina quando graf(f) é um conjunto diofantino.

Exemplo 1.9. Considere a função $T\colon \mathbb{N}^* \longrightarrow \mathbb{N}^*$ definida por ,

$T(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, observe que T é uma função Diofantina, de fato, como graf$(T) = \{(n,m) \in (\mathbb{N}^*)^2 \mid m = T(n)\}$ então $(n,m) \in$ graf$(T) \Leftrightarrow m = \frac{n(n+1)}{2} \Leftrightarrow 2m = n(n+1)$. Logo, graf$(T)$ é um conjunto Diofantino e, portanto, T é uma função Diofantina.

Lema 1.3. Seja a função $T\colon \mathbb{N} \longrightarrow \mathbb{N}$ definida por $T(n) = \frac{n(n+1)}{2}$. Então $T(z)$ é crescente, $T(z) \geq z$ e para cada $z \in \mathbb{N}^*$, existe um único inteiro $n \geq 0$, tal que $T(n) < z \leq T(n+1)$.

Demonstração.

Como $T(z+1) - T(z) = z + 1 > 0$, segue que $T(z)$ é crescente. 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 $S_z \neq \phi$, pois $z \in S_z$. Alem 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 $m = minS_z$, e consequentemente, existe um único $n = m - 1 \in \mathbb{N}$. Como $n < m = minS_z$ temos que $n \notin S_z$. Logo , $T(n) < z$, e como $m \in S_z$, temos que $z \leq T(m)$. Portanto , $T(n) < z \leq T(n+1)$.

■

Teorema 1.1 (Teorema das Funções de Emparelhamento) Existem funções Diofantinas $P(x,y), L(z), R(z)$ tais que :

1) Para todo $x,y,z \in \mathbb{N}^*$ $L(P(x,y)) = x$, $R(P(x,y)) = y$ e $P\big(L(z),R(z)\big) = z$

2) $L(z) \leq z$, $R(z) \leq z$.

Demonstração.

Pelo Lema (1.3) a função T é crescente e para cada $z \in \mathbb{N}^*$, existe um único inteiro $n \geq 0$, tal que $T(n) < z \leq T(n+1) = T(n) + n + 1$. Como $T(n) < z$ temos então que $y := z - T(n) > 0$, logo $y \in \mathbb{N}^*$.Por outro lado, $z \leq T(n+1) = T(n) + n + 1 \Rightarrow y + T(n) \leq T(n) + n + 1 \Rightarrow y \leq n + 1 \Rightarrow n + 1 - y \geq 0 \Rightarrow n + 2 - y > 0 \Rightarrow$

$$x := n + 2 - y \in \mathbb{N}^*.$$

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

$$\begin{cases} L\colon \mathbb{N}^* \longrightarrow \mathbb{N}^*, \text{com } L(z) = x\,; \\ R\colon \mathbb{N}^* \longrightarrow \mathbb{N}^*, \text{com } R(z) = y\,; \end{cases}$$

Como $z = T(n) + y$ e $n = x + y - 2$ definimos $P\colon (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$, como $P(x,y) = T(x+y-2) + y$ note que $P(x,y) = z$.

Prova de 1)

Para todos os números $x, y, z \in \mathbb{N}^*$ $L(P(x,y)) = x$, $R(P(x,y)) = y$, $P\big(L(z), R(z)\big) = z$ de fato pois, $L(P(x,y)) \overset{\text{def}}{=} L(z) \overset{\text{def}}{=} x$, $R(P(x,y)) \overset{\text{def}}{=} R(z) \overset{\text{def}}{=} y$ e $P\big(L(z), R(z)\big) \overset{\text{def}}{=} P(x,y) \overset{\text{def}}{=} z$.

Prova de 2)

Provemos agora que $L(z) \leq z$ *e* $R(z) \leq z$ de fato, como $z = T(n) + y \Rightarrow z \geq y \Rightarrow z \geq R(z)$. Para o que falta usamos o lema (1.3) já que $z \geq T(x+y-2)+1 \geq T(x-1)+1 \geq (x-1)+1 = x$. Logo $z \geq x$, ou seja , $z \geq L(z)$.

***L*, *R e P* são Diofantinas**

Note que $L(z), R(z)$ e $P(x,y)$ são funções diofantinas uma vez que :

$$z = P(x,y) \Leftrightarrow \quad 2z = (x+y-2)(x+y-1) + 2y$$
$$x = L(z) \Leftrightarrow (\exists y)[2z = (x+y-2)(x+y-1) + 2y$$
$$y = R(z) \Leftrightarrow (\exists x)[2z = (x+y-2)(x+y-1) + 2y$$

A função $P(x,y)$ estabelece uma bijeção entre conjunto dos pares ordenados formados por inteiros positivos e o conjunto dos números inteiros positivos. E para cada inteiro z , o par ordenado que esta associado a z por $P(x,y)$ é $\big(L(z), R(z)\big)$

■.

Outra função Diofantina que nos será muito útil esta relacionada ao Teorema Chinês sobre restos. Defina a função $S(i,u) = w$ onde w é o único inteiro positivo para o qual $w \equiv L(u)(mod\ 1 + i.R(u))$ e $w < 1 + iR(u)$. Aqui , w é o resto da divisão euclidiana de $L(u)$ por $1 + iR(u)$.

Teorema 1.2 (Teorema da Sequência de Números) Existe uma função Diofantina $S(i,u)$ tal que :

1) $S(i,u) \leq u$, e

2) Para cada sequência $a_1, \dots, a_n \in \mathbb{N}^*$, existe um número inteiro u tal que $S(i,u) = a_i$ para $1 \leq i \leq n$.

Demonstração.

***S* é Diofantina**

Definimos a função $S\colon (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$, da seguinte forma : $S(i,u) = w$, onde w é o único inteiro positivo para o qual $w \equiv L(u)(mod\ 1 + iR(u))$, $0 < w < 1 + iR(u)$, sendo $u = P(x,y)$ tal que $x = L(u)$ e $y = R(u)$. Mostremos agora que $S(i,u)$ é diofantina.

Veja que $w = S(i,u) \Leftrightarrow \exists z \in \mathbb{N}^*$ tal que $L(u) = (z-1)\big(1+iR(u)\big) + w$ e $0 < w < 1 + iR(u) \Leftrightarrow$

$\Leftrightarrow \exists x, y, z, v \in \mathbb{N}^*$ tais que $\begin{cases} 2u = (x+y-2)(x+y-1) + 2y, \\ x = w + (z-1)(1+iy), \\ iy = w + v - 1. \end{cases}$ $\Leftrightarrow \exists x, y, z, v \in \mathbb{N}^*$ tais que

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

Então usando a Lema 1.1 (somando os quadrados das três equações) prova-se que $S(i,u)$ é Diofantino, note que a terceira equação do sistema $(iy = w + v - 1)$ vem do fato que $0 < w < 1 + iR(u) \Leftrightarrow 0 < 1 + iy - w \stackrel{\text{def}}{=} v \in \mathbb{N}^*$.

Prova de 1)

Provemos agora que $S(i,u) \leq u$. De fato , como $L(u) = (z-1)\big(1+iR(u)\big) + w \Rightarrow L(u) \geq w \Rightarrow L(u) \geq S(i,u)$ mas pelo Teorema (1.1) , $L(u) \leq u$. Logo , $S(i,u) \leq u$.

Prova de 2)

Finalmente, sejam $a_1, \ldots, a_n \in \mathbb{N}^*$ uma sequência de números. Escolha $y \in \mathbb{N}^*$ como sendo algum número maior que cada $a_1, \ldots, a_n$ e divisível por $1,2, \ldots, n$. Então os números $1 + y, 1 + 2y, \ldots, 1 + ny$ são relativamente primos entre si.

De fato, seja $d \in \mathbb{N}^*$ onde $d \mid 1 + iy$, e $d \mid 1 + jy$, com $i < j$, então $d \mid [j(1 + iy) - i(1 + jy)]$, isto é, $d \mid j - i$ de modo que $d \leq j - i \leq n$ daí $d \mid y$.

De $d \mid y$ e $d \mid 1 + iy$ temos $d = 1$ .Sendo assim , podemos aplicar o Teorema Chinês sobre restos para obtermos um número x tal que:

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

Logo para $i = 1,2, \ldots, n$ teremos $a_i \equiv L(u) \big(mod\ 1 + i.R(u)\big)$ e $a_i < y = R(u) < 1 + iR(u)$. Mas por definição da função $S(i,u)$ segue que $a_i = S(i,u)$. ■

Uma impressionante caracterização dos conjuntos Diofantinos de inteiros positivos é dado pelo:

Teorema 1.3 Um conjunto S de inteiros positivos é Diofantino com dimensão 1 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.

Primeiramente, suponha que S é Diofantino, logo, existe um polinômio Q tal que:

$$x \in S \Leftrightarrow (\exists x_1, \dots, x_m \in \mathbb{N}^*)[Q(x, x_1, \dots, x_m) = 0].$$

Seja $P(x, x_1, \dots, x_m) = x.[1 - Q^2(x, x_1, \dots, x_m)]$. Se $x \in S$, escolha $x_1, \dots, x_m$ tais que $Q(x, x_1, \dots, x_m) = 0$, logo $P(x, x_1, \dots, x_m) = x$, o que mostra que x esta no conjunto imagem da função definida por P.

Por outro lado, seja $z = P(x, x_1, \dots, x_m), z > 0$. Como $z = x.[1 - Q^2(x, x_1, \dots, x_m)]$ e $x > 0$, segue que $1 - Q^2(x, x_1, \dots, x_m) > 0$, logo $Q^2(x, x_1, \dots, x_m) = 0$ pois $Q\ (x, x_1, \dots, x_m) \in \mathbb{Z}$, ou seja, $Q(x, x_1, \dots, x_m) = 0$. Portanto $z = x$ e $Q(z, x_1, \dots, x_m) = 0$ o que mostra que $z \in S$.

Reciprocamente, seja S o conjunto dos inteiros positivos na imagem da função definida por P. Logo,

$$x \in S \Leftrightarrow (\exists x_1, \dots, x_m \in \mathbb{N}^*)[P(x_1, \dots, x_m) = x].$$

Defina $R(x, x_1, \dots, x_m) = x - P(x_1, \dots, x_m)$. Então , $x \in S \Leftrightarrow (\exists x_1, \dots, x_m \in \mathbb{N}^*)[R(x, x_1, \dots, x_m) = 0]$, Logo o conjunto S é Diofantino.

■

3 O 10º PROBLEMA DE HILBERT É INSOLÚVEL

3.1 A função exponencial é diofantina

O objetivo desta seção é mostrar que a função exponecial $h(n,k) = n^k$ é Diofantina. Isto é necessário pois esta função servirá de base para mostrarmos que outras funções importantes também são Diofantinas. Para isso serão necessários 25 lemas, os quais enunciaremos e provaremos a seguir. Nestes lemas utilizaremos fortemente a Equação de Pell, a Teoria de Congruências e o Princípio de Indução Finita.

Definição 2.1 A equação diofantina $x^2 - dy^2 = N$, **onde** d e N são inteiros é chamado de equação de PELL. A equação de Pell é de grande importância na teoria dos números devido ao fato de que muitas equações diofantinas podem ser transformadas em uma equação de Pell , ou que dependa de alguma forma dela.

Exemplo 2.1 : Encontre todas as soluções inteiras da equação geral do segundo grau:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0\,,$$

Onde $a\,, b, c, d, e, f$ são inteiros. O procedimento é o seguinte : Agrupamos os termos desta maneira , $ax^2 + (by + d)x + (cy^2 + ey + f) = 0$. Logo a equação inicial pode ser vista como uma simples equação do segundo grau com descriminante,

$\Delta_1 = (by + d)^2 - 4a(cy^2 + ey + f) = (b^2 - 4ac)y^2 + (2bd - 4ae)y + d^2 - 4af$, esse descriminante deve ser um quadrado perfeito , chamaremos então $\Delta_1 = z^2$. Definindo ,

$$p = b^2 - 4ac\,, \quad q = 2bd - 4ae\,, \quad r = d^2 - 4af$$

Logo teremos , $py^2 + qy + r - z^2 = 0$, que de novo é uma equação do segundo grau com descriminante $\Delta_2 = q^2 - 4p(r - z^2)$, novamente esse descriminante deve ser um quadrado perfeito , chamaremos então $\Delta_2 = w^2$. Daí ,

$$q^2 - 4p(r - z^2) = w^2 \Leftrightarrow w^2 - 4pz^2 = q^2 - 4pr.$$

Que é uma equaçãode PELL , com $q^2 - 4pr = N$. Logo , se conhecemos as soluções inteiras dessa equação , obtemos imediatamente as soluções inteiras da equação geral do segundo grau. Nessa dissertação trabalharemos com o caso especial (ou particular) $x^2 - dy^2 = 1$.

A Equação Especial de Pell é dada por $x^2 - dy^2 = 1$, com $x, y \in \mathbb{Z}$, onde $d := a^2 - 1,\ a > 1.\ d \in \mathbb{N}^*$. Observe que $(x, y) = (1,0)$ e $(x, y) = (a, 1)$ são soluções triviais da equação de Pell, além disso se (x, y) é uma solução então $(-x, y)\,, (x, -y)$ e $(-x, -y)$ também são soluções. Note que se $d = k^2$ para algum valor de k , então a equação especial acima so tem a solução trivial $(x, y) = (1,0)$.

Demonstração :

Se $d = k^2$ para algum valor de k , então usando fatoração $(x + ky)(x - ky) = 1$, logo $x + ky = \pm 1$ ou $x - ky = \pm 1$, pois o produto de inteiros é igual a um se e só se ambos são iguais a 1 ou -1. Assim temos os sistemas :

$$\begin{cases} x + ky = -1 \\ x - ky = -1 \end{cases} \quad ou \quad \begin{cases} x + ky = 1 \\ x - ky = 1 \end{cases}$$

Resolvendo temos que a única solução é $(x, y) = (\pm 1, 0)$. De agora em diante consideraremos d como sendo um número que não é quadrado perfeito , ou seja , $\sqrt{d} \notin \mathbb{Q}$.

Definição 2.2 $x_n(a)$ e $y_n(a)$ para $n \in \mathbb{N}, a > 1$, são definidas por $x_n(a) + y_n(a)\sqrt{d} = \left(a + \sqrt{d}\right)^n$. Quando o contexto permitir , a dependência em relação a a **não** será explicitada e escreverei apenas x_n e y_n.

Exemplo 2.2 : $x_1(a) = a \ e \ y_1(a) = 1$, $x_0(a) = 1 \ e \ y_0(a) = 0$

$x_0(a) + y_0(a)\sqrt{d} = \left(a + \sqrt{d}\right)^0 = 1$, o que implica que $x_0(a) = 1 \ e \ y_0(a) = 0$

$x_1(a) + y_1(a)\sqrt{d} = \left(a + \sqrt{d}\right)^1 = a + \sqrt{d}$, o que implica que $x_1(a) = a \ e \ y_1(a) = 1$

Exemplo 2.3 : $b > a \Leftrightarrow x_k(b) > x_k(a)$ **.**Usando binômio de Newton temos $x_k(a) + y_k(a)\sqrt{d} = \left(a + \sqrt{d}\right)^k$

$$\begin{cases} x_k(a) = \sum_{\substack{j=0 \\ j\ par}}^{k} \binom{k}{j} a^{k-j} d^{\frac{j}{2}} \\ y_k(a) = \sum_{\substack{j=1 \\ j\ ímpar}}^{k} \binom{k}{j} a^{k-j} d^{\frac{j-1}{2}} \end{cases}$$. Logo se $b > a \Leftrightarrow b^{k-j} > a^{k-j} \Leftrightarrow x_k(b) > x_k(a)$.

Lema 2.1 Não existem inteiros x, y, que satisfaçam a Equação de Pell para os quais $1 < x + y\sqrt{d} < a + \sqrt{d}$.

Lema 2.2 Sejam x, y e x', y' inteiros, que satisfaçam a Equação de Pell. Definindo $x'' = xx' + yy'd$ e $y'' = x'y + y'x$. Então x'' e y'' satisfazem a Equação de Pell.

Lema 2.3 x_n e y_n satisfazem a Equação de Pell.

Lema 2.4 Sejam x, y soluções não negativas da Equação de Pell. Então para algum $n \in \mathbb{N}$, $x = x_n$ e $y = y_n$.

Lema 2.5 $x_{m\pm n} = x_m x_n \pm d y_m y_n$ e $y_{m\pm n} = y_m x_n \pm x_m y_n$.

Lema 2.6 $y_{m\pm 1} = a y_m \pm x_m$ *e* $x_{m\pm 1} = a x_m \pm d y_m$.

Lema 2.7 $(x_n, y_n) = 1$.

Lema 2.8 $y_n \mid y_{nk}$. $n \in \mathbb{N}^*$

Lema 2.9 $y_n \mid y_t$ se, e somente se, $n \mid t$. $n \in \mathbb{N}^*$

Lema 2.10 $y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}$, $\forall\, k \in \mathbb{N}^*,\ k \geq 1$.

Lema 2.11 $y_n^2 \mid y_{n\,.\,y_n}$. $n \in \mathbb{N}^*$

Lema 2.12 $y_n^2 \mid y_t$ então $y_n \mid t$. $n \in \mathbb{N}^*$

Lema 2.13 $x_{n+1} = 2a x_n - x_{n-1}$ e $y_{n+1} = 2a y_n - y_{n-1}$.

Lema 2.14 $y_n(a) \equiv n \pmod{a-1}$.

Lema 2.15 Se $a \equiv b \pmod{c}$, então $\forall\, n \in \mathbb{N}$, $x_n(a) \equiv x_n(b) \pmod{c}$ e $y_n(a) \equiv y_n(b) \pmod{c}$.

Lema 2.16 Quando n é par, y_n é par e quando n é ímpar, y_n é ímpar.

Lema 2.17 $x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$.

Lema 2.18 $\forall\, n \in \mathbb{N}, y_{n+1} > y_n \geq n$.

Lema 2.19 $\forall\, n \in \mathbb{N}$, $a^n \leq x_n(a) < x_{n+1}(a)$ e $x_n(a) \leq (2a)^n$.

Lema 2.20 $x_{2n\pm j} \equiv -x_j \pmod{x_n}$.

Lema 2.21 $x_{4n\pm j} \equiv x_j \pmod{x_n}$.

Lema 2.22 Seja $x_i \equiv x_j \pmod{x_n}$, $i \leq j \leq 2n$, $n > 0$. Então $i = j$, exceto se $a = 2$, $n = 1$, $i = 0$ *e* $j = 2$.

Lema 2.23 Seja $x_i \equiv x_j \pmod{x_n}$, $0 < n$, $0 < i \leq n$, $0 \leq j < 4n$, então $j = i$ *ou* $j = 4n - i$.

Lema 2.24 Seja $0 < i \leq n$ e $x_i \equiv x_j \pmod{x_n}$ então $j \equiv \pm i \pmod{4n}$.

Lema 2.25 Se $a > y^k$ então $2ay - y^2 - 1 > y^k$

Lema 2.1 Não existem inteiros x, y, que satisfaçam a Equação de Pell e a inequação

$$1 < x + y\sqrt{d} < a + \sqrt{d}.$$

Demonstração.

Suponha que x, y satisfazem $x^2 - dy^2 = 1$ e $1 < x + y\sqrt{d} < a + \sqrt{d}$. Como ,

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

essa igualdade e a inequação implicam que $1 > x - y\sqrt{d} > a - \sqrt{d}$. Daí ,

$$\begin{cases} 1 > x - y\sqrt{d} > a - \sqrt{d} \\ e \\ 1 < x + y\sqrt{d} < a + \sqrt{d} \end{cases} \Longrightarrow \begin{cases} -1 < -x + y\sqrt{d} < -a + \sqrt{d} \\ e \\ 1 < x + y\sqrt{d} < a + \sqrt{d} \end{cases} \Longrightarrow 0 < 2y\sqrt{d} < 2\sqrt{d} \Longrightarrow 0 < y < 1.$$

Por fim chegamos em uma contradição portanto o Lema 2.1 está provado.

■

Lema 2.2 Sejam x, y e x', y' inteiros, que satisfaçam a Equação de Pell. Definindo $x'' = xx' + yy'd$ e $y'' = x'y + y'x$. Então x'' e y'' satisfazem a Equação de Pell.

Demonstração.

Pela definição temos que

$$\begin{cases} x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d}) \\ x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d}) \end{cases} \Longrightarrow (x'')^2 - d(y'')^2 = (x'' + y''\sqrt{d})(x'' - y''\sqrt{d})$$

$$= (x + y\sqrt{d})(x - y\sqrt{d})(x' - y'\sqrt{d})(x' + y'\sqrt{d}) = (x^2 - dy^2)(x'^2 - dy'^2) = 1.$$

■

Lema 2.3 x_n e y_n satisfazem a Equação de Pell.

Demonstração. Para $n = 1$ o lema é verdadeiro. De fato, $x_1(a) + y_1(a)\sqrt{d} = (a + \sqrt{d})^1 = a + \sqrt{d}$, o que implica que $x_1(a) = a$ e $y_1(a) = 1$, é a solução trivial da Equação de Pell. Suponha que o lema seja verdadeiro para $n - 1$, ou seja, $x_{n-1}(a)$ e $y_{n-1}(a)$ também satisfazem a equação. Logo

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

Utilizando o Lema 2.2 e a hipótese de indução, temos que $x_n(a)$ e $y_n(a)$ satisfazem a equação. ■

Lema 2.4 Sejam $x, y \in \mathbb{N}$ soluções da Equação de Pell. Então para algum $n \in \mathbb{N}^*$ temos , $x = x_n$ e $y = y_n$.

Demonstração.

Inicialmente note que $x + y\sqrt{d} \geq 1$. Por outro lado, a medida que n aumenta $\left(a + \sqrt{d}\right)^n$ tende ao infinito. Portanto existe um $n \geq 0$, tal que $\left(a + \sqrt{d}\right)^n \leq x + y\sqrt{d} < (a + \sqrt{d})^{n+1}$ se ocorre a igualdade $\left(a + \sqrt{d}\right)^n = x + y\sqrt{d}$ o resultado esta provado, caso contrario $x_n + y_n\sqrt{d} < x + y\sqrt{d} < \left(x_n + y_n\sqrt{d}\right)\left(a + \sqrt{d}\right)$ como $\left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) = 1$ (ver Lema 2.3), então o número $x_n - y_n\sqrt{d} > 0$ pois $x_n + y_n\sqrt{d} > 0$. Daí:

$$\left(x_n - y_n\sqrt{d}\right)\left(x_n + y_n\sqrt{d}\right) < \left(x_n - y_n\sqrt{d}\right)\left(x + y\sqrt{d}\right)$$
$$< \left(x_n - y_n\sqrt{d}\right)\left(x_n + y_n\sqrt{d}\right)\left(a + \sqrt{d}\right).$$

Logo,

$1 < \left(x_n - y_n\sqrt{d}\right)\left(x + y\sqrt{d}\right) < a + \sqrt{d} \underset{L\,2.2}{\Rightarrow} \exists x'', y'' \in \mathbb{Z} \mid 1 < x'' + y''\sqrt{d} < a + \sqrt{d}$.

Mas isto contradiz o lema 2.1. Logo , devemos ter $\left(a + \sqrt{d}\right)^n = x + y\sqrt{d}$, ou seja, $\exists\, n \in \mathbb{N} \mid x = x_n$ e $y = y_n$. ■

Lema 2.5 $x_{m\pm n} = x_m x_n \pm d y_m y_n$ e $y_{m\pm n} = y_m x_n \pm x_m y_n$.

Demonstração. $x_{m+n} + y_{m+n}\sqrt{d} \overset{\text{def}}{=} (a + \sqrt{d})^{m+n} = (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d}) = (x_m x_n + d y_m y_n) + (y_m x_n + x_m y_n)\sqrt{d}$.

Portanto, $\begin{cases} x_{m+n} = x_m x_n + d y_m y_n \\ \quad\quad e \\ y_{m+n} = y_m x_n + x_m y_n. \end{cases}$

De forma análoga, temos que $(x_{m-n} + y_{m-n}\sqrt{d})\left(x_n + y_n\sqrt{d}\right) = x_m + y_m\sqrt{d}$, e multiplicando por $x_n - y_n\sqrt{d}$ de ambos os lados, obtemos:

$x_{m-n} + y_{m-n}\sqrt{d} = \left(x_m + y_m\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) = (x_m x_n - d y_m y_n) + (y_m x_n - x_m y_n)\sqrt{d}$.

Portanto,

$$\begin{cases} x_{m-n} = x_m x_n - d y_m y_n \\ \quad\quad e \\ y_{m-n} = y_m x_n - x_m y_n. \end{cases} \quad ■$$

Lema 2.6 $y_{m\pm1} = ay_m \pm x_m \ e \ x_{m\pm1} = ax_m \pm dy_{m.}$

Demonstração.

Faça $n = 1$ no Lema 2.5 e lembre que $x_1 = a$ e $y_1 = 1$. Uma consequência desse Lema é que $y_{m+1} > y_m$ de fato pois $y_{m+1} = ay_m + x_m \geq ay_m > y_m$. Portanto segue por indução que $n > r \Leftrightarrow y_n > y_r$

■

Lema 2.7 $(x_n, y_n) = 1$.

Demonstração.

Seja $D \in \mathbb{N}^*$ tal que $D \mid x_n$ e $D \mid y_n$, então $D \mid x_n^2 - dy_n^2 \Longrightarrow D \mid 1 \Longrightarrow D = 1$

■

Lema 2.8 $y_n \mid y_{nk.} \ n \in \mathbb{N}^*$

Demonstração.

Vamos utilizar indução sobre k . O lema é verdadeiro para $k = 1$, já que, $y_n \mid y_{n.}$ .Suponha que seja verdadeiro para $k = m$, ou seja, $y_n \mid y_{nm.}$ Do Lema 2.5 temos que $y_{n(m+1)} = y_{mn+n} = y_{mn}x_n + x_{nm}y_n$. Como $y_n \mid x_{mn}\, y_n$ e pela hipótese de indução $y_n \mid y_{nm}x_n \Longrightarrow y_n \mid (y_{mn}x_n + x_{mn}\, y_n) \Longrightarrow y_n \mid y_{n(m+1)}$. Portanto o lema é válido para $k = m + 1$, o que conclui a prova por indução.

■

Lema 2.9 $y_n \mid y_t \Leftrightarrow n \mid t. \quad n \in \mathbb{N}^*$

Demonstração.

Inicialmente, suponha que $y_n \mid y_t$ mas que $n \nmid t$. Então podemos escrever $t = nq + r, 0 < r < n$. Então $y_t = y_{nq+r}$ e pelo Lema 2.5 temos que, $y_t = y_{nq}x_r + x_{nq}y_r$. Do Lema 2.8 $y_n \mid y_{nq}$ e por hipótese $y_n \mid y_t$, como $x_{nq}y_r = y_t - x_{nq}y_r$ segue que $y_n \mid x_{nq}\, y_r$.

Provemos agora que $(y_n, x_{nq}) = 1$, se $d \mid y_n$ e $d \mid x_{nq}$, pelo Lema 2.8 , $d \mid y_{nq}$ e do Lema 2.7 temos que $(x_{nq}, y_{nq}) = 1$, segue que $d \mid 1$, ou seja, $d = 1$. Portanto $y_n \mid y_r$, e daí $y_n \leq y_r$. Por outro lado como $n > r$, pela consequência do Lema 2.6 teriamos $y_n > y_r$, ou seja , $y_n \leq y_r$ e $y_n > y_r$ que é uma contradição. Portanto $r = 0 \Longrightarrow t = nq \Longrightarrow n \mid t$.

Reciprocamente, se $n \mid t \Longrightarrow t = nk$, pelo Lema 2.8 $y_n \mid y_{nk}$, ou seja, $y_n \mid y_t$.

■

Lema 2.10 $y_{nk} \equiv kx_n^{k-1}y_n \pmod{y_n^3}, \quad \forall\, k \in \mathbb{N}^*$.

Demonstração.

Por definição $x_{nk} + y_{nk}\sqrt{d} = (a+\sqrt{d})^{nk} = (x_n + y_n\sqrt{d})^k$ e pela fórmula do Binômio de Newton:

$$\left(x_n + y_n\sqrt{d}\right)^k = \sum_{j=0}^{k} \binom{k}{j} {x_n}^{k-j} {y_n}^j d^{\frac{j}{2}}$$

$$= \binom{k}{0}x_n^k + \binom{k}{1}x_n^{k-1}y_n d^{\frac{1}{2}} + \binom{k}{2}x_n^{k-2}y_n^2 d + \cdots + \binom{k}{k}y_n^k d^{\frac{k}{2}}.$$

Desta igualdade concluimos que ,

$$y_{nk}\sqrt{d} = \sum_{\substack{j=0 \\ j\ impar}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j}{2}} = kx_n^{k-1}y_n\sqrt{d} + \sqrt{d} \sum_{\substack{j=3 \\ j\ impar}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j-1}{2}} \implies$$

$$\implies y_{nk} = \sum_{\substack{j=0 \\ j\ impar}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j}{2}} = kx_n^{k-1}y_n + \sum_{\substack{j=3 \\ j\ impar}}^{k} \binom{k}{j} x_n^{k-j} y_n^j d^{\frac{j-1}{2}}$$

Para $j \geq 3$, os termos desta expansão são todos congruentes a zero (mod y_n^3). Então $y_{nk} \equiv kx_n^{k-1}y_n \pmod{y_n^3}$.

■

Lema 2.11 $y_n^2 \mid y_{n\,.\,y_n}$. $\quad n \in \mathbb{N}^*$

Demonstração. Utilizando $k = y_n$ no Lema 2.10 obtemos $y_{n\,.\,y_n} \equiv y_n^2 x_n^{y_n-1} \pmod{y_n^3}$ e desta congruência temos que $\exists t \in \mathbb{Z}$ tal que $y_{n\,.\,y_n} = (y_n)^3 t + y_n^2 x_n^{y_n-1} = y_n^2\left(y_n t + x_n^{y_n-1}\right)$, de onde concluímos que $y_n^2 \mid y_{n\,.\,y_n}$. ■

Lema 2.12 $y_n^2 \mid y_t \Rightarrow y_n \mid t. \quad n \in \mathbb{N}^*$

Demonstração.

Como $y_n^2 \mid y_t$, segue que $y_n \mid y_t$ e pelo Lema 2.9, $n \mid t$. Seja $t = nk$. Do Lema 2.10 temos que, $\exists u \in \mathbb{Z}$ tal que $kx_n^{k-1}y_n = y_{nk} - u(y_n)^3$ e como $y_n^2 \mid y_{nk}$ e $y_n^2 \mid (y_n)^3$ concluímos que $y_n^2 \mid kx_n^{k-1}y_n$, ou ainda, $y_n \mid kx_n^{k-1}$. Mas pelo Lema 2.7, $(x_n, y_n) = 1$. Então $y_n \mid k$, e como $t = nk$, segue que $y_n \mid t$. ■

Lema 2.13 $x_{n+1} = 2ax_n - x_{n-1}$ e $y_{n+1} = 2ay_n - y_{n-1}$.

Demonstração.

Do Lema 2.6 temos: $\begin{cases} x_{n+1} = ax_n + dy_n \ \ e \ \ y_{n+1} = ay_n + x_n, \\ \\ x_{n-1} = ax_n - dy_n \ \ e \ \ y_{n-1} = ay_n - x_n, \end{cases} \Longrightarrow \begin{cases} x_{n+1} + x_{n-1} = 2ax_n \\ e \\ y_{n+1} + y_{n-1} = 2ay_n \end{cases}$

e então , $x_{n+1} = 2ax_n - x_{n-1}$ e $y_{n+1} = 2ay_n - y_{n-1}$. Estas equações mais as condições iniciais $x_0 = 1, x_1 = a$, $y_0 = 0$ e $y_1 = 1$ determinam todos os valores de x_n e y_n.

■

Lema 2.14 $y_n(a) \equiv n \pmod{a-1}$.

Demonstração.

Para $n = 0 \ e \ n = 1$ a congruência é trivialmente satisfeita já que $y_0(a) = 0 \ \ e \ y_1(a) = 1$. Vamos supor que o lema é verdadeiro para $k \leq n$. Devemos mostrar que $y_{n+1}(a) \equiv n + 1 \pmod{a-1}$. Da hipótese de indução temos ,

$$\begin{cases} y_n(a) \equiv n \pmod{a-1} \\ e \\ y_{n-1}(a) \equiv n - 1 \pmod{a-1}. \end{cases}$$

Como $a \equiv 1 \pmod{a-1}$, segue das propriedades de conguência que $2ay_n(a) \equiv 2n \pmod{a-1}$, daí

$$\begin{cases} 2ay_n(a) \equiv 2n \pmod{a-1} \\ e \\ -y_{n-1}(a) \equiv -(n-1) \pmod{a-1} \end{cases}$$

Logo , $y_{n+1}(a) \overset{L2.13}{\equiv} 2ay_n(a) - y_{n-1}(a) \equiv 2n - (n-1) \equiv n + 1 \pmod{a-1}$. ■

Lema 2.15 Se $a \equiv b \pmod{c}$, então $\forall\, n \in \mathbb{N}, x_n(a) \equiv x_n(b) \pmod{c}$ e $y_n(a) \equiv y_n(b) \pmod{c}$.

Demonstração.

Vamos provar que $x_n(a) \equiv x_n(b) \pmod{c}$. Para $n = 0$ e $n = 1$ a congruência é trivialmente satisfeita já que $x_0(a) = x_0(b) = 1$, $y_0(a) = y_0(b) = 0$, $x_1(a) = a$, $x_1(b) = b$, $y_1(a) = y_1(b) = 1$. Vamos supor que o lema é verdadeiro para $k \leq n$. Em particular, $x_n(a) \equiv x_n(b) \pmod{c}$ e $x_{n-1}(a) \equiv x_{n-1}(b) \pmod{c}$. Daí,

$$\begin{cases} x_n(a) \equiv x_n(b) \pmod{c} \\ e \\ x_{n-1}(a) \equiv x_{n-1}(b) \pmod{c}. \end{cases} \Longrightarrow \begin{cases} 2ax_n(a) \equiv 2ax_n(b) \pmod{c} \\ e \\ -x_{n-1}(a) \equiv -x_{n-1}(b) \pmod{c}. \end{cases}$$

$$\Longrightarrow 2ax_n(a) - x_{n-1}(a) \equiv 2ax_n(b) - x_{n-1}(b) \pmod{c} \overset{L\,2.13}{\Rightarrow} x_{n+1}(a) \equiv x_{n+1}(b) \pmod{c}$$

A prova de que $y_n(a) \equiv y_n(b) \pmod{c}$ é feita de forma inteiramente análoga.

■

Lema 2.16 Quando n é par, y_n é par e quando n é ímpar, y_n é ímpar.

Demonstração.

Do Lema 2.13 $y_{m+1} \equiv 2ay_m - y_{m-1} \equiv y_{m-1} \pmod 2 \Longrightarrow y_{m+1} \equiv y_{m-1} \pmod 2$ daí temos dois casos

$0 = y_0 \equiv y_2 \equiv y_4 \equiv \cdots \equiv y_n \pmod 2$. Logo y_n é par quando n é par.

$1 = y_1 \equiv y_3 \equiv y_5 \equiv \cdots \equiv y_n \pmod 2$. Logo y_n é ímpar, quando n é ímpar.

■

Lema 2.17 $x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$.

Demonstração.

Para $n = 0$ e $n = 1$ a congruência é satisfeita.

$$x_0 - y_0(a-y) = 1 = y^0 \quad \text{e} \quad x_1 - y_1(a-y) = a - 1(a-y) = y = y^1.$$

Devemos mostrar que $x_{n+1}(a) - y_{n+1}(a)(a-y) \equiv y^{n+1} \pmod{2ay - y^2 - 1}$ para isso suponha que o lema seja verdadeiro para $k \leq n$. temos que:

$$x_{n+1}(a) - y_{n+1}(a)(a-y) \overset{L\,2.13}{=} (2ax_n - x_{n-1}) - (2ay_n - y_{n-1})(a-y) =$$
$$= 2a[x_n - y_n(a-y)] - [x_{n-1} - y_{n-1}(a-y)]$$

Mas pela hipótese de indução,

$$\begin{cases} x_n - y_n(a-y) \equiv y^n \pmod{2ay - y^2 - 1} \\ e \\ -[x_{n-1} - y_{n-1}(a-y)] \equiv -y^{n-1} \pmod{2ay - y^2 - 1} \end{cases}$$

Então,

$$x_{n+1}(a) - y_{n+1}(a)(a-y) \equiv 2ay^n - y^{n-1} \equiv y^{n-1}(2ay - 1) \equiv y^{n-1}.y^2 \equiv y^{n+1}$$

$\pmod{2ay - y^2 - 1}$ o que conclui a prova. Perceba que na última igualdade foi usado que $2ay - 1 \equiv y \pmod{2ay - y^2 - 1}$.

■

Lema 2.18 $\forall\, n \in \mathbb{N}$, $y_{n+1} > y_n \geq n$.

Demonstração.

Pela consequência do Lema 2.6, $y_{n+1} > y_n$. Resta provar que $y_n \geq n$. Se $n = 0$, o lema é verdadeiro, pois $y_0 = 0 \geq 0$. Suponha que o lema seja verdadeiro para n, ou seja, $y_n \geq n$. Sabemos que $y_{n+1} > y_n \Longrightarrow y_{n+1} \geq y_n + 1$, e pela hipótese de indução $y_{n+1} \geq n + 1$, o que conclui a prova.

■

Lema 2.19 $\forall\, n \in \mathbb{N}$, $a^n \leq x_n(a) < x_{n+1}(a)$ e $x_n(a) \leq (2a)^n$.

Demonstração.

Primeiro Provemos que $a^n \leq x_n(a) < x_{n+1}(a)$. Para $n = 0$, as desigualdades se verificam, pois $x_0 = 1$ e $x_1 = a > 1 = a^0$ portanto , $a^0 \leq x_0 < x_1$ suponha o lema válido para n. Devemos provar que $a^{n+1} \leq x_{n+1}(a) < x_{n+2}(a)$. De fato , pois

$$x_{n+2} \overset{L2.6}{=} ax_{n+1} + dy_{n+1} \geq ax_{n+1} > x_{n+1} \overset{L2.6}{=} ax_n + dy_n \geq ax_n \overset{indução}{\geq} a^{n+1}$$

$\Longrightarrow a^{n+1} \leq x_{n+1}(a) < x_{n+2}(a)$.

Provemos agora tambem por indução que $x_n(a) \leq (2a)^n$. Para $n = 0$ a desigualdade é verdadeira já que $x_0 \leq (2a)^0$, como $x_{n+1} \overset{L2.13}{=} 2ax_n - x_{n-1} \leq 2ax_n \overset{indução}{\leq} (2a)^{n+1} \Longrightarrow x_{n+1}(a) \leq (2a)^{n+1}$.

■

Lema 2.20 $x_{2n\pm j} \equiv -x_j \pmod{x_n}$.

Demonstração.

Pelas fórmulas de adição do Lema 2.5 e lembrando que $dy_n^2 = x_n^2 - 1$ temos :

$$x_{2n\pm j} \equiv x_{n+(n\pm j)} \equiv x_n x_{n\pm j} + dy_n y_{n\pm j} \equiv x_n\left(x_n x_j \pm dy_n y_j\right) + dy_n\left(y_n x_j \pm x_n y_j\right)$$

$\equiv dy_n^2 x_j \equiv (x_n^2 - 1)x_j \equiv -x_j \pmod{x_n}$.

■

Lema 2.21 $x_{4n\pm j} \equiv x_j \pmod{x_n}$.

Demonstração.

Pelo Lema 2.20. $x_{4n\pm j} \equiv x_{2n+(2n\pm j)} \equiv -x_{2n\pm j} \equiv -(-x_j) \equiv x_j \pmod{x_n}$.

■

Lema 2.22 Seja

$$x_i \equiv x_j \pmod{x_n}, \quad i \leq j \leq 2n \ , \ n > 0.$$

Então $i = j$, exceto se $a = 2 \ , \ n = 1 \ , \ i = 0 \ e \ j = 2$.

Demonstração.

$\boldsymbol{x_n}$ ***ímpar :*** Suponha que x_n é ímpar e seja $q = \frac{x_n - 1}{2}$. Então os números

$$-q, -q+1, -q+2, \dots, -1, 0, 1, \dots, q-1, q$$

Formam um sistema completo de restos módulos x_n.

Pelo Lema 2.19, $1 = x_0 < x_1 < \cdots < x_{n-1}$. Usando o Lema 2.6 $x_n = ax_{n-1} + dy_{n-1} \Longrightarrow x_{n-1} \leq \frac{x_n}{a} \leq \frac{x_n}{2}$, assim $x_{n-1} \leq q$.

Se $x_{n-1} = q \Longrightarrow 2x_{n-1} = x_n - 1 \Longrightarrow 2x_{n-1} + 1 = x_n \Longrightarrow dy_{n-1} = 1 \Longrightarrow d = 1$ absurdo já que $d > 1$. Se $x_{n-1} < q$ pelo Lema 2.20 os números $x_{n+1}, x_{n+2}, \dots, x_{2n-1}, x_{2n}$ são congruentes módulo x_n a respectivamente a $-x_{n-1}, -x_{n-2}, \dots, -x_1, -x_0$. Deste modo os números $x_0, x_1, \dots, x_{2n}$ são mutuamente incongruentes módulos x_n o que prova o resultado. Note que $x_n \equiv 0 \pmod{x_n}$.

$\boldsymbol{x_n}$ ***par :*** Suponha que x_n é par e seja $q = \frac{x_n}{2}$. Neste caso, os números abaixo formam um sistema completo de restos módulo x_n

$$-q+1, -q+2, \dots, -1, 0, 1, \dots, q-1, q$$

Como acima $x_{n-1} \leq q$. Assim, o resultado segue como acima, exceto se $x_{n-1} = q = \frac{x_n}{2}$, de modo que pelo Lema 2.13, $x_{n+1} \equiv -q \pmod{x_n}$ e se $i = n-1$ e $j = n+1$ nosso resultado seria falso já que

$$x_{n+1} \equiv -q \equiv q \equiv x_{n-1} (\text{mod } x_n) \Rightarrow \ x_{n+1} \equiv x_{n-1} (\text{mod } x_n)$$

mas $n - 1 \neq n + 1$. Novamente do Lema 2.6, $x_n = ax_{n-1} + dy_{n-1}$, e desse modo $x_n = 2x_{n-1}$ implica $a = 2$ e $y_{n-1} = 0$ já que $d > 0$, isto é, $n = 1$. Assim,o resultado pode falhar somente quando $a = 2 \ , \ n = 1 \ , \ i = 0 \ e \ j = 2$.

■

Repare que $x_i \equiv x_j \pmod{x_n} \iff x_j \equiv x_i \pmod{x_n}$ Assim,o resultado pode falhar quando $a = 2, n = 1, i = 2 \ e \ j = 0$.

Lema 2.23 Seja $x_i \equiv x_j \pmod{x_n}$, $0 < i \leq n$, $0 \leq j < 4n$, então $j = i$ *ou* $j = 4n - i$.

Demonstração.

Primeiro suponha que $j \leq 2n$. Então pelo Lema 2.22, $j = i$, exceto se o caso excepcional ocorrer.Como $i > 0$, então isto só pode acontecer se $j = 0$, $a = 2$, $n = 1$ e $i = 2$ que é uma contradição já que por hipótese $i \leq n$.

Por outro lado, seja $j > 2n$ e considerando $j' = 4n - j$, temos $0 < j' < 2n$. Do Lema 2.21,$x_{j'} \equiv x_j \pmod{x_n}$ mas por hipótese $x_i \equiv x_j \pmod{x_n}$ segue que $x_{j'} \equiv x_i \pmod{x_n}$. Novamente $j' = i$, exceto se o caso excepcional do Lema 2.22 ocorrer, mas isto esta fora de questão já que , i e $j' > 0$.

■

Lema 2.24 Seja $0 < i \leq n$ e $x_i \equiv x_j \pmod{x_n}$ então $j \equiv \pm i \pmod{4n}$.

Demonstração.

Escrevendo $j = 4nq + j'$, $0 \leq j' < 4n$. Note agora que

$4nk + j' = 4n + 4n(k-1) + j'$, $1 \leq k \leq q \implies x_j \equiv x_{4n(q-1)+j'} \equiv \cdots \equiv$

$x_{4n(1-1)+j'} \pmod{x_n} \underset{L2.8}{\implies} x_j \equiv x_{j'} \pmod{x_n} \implies x_i \overset{Hipótese}{\equiv} x_j \equiv x_{j'} \pmod{x_n}$. E pelo Lema 2.23, $i = j'$ ou $i = 4n - j'$.Se $i = 4n - j'$, como $j = 4nq + j' \implies i + j \equiv 4n(q+1) \equiv 0 \ (mod\ 4n) \implies j \equiv -i \pmod{4n}$.Se $i = j'$, como $j = 4nq + j' \implies j - i \equiv 4nq \equiv 0 \ (mod\ 4n) \implies j \equiv i \pmod{4n}$.

■

Lema 2.25 Se $a > y^k$ então $2ay - y^2 - 1 > y^k$

Demonstração.

Defina $g: \mathbb{R} \longrightarrow \mathbb{R}$, $g(y) = 2ay - y^2 - 1$. Então $g(1) = 2a - 2 \geq a$, pois $a \geq 2$. Derivando $g(y)$ temos $g'(y) = 2a - 2y$, Para $1 \leq y < a$, $g'(y) = 2a - 2y > 0$, ou seja, a função $g(y)$ é crescente nesse intervalo e consequentimente $g(y) \geq a$ no intervalo , como por hipótese $a > y^k$ portanto ,

$g(y) > y^k \implies 2ay - y^2 - 1 \geq a > y^k$.

■

Estes lemas serão necessarios para provarmos os dois resultados seguintes. Considere o seguinte sistema de equações Diofantinas.

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. $y = k + e - 1.$

Vale o seguinte resultado:

Teorema 2.1 Dados $a, x, k,\ (a > 1)$, o sistema de (I)-(VIII) tem solução em $\mathbb{N}^*$ 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 dadas as soluções de (I)-(VIII).De (V), $b > a > 1$. Pelo Lema 2.4 concluímos a partir de (I), (II) e (III) que existem $i, j, n > 0$ tais que:

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

Perceba que i, j ou n não pode ser nulo.

1) $\boldsymbol{b \equiv a \pmod{x_n(a)}}$ **e** $\boldsymbol{x_i(a) \equiv x_j(b) \pmod{x_n(a)}}$

As equações (V) e (VI) produzem respectivamente essas congruências.

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

Como $b \equiv a \pmod{x_n(a)} \overset{L2.15}{\Rightarrow} x_j(b) \equiv x_j(a) \pmod{x_n(a)}$.

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

Usando 1) e 2) temos $x_i(a) \equiv x_j(b) \equiv x_j(a) \pmod{x_n(a)} \Longrightarrow x_i(a) \equiv x_j(a) \pmod{x_n(a)}$.

4) $\boldsymbol{j \equiv \pm i \pmod{4n}}$

Usando (IV) temos que $v > y \Longrightarrow y_n(a) > y_i(a) \overset{L2.6}{\Rightarrow} n > i > 0$.

$x_i(a) \equiv x_j(a) \pmod{x_n(a)} \overset{L2.24}{\Rightarrow} j \equiv \pm i \pmod{4n}$

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

Da equação (IV) deduz-se que $(y_i(a))^2 \mid y_n(a)$ e do Lema 2.12 $y_i(a) \mid n$, daí (4) implica que $j \equiv \pm i \pmod{4y_i(a)}$.

6) $\boldsymbol{y_j(b) \equiv j \pmod{4y_i(a)}}$

Da equação (V) $b - 1 = 4py$ e do Lema 2.14 $y_j(b) \equiv j \pmod{b-1} \Longrightarrow y_j(b) \equiv j \pmod{4py} \Longrightarrow y_j(b) \equiv j \pmod{4y} \Longrightarrow y_j(b) \equiv j \pmod{4y_i(a)}$.

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

Segue diretamente de (VII).

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

Segue diretamente da relação de transitividade entre 5), 6) e 7)

9) $\boldsymbol{k = i}$

A equação (VIII) produz $k \leq y_i(a)$ e o Lema 2.18 $i \leq y_i(a)$, ou seja, $-2y_i(a) < k \pm i \leq 2y_i(a)$, mas $4y_i(a) \mid k \pm i$, daí $k \pm i = 0$. como $k + i > 0$, temos $k - i = 0$, isto é , $k = i$ assim $x = x_i(a) = x_k(a)$.

Reciprocamente, seja $x = x_k(a)$ devemos mostrar que o sistema de (I)-(VIII) tem solução nos argumentos restantes $y, u, v, s, t, b, r, p, q, c, d, e$.

1) Como $x = x_k(a)$ então $y = y_k(a)$ satisfaz **(I)**.

2) Considere $m = 2ky_k(a)$ e seja $u = x_m(a)$ e $v = y_m(a)$. Então **(II)** é satisfeita.

3) Pelo Lema 2.11 , $y_k^2 \mid y_{k\,.y_k}$, mas $k.y_k \mid m$, pelo Lema 2.9, $y_{k.y_k} \mid y_m$. Portanto $y_k^2 \mid y_m$, isto é, $y_k^2 \mid v$.com isto podemos escolher r satisfazendo **(IV)**.

4) Além disso, como m é par, pelo Lema 2.16, v é par e como u e v satisfazem (II) segue que u é ímpar. Pelo Lema 2.7, $(u, v) = 1$. Provemos agora que $(u, 4y) = 1$, de fato, seja p um número primo que divide u e $4y$ então $p \mid y$ pois u é ímpar, e como $k \mid m$ pelo Lema 2.9. $y_k \mid y_m$, isto é , $y \mid v$, logo $p \mid v$ e como $(u, v) = 1$ segue que $p \mid 1$, uma contradição.

   Pelo Teorema do Resto Chinês podemos encontrar b_0 tal que: $\begin{cases} b_0 \equiv 1 \ (mod\ 4y) \\ \qquad e \\ b_0 \equiv a \ (mod\ u), \end{cases}$

   Como $4jyu \equiv 0 \pmod{4y}$ e $4jyu \equiv 0 \pmod{u}$, então $b_0 + 4jyu$ também satisfaz as congruências, e podemos encontrar b, p, q satisfazendo a equação **(V)**.

5) A equação **(III)** é satisfeita, definindo, $s = x_k(b)$ e $t = y_k(b)$. Perceba que $s > x$. pois,

$$b > a \overset{Exemplo\ 2.3}{\Rightarrow} x_k(b) > x_k(a) \Rightarrow s > x.$$

6) Provemos agora que $s \equiv x \pmod{u}$. De fato , da equação (V) temos que $b \equiv a \ (mod\ u)$, agora usando o Lema 2.15 temos $x_k(b) \equiv x_k(a) (mod\ u)$. Assim c , pode ser escolhido de forma a satisfazer **(VI)**.

7) Pelo Lema 2.18, $y_k(b) \geq k$, ou seja, $t \geq k$ e pelo Lema 2.14, $t = y_k(b) \equiv k \pmod{b-1}$ e assim, usando (V) temos que $4y \mid (b-1)$ daí , $t \equiv k \pmod{4y}$. Podemos então escolher d satisfazendo a equação **(VII)**.

8) Ainda pelo Lema 2.18 , $y \geq k$, então **(VIII)** pode ser satisfeito tomando $e = y - k + 1$.

■

O Teorema 2.1 implica que o conjunto

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

é Diofantino, basta utilizar o Lema 1.1 para reduzir o sistema de equações Diofantinas (I)-(VIII) a uma só equação.

Colorário 2.1 A função $g(z, k) = x_k(z + 1)$ é Diofantina.

Incluindo ao sistema (I)-(VIII) a equação $a = z + 1$ (*)Pelo teorema 2.1, o sistema (*),(I)-(VIII) tem solução se, $x = x_k(a) = g(z, k)$.Desse modo, pode-se mostrar que g é Diofantina utilizando a maneira usual de somar os quadrados dos nove polinômios. ■

Agora acrescente ao sistema (I)-(VIII) as seguintes equações:

(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) $a^2 - (w^2 - 1)(w-1)^2 z^2 = 1$.

Com isto podemos provar o seguinte Lema.

Lema 2.26 $m = n^k \iff$ as equações (I)-(XII) tem uma solução em $\mathbb{N}^*$ nos argumentos restantes.

Demonstração.

Suponha que (I)-(XII) é satisfeito.

1) $w > 1$ e $a > 1$.

Por (XI), $w > 1$. Assim $(w-1)z > 0$, e por (XII), $a > 1$.

2) $\exists k \in \mathbb{N} \mid\ x = x_k(a)$ e $y = y_k(a)$

Basta aplicar o Teorema 2.1.

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

Basta extrair as raízes quadradas em (IX) e usar o Lema 2.17 respectivamente.

4) $m \equiv n^k \pmod{2an - n^2 - 1}$ e $n, k < w$.

Aplicando transitividade em 3) e usando a equação (XI) respectivamente.

5) $\exists j \in \mathbb{N} \mid\ a = x_j(w)$, $(w-1)z = y_j(w)$ e $y_j(w) \equiv j \pmod{w-1}$

Segue diretamente do Lema 2.4 aplicado em XII e do Lema 2.14 respectivamente

6) $j \equiv 0 \pmod{w-1}$
De 5) temos $(w-1)z = y_j(w)$ ou seja $y_j(w) \equiv 0 \pmod{w-1}$. Mas $y_j(w) \equiv j \pmod{w-1}$,Logo por transitividade $j \equiv y_j(w) \equiv 0 \pmod{w-1}$.

7) $w - 1 \leq j$ e $a \geq w^j$
De 6) $w - 1 \mid j$ e $j \neq 0$, segue que $w - 1 \leq j$. Para segunda afirmação basta usar o Lema 2.19 lembrando que $x_j(w) = a$.

8) $a > n^k$
Lembrando que $n, k < w$, $a \geq w^j$ e $w - 1 \leq j$. Obtemos que $a \geq w^j \geq w^{w-1} > n^{w-1} \geq n^k$

9) $m < 2an - n^2 - 1$ e $n^k < 2an - n^2 - 1$.

Basta usar a equação (X) e aplicar o Lema 2.25 em 8) respectivamente.

10) $m = n^k$

Segue diretamente da combinação entre 4) e 9).

Reciprocamente, suponha que $m = n^k$. Devemos encontrar soluções para o sistema (I)-(XII).

1) Escolha algum w tal que $w > k, n$ .Seja $a = x_{w-1}(w)$ tal que $a > 1$. Pelo Lema 2.14,

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

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

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

Tomando

$$\begin{cases} x_{w-1}(w) = a \\ e \\ y_{w-1}(w) = z(w-1) \end{cases}$$

Temos que **(XII)** é satisfeita.

2) Definindo $h = w - n$ e $l = w - k$, temos que a equação **(XI)** é satisfeita.

3) Provemos agora que $a > n^k$, como $w > k, n$ e $x_{w-1}(w) = a$. Daí

$$a \overset{L2.19}{\geq} w^{w-1} > n^{w-1} \geq n^k$$

e novamente pelo Lema 2.25, $m = n^k < 2an - n^2 - 1$.

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

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

Assim, **(X)** é satisfeita.

4) Definindo $x = x_k(a)$ e $y = y_k(a)$. O Lema 2.17 nos permite definir $f \in \mathbb{N}^*$ tal que:

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

De forma que **(IX)** é satisfeita.

5) Finalmente, o sistema **(I)-(VIII)** pode ser satisfeito pelo Teorema 2.1.

■

Pelo Lema 2.26, temos que o conjunto $N = \{(m,n,k) \in (\mathbb{N}^*)^3 \mid m = n^k\}$.é Diofantino. Basta utilizar o Lema 1.1 para reduzir o sistema de equações Diofantinas (I)-(XII) a uma só equação. E esta conclusão implica diretamente no resultado mais importante desta seção que enunciamos no próximo teorema.

Teorema 2.2 A função exponencial $h : (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$, $h(n,k) = n^k$ é Diofantina

3.2 A linguagem dos predicados diofantinos

Agora que provamos que a função exponecial é Diofantina, podemos mostrar que muitas outras funções e conjuntos também são.

Exemplo 2.4. A função $h: (\mathbb{N}^*)^3 \longrightarrow \mathbb{N}^*$, $h(u,v,w) = u^{v^w}$ é diofantina.

De fato, $y = u^{v^w} \iff (\exists\, z \in \mathbb{N}^*)(y = u^z \wedge z = v^w)$,

Onde "∧" é o simbolo lógico para "e". Usando o Teorema 2.2, existe um polinômio P tal que:

$$y = u^z \iff (\exists\, r_1, \dots, r_n \in \mathbb{N}^*)[P(y,u,z,r_1,\dots,r_n) = 0],$$

$$z = v^w \iff (\exists\, s_1, \dots, s_n \in \mathbb{N}^*)[P(z,v,w,s_1,\dots,s_n) = 0].$$

Então, $y = u^{v^w} \iff (\exists\, r_1, \dots, r_n, s_1, \dots, s_n)[P^2(y,u,z,r_1,\dots,r_n) + P^2(z,v,w,s_1,\dots,s_n) = 0]$.

■

Este procedimento é perfeitamente generalizável e isso já sabemos das proposições 1.1 e 1.2 vistas no capítulo 1. Expressões que já são conhecidas por gerar conjuntos Diofantinos podem ser combinadas livremente utilizando os operadores lógicos "∧" e "∨", a expressão resultante será novamente um conjunto Diofantino. Estas expressões são chamadas de predicados Diofantinos.

Nesta linguagem é permitido o uso dos símbolos lógicos "∨" para "ou", assim

$$(\exists\, r_1, \dots, r_n \in \mathbb{N}^*)[P_1 = 0] \ \vee\ (\exists\, s_1, \dots, s_m \in \mathbb{N}^*)[P_2 = 0]$$
$$\iff (\exists\, r_1, \dots, r_n, s_1, \dots, s_m \in \mathbb{N}^*)[P_1.P_2 = 0].$$

$$(\exists\, r_1, \dots, r_n \in \mathbb{N}^*)[P_1 = 0] \wedge (\exists\, s_1, \dots, s_m \in \mathbb{N}^*)[P_2 = 0]$$
$$\iff (\exists\, r_1, \dots, r_n, s_1, \dots, s_m \in \mathbb{N}^*)[{P^2}_1 + {P^2}_2 = 0].$$

Três importantes funções Diofantinas são dadas pelo :

Teorema 2.3 As seguintes funções são Diofantinas:

$$\begin{cases} f(n,k) = \binom{n}{k} \\ g(n) = n! \\ h(a,b,y) = \prod_{k=1}^{y} (a + bk) \end{cases}$$

Na prova deste teorema a notação $[\alpha]$, onde α é um número real, será usada para denotar o único inteiro tal que:

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

Lema 2.27 Para $0 < k \leq n, \quad u > 2^n$ temos que

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

Demonstração.

$(u+1)^n = \sum_{i=0}^{n} \binom{n}{i} u^i \Longrightarrow \frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = S + R,$ Onde $S = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$ e $R = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$. Como $u^{i-k} \in \mathbb{N}^*$ para $k \leq i \leq n$ então S é um inteiro e para

$0 \leq i \leq k-1$, $-k \leq i-k \leq -1$, logo $u^{i-k} \leq u^{-1}$ assim ,

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

Assim, $S \leq \frac{(u+1)^n}{u^k} < S + 1,$ O que prova o resultado.

■

Lema 2.28 Para $0 < k \leq n, \quad u > 2^n$ temos que.

$$\left[\frac{(u+1)^n}{u^k}\right] \equiv \binom{n}{k} \pmod{u}.$$

Demonstração.

Pelo Lema 2.27 , temos que $\left[\frac{(u+1)^n}{u^k}\right] = \sum_{i=k}^{n} \binom{n}{i} u^{i-k} = \binom{n}{k} u^0 + \binom{n}{k+1} u^1 + \cdots + \binom{n}{n} u^{n-k} \equiv \binom{n}{k} \pmod{u}$. ■

Lema 2.29 $f : (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*,\ f(n,k) = \binom{n}{k}$ é Diofantina.

Demonstração.

Como

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

Do Lema 2.28 $\left[\frac{(u+1)^n}{u^k}\right] \equiv \binom{n}{k} \pmod{u}$ e sabemos que $0 < \binom{n}{k} < u$. Portanto $\binom{n}{k}$ é o único inteiro positivo congruente a $\left[\frac{(u+1)^n}{u^k}\right] \pmod{u}$ e menor que u. Desse modo,

$$z = \binom{n}{k} \Leftrightarrow (\exists\, u, v, w \in \mathbb{N}^*)(v = 2^n \ \wedge\ u > v \ \wedge\ w = \left[\frac{(u+1)^n}{u^k}\right] \ \wedge\ z \equiv w \pmod{u}$$

$$\wedge\ z < u).$$

Para ver que $\binom{n}{k}$ é Diofantina, é suficiente notar que cada expressão acima separada por "∧" é um predicado Diofantino.

1) $v = 2^n$ é claramente Diofantino pelo Teorema 2.2.
2) A inequação $u > v$ é claramente Diofantina pelo exemplo 1.4.
3) A congruência $z \equiv w \pmod{u}$ é Diofantina pelo exemplo 1.8.
4) $w = \left[\frac{(u+1)^n}{u^k}\right] \Leftrightarrow (\exists\, x, y, t)\left(t = u+1 \wedge x = t^n \wedge y = u^k \wedge w \leq \frac{x}{y} < w+1\right)$,

E

$$w \leq \frac{x}{y} < w+1 \Leftrightarrow wy \leq x < (w+1)y.$$

■

Lema 2.30 Se $r > (2x)^{x+1}$, então $x! = \left[\frac{r^x}{\binom{r}{x}}\right]$.

Demonstração.

Para $x = 0$, o resultado é imediato pois $1! = \left[\frac{r^0}{\binom{r}{0}}\right]$, consideremos agora $x > 0$ então, é verdade que

$\frac{r^x}{\binom{r}{x}} < x!\frac{1}{\left(1-\frac{x}{r}\right)^x}$ pois ,

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

$$= x!\left(\frac{1}{\left(1-\frac{0}{r}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{(x-1)}{r}\right)}\right) < x!\frac{1}{\left(1-\frac{x}{r}\right)^x}$$

$$\frac{\mathbf{1}}{\mathbf{1}-\frac{\boldsymbol{x}}{\boldsymbol{r}}} < 1+\frac{\boldsymbol{2x}}{\boldsymbol{r}}$$

Por hipótese , $r > (2x)^{x+1} \Longrightarrow \frac{x}{r} < \frac{1}{2.(2x)^x} < \frac{1}{2}$. Logo ,

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

$$\left(\mathbf{1}+\frac{\boldsymbol{2x}}{\boldsymbol{r}}\right)^{\boldsymbol{x}} < 1+\frac{\boldsymbol{2x}}{\boldsymbol{r}}.\boldsymbol{2^x}$$

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

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

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

Pois $x\,.\,x! \leq x^{x+1}$.

$$\frac{\boldsymbol{r^x}}{\binom{\boldsymbol{r}}{\boldsymbol{x}}} < x! + 1$$

Por hipótese $\frac{(2x)^{x+1}}{r} < 1$, Portanto $\frac{r^x}{\binom{r}{x}} \leq x! + \frac{(2x)^{x+1}}{r} < x! + 1.$

$$\boldsymbol{x!} \leq \frac{\boldsymbol{r^x}}{\binom{\boldsymbol{r}}{\boldsymbol{x}}}$$

Como $\frac{r^x}{r.(r-1)\ldots(r-x+1)} \geq 1$, teremos $\frac{r^x.x!}{r.(r-1)\ldots(r-x+1)} \geq x! \Rightarrow \frac{r^x}{\binom{r}{x}} \geq x!$, segue que

$$x! \leq \frac{r^x}{\binom{r}{x}} < x! + 1.$$

O que conclui a prova do lema.

■

Lema 2.31 $g: \mathbb{N}^* \longrightarrow \mathbb{N}^*,\ g(n) = n!$ é uma função Diofantina.

Demonstração.

Basta mostrar que

$$m = n! \Leftrightarrow \begin{cases} \exists\, r,s,t,u,v \in \mathbb{N}^* \mid s = 2n+1 \ \wedge\ t = n+1 \\ \wedge\ r = s^t \ \wedge\ u = r^n \ \wedge \\ \wedge\ v = \binom{r}{n} \wedge\ mv \leq u < (m+1)v. \end{cases}$$

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 2.30 ,

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

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

Como $mv \leq u < (m+1)v \implies \left[\frac{u}{v}\right] = m \implies \left[r^n / \binom{r}{n}\right] = m$, Note que $r = s^t = (2n+1)^{n+1} > (2n)^{n+1}$, daí novamente pelo Lema 2.30 ,

$$n! = \left[r^n / \binom{r}{n}\right] \implies m = n!$$

■

Lema 2.32 Seja $bq \equiv a \pmod m$. Então,

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

Demonstração.

$$\begin{aligned} b^y \cdot y! \binom{q+y}{y} &= \frac{b^y \cdot y! \cdot (q+y)!}{y! \cdot q!} = \frac{b^y \cdot (q+y)!}{q!} \\ &= \frac{b^y \cdot (q+y) \cdot (q+y-1) \cdots (q+1) \cdot q!}{q!} \\ &= b^y \cdot (q+y) \cdot (q+y-1) \cdots (q+1) \\ &= (bq+yb) \cdot (bq+(y-1)b) \cdots (bq+b). \end{aligned}$$

Mas por hipótese $bq \equiv a \ (mod\, m)$, segue que:

$$\begin{aligned} &(bq+yb) \cdot (bq+(y-1)b) \cdots (bq+b) \equiv (a+yb) \cdot (a+(y-1)b) \cdots (a+b) \\ &\equiv \prod_{k=1}^{y}(a+bk) \quad (mod\, m). \end{aligned}$$

E isto prova o resultado.

■

Lema 2.33 $h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ é uma função Diofantina.

Demonstração.

No Lema 2.32, faça $m = b(a+by)^y + 1$. Então $(m,b) = 1$ e $m > \prod_{k=1}^{y}(a+bk) > 0$. Logo, a congruência $bX \equiv a\ (mod\ m)$ possui uma única solução $X = q$ tal que $0 \leq q < m$ daí $bq \equiv a\ (mod\ m)$.Do Lema 2.32 $\prod_{k=1}^{y}(a+bk)$ é o único número menor que m que é congruente módulo m a $b^y y!\binom{q+y}{y}$, isto é,

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

$$\{r = a+by \ \wedge\ s = r^y \ \wedge\ m = bs+1 \ \wedge\ bq = a+mt \ \wedge\ u = b^y \ \wedge\ v = y! \ \wedge\ z < m$$

$$\wedge\ \ w = q+y \ \wedge\ x = \binom{w}{y} \ \wedge\ z + mp = uvx\}$$

Como a função exponencial, combinatorial e fatorial são diofantinas segue que h é uma função diofantina.A afirmação do Teorema 2.3 está provada pelos Lemas 2.29, 2.31 e 2.33.

■

3.3 Novos conjuntos diofantinos

Com este lema 2.33 , combinado com os próximos Lemas 2.34 e 2.35 poderemos mostrar que é diofantino o seguinte conjunto:

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

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 2.34

$$\forall k \in \mathbb{N}^* \text{com } k \leq y,\ \exists\ y_1 \dots, y_m\ \in \mathbb{N}^* \mid P(y,k,x_1,\dots,x_n,y_1,\dots,y_m) = 0$$

$$\Updownarrow$$

$$\exists u \in \mathbb{N}^* \mid \forall k \in \mathbb{N}^* \text{com } k \leq y, \exists\ y_1 \dots, y_m\ \in \mathbb{N}^* \text{ com } y_i \leq u,\ i = 1, \dots, m \ \mid\ P(y,k,x_1,\dots,x_n,y_1,\dots,y_m) = 0$$

Demonstração.

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

$P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right)=0$.

Tomando u como sendo o máximo destes números , isto é.

$$u = \max\{\, y_i^{(k)} \mid \ 1 \le i \le m \ ; 1 \le k \le y\}.$$

Segue que,

$$\exists u \in \mathbb{N}^* \mid \forall k \in \mathbb{N}^* \text{com } \ k \le y, \exists\, y_1 \dots, y_m \ \in \mathbb{N}^* \text{ com } y_i \le u, \ i = 1,\dots,m \ \mid \ P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)=0$$

A recíproca é trivial.

■

Lema 2.35 Seja $Q(y,u,x_1,\dots,x_n)$ um polinômio com as propriedades:

(1) $Q(y,u,x_1,\dots,x_n) > u$,

(2) $Q(y,u,x_1,\dots,x_n) > y$,

(3) $k \le y \ e \ y_1,\dots,y_m \le u \implies \mid P(y,k,x_1,\dots,x_n,y_1,\dots,y_m\,)\mid \ \le Q(y,u,x_1,\dots,x_n)$.

Então,

$$\forall k \in \mathbb{N}^* \text{com } k \le y, \ \exists\, y_1 \dots, y_m \ \in \mathbb{N}^* \mid P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)=0$$

$$\Updownarrow$$

$$(*)\begin{cases} \exists\, c,t,a_1,\dots,a_m \in \mathbb{N}^* \mid \ 1+ct=\prod_{k=1}^{y}(1+kt) \\ t = Q(y,u,x_1,\dots,x_n)! \\ 1+ct \mid \prod_{j=1}^{u}(a_i-j)\,, \qquad 1 \le i \le m \\ P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv 0 \ \ (mod\ 1+ct). \end{cases}$$

Demonstração.

Provemos que $\forall k \in \mathbb{N}^* \text{com } \ k \le y, \ \exists\, y_1 \dots, y_m \ \in \mathbb{N}^* \mid P(y,k,x_1,\dots,x_n,y_1,\dots,y_m)=0$,supondo a validade de **(1), (2), (3)** e **(*)**. Para cada $k = 1,2,\dots,y,$ seja p_k um fator primo de $1+kt$. Seja $y_i^{(k)}$ o resto da divisão de a_i por p_k , ou seja, $a_i \equiv y_i^{(k)} \ \ (mod\ p_k)$ onde $(1 \le k \le y \ ; \ 1 \le i \le m)$. Disto segue que para cada k,i:

$$\begin{cases} \boldsymbol{a}) \quad 1 \le y_i^{(k)} \le u, \\ \boldsymbol{b}) \quad P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right)=0 \end{cases}$$

Demonstração de (a)

Note que por definição $p_k \mid 1+kt$, por hipótese $(*)$ $1+kt \mid 1+ct$ e $1+ct \mid \prod_{j=1}^{u}(a_i-j)$, por transitividade, $p_k \mid \prod_{j=1}^{u}(a_i-j)$. Assim, como p_k é primo, $p_k \mid a_i-j$ para algum $j \in \{1,2,\dots,u\}$, ou seja, $j \equiv a_i \ (mod\ p_k)$.Daí também por transitividade , $j \equiv y_i^{(k)} \ (mod\ p_k)$.

Uma vez que $t = Q(y,u,x_1,\dots,x_n)$! isso implica que $p_k > Q(y,u,x_1,\dots,x_n)$, suponha o contrário então isso implicaria que $p_k \leq Q(y,u,x_1,\dots,x_n) \Longrightarrow p_k \mid t$, mas por definição $p_k \mid 1+kt$, portanto $p_k \mid 1$, absurdo. Daí todo divisor primo de $1+kt$ deve ser maior que $Q(y,u,x_1,\dots,x_n)$.

De **(1)**, $p_k > u$. Portanto, $j \leq u < p_k$. Uma vez que $y_i^{(k)}$ é o resto da divisão de a_i por p_k temos também que $y_i^{(k)} < p_k$. Assim. $y_i^{(k)}, j$ são ambos menores que p_k ,positivos e congruentes a p_k então $y_i^{(k)} = j$ e como $1 \leq j \leq u$ segue que $1 \leq y_i^{(k)} \leq u$.

Demonstração de (b)

Primeiro provemos que $k \equiv c \ (mod\ p_k)$ para isso lembre que $p_k \mid 1+kt$ e $p_k \mid 1+ct$, então$p_k \mid k(1+ct) - c(1+kt) \Longrightarrow p_k \mid k-c \Longrightarrow k \equiv c \ (mod\ p_k)$.Por definição já sabemos que $a_i \equiv y_i^{(k)} \ (mod\ p_k)$, $1 \leq i \leq m$.

E por hipótese **(*)**,

$$P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right) \equiv P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv 0 \ (mod\ 1+ct).$$

Como, $p_k \mid (1+ct)$ temos ,

$$P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right) \equiv P(y,c,x_1,\dots,x_n,a_1,\dots,a_m) \equiv 0 \ (mod\ p_k).$$

Assim, $P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right)$ é múltiplo de p_k e , por **(3)** , temos que

$$\left| P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right) \right| \leq Q(y,u,x_1,\dots,x_n) < p_k.$$

Portanto, $P\left(y,k,x_1,\dots,x_n,y_1^{(k)},\dots,y_m^{(k)}\right) = 0$. Isto prova **(b)** e completa a primeira parte da demonstração.

Reciprocamente, supondo válida que $\forall k \in \mathbb{N}^*$com $k \leq y$, $\exists\, y_1 \ldots, y_m \in \mathbb{N}^* \mid P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$ e também a validade de **(1),(2)** e **(3)** . Verifiquemos a validade de (*).

I) Supondo que, $P\left(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}\right) = 0$, para cada $1 \leq k \leq y$, onde cada $y_j^{(k)} \leq u$. Nós fixamos $\boldsymbol{t := Q(y, u, x_1, \ldots, x_n)!}$.

II) Note que $\prod_{k=1}^{y}(1 + kt) \equiv 1 \ (mod\ t)$, então existe $c \in \mathbb{N}^*$ tal que $\boldsymbol{1 + ct = \prod_{k=1}^{y}(1 + kt)}$.

III) 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 $p \mid (l - k)t$ daí como p é primo temos dois casos:

Se $p \mid (l - k)$ teríamos que $p \leq l - k < y$ e por **(2)** temos $p < y < Q(y, u, x_1, \ldots, x_n) \Longrightarrow p \mid Q(y, u, x_1, \ldots, x_n)\ ! \Longrightarrow p \mid t \Longrightarrow p \mid 1$,contradição. Se $p \mid t \Longrightarrow p \mid 1$ temos um absurdo. Portanto, $(1 + kt, 1 + lt) = 1$. Desse modo os números $1 + kt$, com $1 \leq k \leq y$ são primos entre si, e o Teorema Chinês do Resto pode ser aplicado para produzir, para cada i, $1 \leq i \leq m$, um número a_i tal que

$$a_i \equiv y_i^{(k)} \quad (mod\ 1 + kt), \qquad 1 \leq k \leq y$$

Provemos agora que $k \equiv c \ (mod\ 1 + kt)$. Como $1 + kt \mid 1 + ct$, temos que $1 + kt \mid k(1 + ct) - c(1 + kt)$,ou seja , $1 + kt \mid k - c$. Assim, para cada $1 \leq k \leq y$, temos que $P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv P\left(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}\right) \ (mod\ 1 + kt)$ .Como por hipótese $P\left(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}\right) = 0$, temos que

$$P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \ (mod\ 1 + kt)$$

Uma vez que os números $1 + kt$ são primos entre si e cada um divide $P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m)$, fazendo seu produto,obtemos:

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

Pois,

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

IV) Lembrando que ,

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

Isto é,

$$1 + kt \mid a_i - y_i^{(k)}$$

e como $1 \leq y_i^{(k)} \leq u$,

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

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

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

■

Teorema 2.4

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

$$\begin{cases} R = \{(y, x_1, \dots, x_n) \in (\mathbb{N}^*)^{n+1} : \exists k \in \mathbb{N}^* \text{ com } k \leq y\ , \exists\ y_1 \dots, y_m\ \in \mathbb{N}^* \mid P(y, k, x_1, \dots, x_n, y_1, \dots, y_m) = 0\}. \\ S = \{(y, x_1, \dots, x_n) \in (\mathbb{N}^*)^{n+1} : \forall k \in \mathbb{N}^* \text{ com } k \leq y\ , \exists\ y_1 \dots, y_m\ \in \mathbb{N}^* \mid P(y, k, x_1, \dots, x_n, y_1, \dots, y_m) = 0\}. \end{cases}$$

Demonstração.

R é um conjunto diofantino

Como $(y, x_1, \dots, x_n) \in R \Leftrightarrow \exists\ k, y_1 \dots, y_m \in \mathbb{N}^* \mid k \leq y$ e $P(y, k, x_1, \dots, x_n, y_1, \dots, y_m) = 0$. Segue que R é um conjunto diofantino.

S é um conjunto diofantino

Agora é fácil completar a prova do Teorema 2.4 usando os Lemas 2,34 e 2.35.Primeiro encontre um polinômio Q satisfazendo **(1), (2), (3)** no Lema 2,35

Para isso , escreva: $P(y, k, x_1, \dots, x_n, y_1, \dots, y_m) = \sum_{r=1}^{N} t_r$, onde cada t_r tem a seguinte forma:

$$t_r = c_r y^a k^b x_1^{q_1} x_2^{q_2} \dots x_n^{q_n} y_1^{s_1} y_2^{s_2} \dots y_m^{s_m}$$

Para cada c_r positivo ou negativo.

Seja $u_r = \mid c_r \mid\ y^{a+b} x_1^{q_1} x_2^{q_2} \dots x_n^{q_n} u^{s_1+s_2+\cdots+s_m}$ e $Q(y, u, x_1, \dots, x_n) = u + y + \sum_{r=1}^{N} u_r$.

Lembrando que

$$u = \max\{y_i^{(k)} \mid\ 1 \leq i \leq m\ ; 1 \leq k \leq y\}.$$

Então **(1) , (2)** e **(3)** do Lema 2.35 é trivialmente satisfeito. Desse modo,

$$\forall k \in \mathbb{N}^* \text{ com } k \leq y,\ \exists\, y_1 \ldots, y_m\ \in \mathbb{N}^* \mid P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0$$

É equivalente a,

$$\begin{cases} \exists\, c, t, a_1, \ldots, a_m \in \mathbb{N}^* \mid\ 1 + ct = \prod_{k=1}^{y}(1 + kt)\,, \\ \qquad t = Q(y, u, x_1, \ldots, x_n)!\ , \\ 1 + ct \mid \prod_{j=1}^{u}(a_i - j)\,, \qquad 1 \leq i \leq m \\ P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0\ \ (mod\ 1 + ct). \end{cases}$$

Que por sua vez, é equivalente a

$$\begin{cases} \exists\, u, c, t, a_1, \ldots, a_m, e, f, g_1, \ldots, g_m, h_1, \ldots, h_n, l \in \mathbb{N}^*\ \mid \\ e = 1 + ct\ \ \wedge\ \ e = \prod_{k=1}^{y}(1 + kt)\ \wedge\ f = Q(y, u, x_1, \ldots, x_n) \\ t = f!\ \ \wedge\ \ g_i = a_i - u - 1, \qquad 1 \leq i \leq m \\ h_i = \prod_{j=1}^{u}(g_i + j)\ \ \wedge\ \ e \mid h_i \\ l = P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0\ \ (mod\ 1 + ct)\ \ \wedge\ e \mid l\,. \end{cases}$$

Note que ,

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

Como cada uma dessas expressões acima são diofantinas a combinação delas utilizando o operador "∧" e "∃" também será, portanto o conjunto

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

É diofantino.

■

Lembre que já provamos no teorema 2.3 que as funções $h(a, b, y) = \prod_{k=1}^{y}(a + bk)$,

$g(n) = n!$

e $f(n, k) = \binom{n}{k}$ são diofantinas.

3.4 Conceito de algoritmo e modelos de computabilidade

Um algoritmo é um método cuja execução consiste na aplicação, passo a passo , de certas regras especificas a priori. Estas regras devem determinar o resultado final completamente. As operações básicas da aritmética ; somar , multiplicar e dividir são procedimentos algorítmicos. Um algoritmo conhecido é o algoritmo de Euclides para determinar o máximo divisor comum de dois inteiros não negativos. Necessitamos definir as funções calculáveis, existem os seguintes modelos de computabilidade :

1) **Godel – Herbrabd - Kleene (1936) :** Funções recursivas gerais definidas por meio de uma equação de Cálculo.
2) **Church (1936) :** Funciones $\lambda -$ definidas.
3) **Godel - Kleene (1936) :** Funções $\mu -$recursivas e funções recursivas parciais.
4) **Turing (1936) :** Funções calculáveis definidas por máquinas finitas conhecidas como máquinas de Turing.
5) **Post (1943) :** Funções definidas por sistemas de deduções canônica.
6) **Markov (1951) :** Funções obtidas por certo algoritmo sobre um alfabeto finito.
7) **Shepherdson - Sturgis (1963) :** Máquinas ilimitadas de registro.

Todos os modelos anteriores de Computabilidade são equivalentes e determinam a classe das funções calculáveis denotada por $\mathfrak{C}$. Nesse trabalho usaremos o modelo de computabilidade 3.

A Classe de Funções recursivas surge ao tornar mais preciso o conceito intuitivo de uma função calculável. Algumas **Funções Iniciais** , que podem ser consideradas imediatamente calculáveis , são chamadas de recursivas , e certas **regras** (Recursão Primitiva , Composição e Minimização) são especificadas por meio das quais novas funções recursivas podem ser geradas a partir de funções que já sabemos ser recursivas. As regras são tais que , para cada nova função recursiva , é possível indicar de uma só vez um algoritmo para calcular os valores da função , se tais algoritmos estiverem disponíveis para as funções recursivas dadas.

Definição 2.3 : Uma função $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ é computável (ou calculável) se para um $x \in dom\,(f)$. Pudermos encontrar um algoritmo tal que o valor de $y = f(x)$.

Exemplo 2.5 Seja $f:\mathbb{N}^2 \longrightarrow \mathbb{N}$, $f(x,y) = mdc(x,y)$. Esta função pode ser calculada pelo método de Euclides.

Exemplo 2.6 Seja $f:\mathbb{N} \longrightarrow \mathbb{N}$, $f(x) = \begin{cases} 1, & x \text{ é } primo \\ 2, & x \text{ não é } primo \end{cases}$ Esta função pode ser calculada pelo Crivo de Eratóstenes.

3.5 Funções recursivas

Para definir função recursiva considere a função $S(i,u)$ definida no Teorema 1.2.

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

$$\begin{cases} c_1(x) = 1\,; & (\boldsymbol{Identidade}) \\ S(x) = x+1\,; & (\boldsymbol{Sucessor}) \\ U_i^n(x_1,\dots,x_n) = x_i\,,\ 1 \le i \le n\,; & (\boldsymbol{Proje}\text{ção}) \\ S(i,u). & (\boldsymbol{Teorema\ 1.2}) \end{cases}$$

Aplicando interativamente três operações básicas: Composição, Recursão Primitiva e Minimização definida abaixo podemos obter uma função h também recursiva.

Composição:

Define a função h que satisfaz a equação:

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

a partir das funções recursivas $g_1,\dots,g_m$ e $f(t_1,\dots,t_m)$ dadas.

Recursão Primitiva: Define a função $h(x_1,\dots,x_n,z)$ que satisfaz as equações:

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

a partir das funções f,g dadas. Quando $n=0$, f torna-se uma constante e h é obtida diretamente de g. Note que a sequência de fibonacci pode ser escrita como uma função recursiva.

Minimização: Define a função h que satisfaz a equação:

$$h(x_1,\dots,x_n) = \min_{y}[f(x_1,\dots,x_n,y) = g(x_1,\dots,x_n,y)],$$

A partir das funções f,g dadas e assumindo que f,g são tais que para cada $x_1,\dots,x_n$ existe pelo menos um y satisfazendo a equação

$$f(x_1,\dots,x_n,y) = g(x_1,\dots,x_n,y),$$

Ou seja, h está definida para toda n-upla $(x_1,\dots,x_n)$.

Abaixo temos uma lista de algumas funções recursivas.

Proposição 2.1: A função $h(x,y) = x + y$ é recursiva.

Demonstração.

Defina $g(u,v,w) = v + 1$ e $f(x) = x + 1$. Note que g e f são recursivas pois podem ser obtidas a partir das funções recursivas iniciais, $g(u,v,w) = S\big(U_2^3(u,v,w)\big) = S(v)$ e $f(x) = S(x) = x + 1$. Agora considere a função $h(x,y)$ definida por ,

$$\begin{cases} h(x,1) = f(x) \\ h(x,t+1) = g(t,h(x,t),x). \end{cases}$$

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

■

Proposição 2.2: A função $h(x,y) = xy$ é recursiva.

Demonstração.

Defina $f(x) = x$ e $g(u,v,w) = v + w$. Note que g e f são recursivas, pois $f(x) = U_1^1(x)$ e $g(u,v,w) = \boldsymbol{s}(U_2^3(u,v,w), U_3^3(u,v,w))$. Onde $\boldsymbol{s}$ é a função soma que já sabemos que é recursiva, veja que g é recursiva por composição.Agora, considere a função $h(x,t)$ definida por,

$$\begin{cases} h(x,1) = f(x) \\ h(x,t+1) = g(t,h(x,t),x). \end{cases}$$

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

■

Proposição 2.3: Para cada $k \in \mathbb{N}^*$, a função constante $c_k(x) = k$ é recursiva.

Demonstração.

Para $k = 1$ vale o resultado. Suponha que $c_k(x) = k$ é recursiva, então $c_{k+1}(x)$ é recursiva por composição pois,

$$c_{k+1}(x) = k + 1 = c_k(x) + c_1(x) = \boldsymbol{s}(c_k(x), c_1(x)).$$

■

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

$$2x^2y + 3xz^3 + 5 = c_2(x) \cdot x \cdot x \cdot y + c_3(x) \cdot x \cdot z \cdot z \cdot z + c_5(x).$$

Teorema 2.5 Uma função é recursiva se e só se é computável .

A demonstração desse resultado pode ser visto com detalhes na referência bibliográfica [**Computability Theory ,** veja as páginas 61 e 69].

Agora enunciaremos um dos resultados centrais deste trabalho:

Teorema 2.6 Uma função é Diofantina se, e somente se, é recursiva.

Demonstração. Seja f uma função diofantina , $y = f(x_1, \dots, x_n) \Leftrightarrow \exists t_1, \dots, t_m \in \mathbb{N}^* \mid P(x_1, \dots, x_n, y, t_1, \dots, t_m) = Q(x_1, \dots, x_n, y, t_1, \dots, t_m)$ onde P e Q são polinômios com coeficientes inteiros e positivos. Então pelo Teorema da Seqüência de Números, $\exists u \in \mathbb{N}^* \mid S(1,u) = y$ e $S(i+1,u) = t_i$, $1 \leq i \leq m$, Assim ,

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

Logo, o conjunto

$A = \{u \in \mathbb{N}^* \mid P(x_1, \dots, x_n, S(1,u), \dots, S(m+1,u)) = Q(x_1, \dots, x_n, S(1,u), \dots, S(m+1,u)\}$ é não vazio. Pelo princípio da Boa Ordem , existe $u_0 = minA$. Daí ,

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

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

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

Portanto ,

$$f(x_1, \dots, x_n) = S(1,u_0) = S(1, minA).$$

Assim , por composição , P e Q são recursivas já que são polinômios com coeficientes inteiros e positivos , por minimalidade , $minA$ é recursiva e , novamente por composição , f é recursiva.

Reciprocamente, como $c(x), S(x), U_i^n(x_1, \dots, x_n)$ e $S(i,u)$ são diofantinas ,basta mostrar que as funções diofantinas são fechadas para as operações de composição, recursão primitiva e minimização, já que no Teorema 1.2 mostramos que $S(i,u)$ é Diofantina e as funções recursivas iniciais são trivialmente Diofantinas. Faremos isto a seguir:

Composição:

Se $h(x_1, \dots, x_n) = f\big(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)\big)$, onde $f, g_1, \dots, g_m$ são Diofantinas então h também é , pois , $y = h(x_1, \dots, x_n) \Leftrightarrow \exists t_1, \dots, t_m \in \mathbb{N}^*$: $t_i = g_i(x_1, \dots, x_n)$, $1 \leq i \leq m$ e $y = f(t_1, \dots, t_m)$.

$$\begin{cases} t_1 = g_1(x_1, \dots, x_n) \\ \quad\quad \dots \\ \quad\quad \dots \\ t_m = g_m(x_1, \dots, x_n) \\ y = f(t_1, \dots, t_m) \end{cases}$$

Pelo Lema 1.1 podemos reduzir o sistema em uma única equação $E(x_1, .., x_n, y, t_1, .., t_m) = 0$.

Recursão primitiva:

Se

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

Onde f, g são Diofantinas, então h também é, pois, usando o Teorema da Sequência de Números para codificar os números $S(1,u) = h(x_1, \dots, x_n, 1)$, … , $S(z,u) = h(x_1, \dots, x_n, z)$ temos que ,

$$y = h(x_1, \dots, x_n, z) \Leftrightarrow \begin{cases} \exists u, v \in \mathbb{N}^* \mid [\ v = S(1,u) \text{ e } v = f(x_1, \dots, x_n)], \\ e\ [\ \forall t \in \mathbb{N}^*, 1 \leq t \leq z \text{ temos } t = z\ ] \text{ ou } t < z \text{ e nesse caso} \\ [\ \exists v' \in \mathbb{N}^* \mid v' = S(t+1,u)\ e\ v' = g(t, S(t,u), x_1, \dots, x_n))] \\ e\ [y = S(z,u)] \end{cases}$$

Do teorema 1.2 temos que $S(i,u)$ é diofantino alem disso os operadores $\wedge$ e $\vee$ geram conjuntos diofantinos , os quantificadores $\exists$ e $\forall$ também geram. Esse último quantificador gera conjuntos diofantinos por causa do Teorema 2.4, assim h é Diofantina.

Minimização:

Se

$h(x_1, \dots, x_n) = \min_{y}[\ f(x_1, \dots, x_n, y) = g(x_1, \dots, x_n, y)]$, onde f, g são Diofantinas, então h também é, pois,

$$y = h(x_1, \dots, x_n, z) \Leftrightarrow \begin{cases} \exists z \in \mathbb{N}^* \mid [\ z = f(x_1, \dots, x_n, y)\ e\ z = g(x_1, \dots, x_n, y)], \\ e\ [\ \forall t \in \mathbb{N}^*, 1 \leq t \leq y \text{ temos } t = y\ ] \text{ ou } t < y \text{ e nesse caso} \\ [\ \exists u, v \in \mathbb{N}^* \mid u = f(x_1, \dots, x_n, t)\ e\ v = g(x_1, \dots, x_n, t) \\ e\ [(u < v \text{ ou } v < u). \end{cases}$$

■

3.6 O conjunto diofantino universal

Seja S o conjunto de todos os polinômios a coeficientes inteiros e positivos. Fixado um alfabeto infinito de variáveis $x_0, x_1, x_2, \ldots$ e considerando o número 1, as operações de adição e multiplicação sucessivas e também as funções de emparelhamento descritas no teorema 1.1 , temos que a função $P: \mathbb{N}^* \to S$, $P_x = P_x(x_0, x_1, \ldots, x_n)$ definida por.

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

É sobrejetora, isto é, a função P gera todos os polinômios de S. Escrevendo $P_i = P_i(x_0, x_1, \ldots, x_n)$, onde n é grande o suficiente para que todas as variáveis que ocorram em P_i estejam incluídas (É claro que P_i geralmente não depende de todas as variáveis). Finalmente, seja

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

Observe que $P_{L(n)}$ e $P_{R(n)}$ não envolvem todas as variáveis $x_0, x_1, \ldots, x_n$, mas claramente não podem envolver qualquer outra (Lembre-se que $0 < L(n), R(n) \leq n$). Pela forma como a sequência P_i foi construída, vê-se que a sequência de conjuntos $D_1, D_2, D_3, \ldots$ inclui todos os conjuntos Diofantinos de números inteiros positivos.

Proposição 2.4. A família $D = \{D_1, D_2, D_3, \ldots\}$ contem todos os conjuntos diofantinos de números inteiros positivos.

Demonstração.

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

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

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 $x, y \in \mathbb{N}^* \mid P_x = f$ e $P_y = g$. Como $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$, existe $n \in \mathbb{N}^* \mid x = L(n)$ e $y = R(n)$. Logo, $D = f - g = P_x - P_y = P_{L(n)} - P_{R(n)}$ .Portanto , $A = D_n$

■

Teorema 2.6 (Teorema da Universalidade)

O conjunto $U = \{(n, x) \in (\mathbb{N}^*)^2 \mid x \in D_n\}$ é Diofantino.

Demonstração.

Basta mostrar que

$$x \in D_n \Leftrightarrow \begin{cases} \exists u \in \mathbb{N}^* \mid \ S(1,u) = 1 \ e \ S(2,u) = x \\ e \\ \forall i \in \{1, \dots, n\} \ temos \ S(3i,u) = S(L(i),u) + S(R(i),u) \\ e \\ S(3i+1,u) = S(L(i),u) \cdot S(R(i),u) \\ e \\ S(L(n),u) = S(R(n),u). \end{cases}$$

Seja $x \in D_n$ para x e n dados. Então , por definição $\exists t_1, \dots, t_n \in \mathbb{N}^*$ tais que:

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

Pelo Teorema da Sequência de Números, $\exists u \in \mathbb{N}^*$ tal que $S(j,u) = P_j(x, t_1, \dots, t_n)$ onde $1 \leq j \leq 3n + 2$.

Então em particular $S(1,u) = P_1(x, t_1, \dots, t_n) = P_1 = 1$ e $S(2,u) = P_2(x, t_1, \dots, t_n) = x_0 = x$, ou seja, $\boldsymbol{S(1,u) = 1}$ e $\boldsymbol{S(2,u) = x}$ para $i \in \{1, \dots, n\}$ temos que

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

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

Como $x \in D_n$, sabemos que

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

Ou seja,

$$\boldsymbol{S(L(n),u) = S(R(n),u)}.$$

Reciprocamente, seja o lado direito verdadeiro para x e n dados. Seja $t_{j'} = S(3j' + 2, u)$ para $1 \leq j' \leq n$. Então

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

Vejamos por indução que $S(j,u) = P_j(x, t_1, \dots, t_n)$ onde $1 \leq j \leq 3n + 2$. Para $j = 1$, temos que

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

Agora, suponha válido para valores até $j-1$, e vamos mostrar que vale para j.

Se $j = 3i-1$

Então, $S(3i-1,u) = S(3(i-1)+2,u) = t_{i-1} = P_{3i-1}(x,t_1,\dots,t_n)$. Lembre que $t_{j'} = S(3j'+2,u)$ e note que $1 \le i-1 \le n$.

Se $j = 3i$

Então , $S(3i,u) \overset{Hip}{=} S(L(i),u) + S(R(i),u) \overset{Ind}{=} P_{L(i)}(x,t_1,\dots,t_n) + P_{R(i)}(x,t_1,\dots,t_n) = P_{3i}(x,t_1,\dots,t_n)$.

Se $j = 3i-1$

Entã , $S(3i+1,u) \overset{Hip}{=} S(L(i),u)\cdot S(R(i),u) \overset{Ind}{=} P_{L(i)}(x,t_1,\dots,t_n).P_{R(i)}(x,t_1,\dots,t_n) = P_{3i+1}(x,t_1,\dots,t_n)$.

Portanto $S(j,u) = P_j(x,t_1,\dots,t_n)$ onde $1 \le j \le 3n+2$. Como $S(L(n),u) = S(R(n),u)$, segue que

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

Logo , $x \in D_n$

■

Uma vez que $D_1, D_2, D_3, \dots$ dão uma enumeração de todos os conjuntos Diofantinos de inteiros positivos, é fácil construir um conjunto diferente de todos eles e, portanto não Diofantino. Basta definir:

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

Teorema 2.7 O conjunto $V = \{n \in \mathbb{N}^* \mid n \notin D_n\}$ não é Diofantino.

Demonstração.

Esta é uma aplicação do método de diagonalização de Cantor. Suponha que V é Diofantino , então existe $k \in \mathbb{N}^* \mid V = D_k$, como $V = D_k$ temos , $k \in V \Leftrightarrow k \in D_k$ e da definição de V temos $k \in V \Leftrightarrow k \notin D_k$, absurdo.

$$\begin{cases} k \in V \Leftrightarrow k \in D_k \\ \qquad e \\ k \in V \Leftrightarrow k \notin D_k. \end{cases}$$

■

Teorema 2.8 A função $g(n,x)$ definida por:

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

não é recursiva.

Demonstração.

Se g fosse recursiva, então g seria diofantina, isto é,

$$y = g(n,x) \Leftrightarrow \exists y_1, \dots, y_m \in \mathbb{N}^* \mid P(n,x,y,y_1,\dots,y_m) = 0.$$

Mas disto segue que:

$$V = \{x \in \mathbb{N}^* \mid x \notin D_x\} = \{x \in \mathbb{N}^* \mid g(x,x) = 1\}$$
$$= \{x \in \mathbb{N}^* : \exists y_1, \dots, y_m \in \mathbb{N}^* \mid P(x,x,1,y_1,\dots,y_m) = 0\},$$

Logo, V é diofantina , absurdo.

■

Teorema 2.9 O Décimo problema de Hilbert é insolúvel nos inteiros positivos.

Demonstração.

Pelo Teorema da Universalidade , sabemos que o conjunto $U = \{(n,x) \in (\mathbb{N}^*)^2 \mid x \in D_n\}$ é Diofantino , isto é,

$$x \in D_n \Leftrightarrow \exists z_1, \dots, z_k\ \in \mathbb{N}^* \mid\ P(n,x,z_1,\dots,z_k) = 0.$$

Suponha por absurdo que o Décimo problema de Hilbert seja solúvel nos inteiros positivos,ou seja , suponha que exista 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

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

Tem solução, isto é, se $x \in D_n$ ou não. Desse modo o algoritmo calcula a função $g(n,x)$. Uma vez que as funções recursivas são apenas aquelas para as quais existe um algoritmo de computação, $g(n,x)$ seria recursiva, ou melhor , se existe um algoritmo para determinar $g(n,x)$, para cada n e cada x inteiros positivos , então g é recursiva, mas isto contraria o Teorema 2.8. Logo o Décimo Problema de Hilbert é insolúvel nos inteiros positivos.

■

Teorema 2.10 O Décimo problema de Hilbert é insolúvel nos naturais.

Demonstração.

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

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

Suponha por absurdo que o décimo problema de Hilbert é solúvel nos naturais. Então ,existe um algoritmo que testa se $\exists y_1, \dots, y_m \in \mathbb{N} \mid Q(y_1, \dots, y_m) = 0$. Escrevendo $x_i = y_i + 1$, onde $1 \leq i \leq m$, esse algoritmo testa se $\exists x_1, \dots, x_m \in \mathbb{N}^* \mid P(x_1, \dots, x_m) = 0$. Logo o décimo problema de Hilbert é solúvel nos inteiros positivos, absurdo.

■

Teorema 2.11 O Décimo problema de Hilbert é insolúvel

Demonstração.

Seja $P(x_1, \dots, x_m) = 0$ uma equação diofantina. Pela proposição 1.1 sabemos que o sistema

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

Pode ser simplificado na equação, $E(x_1, \dots, x_m, y_{1,1}, \dots, y_{m,4}) = 0$. Suponha por absurdo que o décimo problema de Hilbert seja solúvel, logo, existe um algoritmo que testa se a equação, $E(x_1, \dots, x_m, y_{1,1}, \dots, y_{m,4}) = 0$ possui solução inteira. Pelo Lema 1.2, isso equivale a dizer que esse algoritmo testa se, $P(x_1, \dots, x_m) = 0$ possui solução nos naturais. Portanto, o décimo problema de Hilbert é solúvel nos naturais, absurdo.

■

Note que este resultado não dá informações sobre a existência de soluções para qualquer equação Diofantina específica, limita-se a garantir que **não existe** um algoritmo **único** para testar todas as classes de equações Diofantinas. 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.

4 UMA APLICAÇÃO PARA O 10º PROBLEMA DE HILBERT

Uma implicação muito importante dessa solução negativa do décimo problema de HILBERT é o teorema de incompletude de GÖDEL demonstrado em 1931.

4.1 Teorema de incompletude de Godel

Teorema 3.1. Não existe um sistema axiomático consistente do qual se pode deduzir todas as verdades da aritmética.

Demonstração.

Suponhamos que existe um sistema Γ consistente que deduz todas as verdades da aritmética. A notação $\Gamma \vdash \psi$ indica que a fórmula da aritmética ψ se deduz de Γ. O conceito de dedução formal é um processo algorítmico, no sentido de que, dada uma sucessão de fórmulas, é possível deduzir se é ou não é uma dedução correta. É então possível fornecer um algoritmo que liste todas as deduções corretas. Agora, dada uma equação diofantina $P(x) = 0$, ela pode ser escrita na forma $P_1(\overline{x}) = P_2(\overline{x})$ onde ´´$P_1(\overline{x}) = P_2(\overline{x})$`` pertence a linguagem da aritmética. Consideremos a fórmula

$$\psi : \exists \overline{x}\, [P_1(\overline{x}) = P_2(\overline{x})].$$

Este fórmula deve ser verdadeira ou falsa. Se ψ é verdadeira , $\Gamma \vdash \psi$ por hipótese. Se ψ é falsa então $\neg\psi$ é verdadeira, assim $\Gamma \vdash \neg\psi$. Como Γ é consistente , Γ não pode deduzir a ψ e $\neg\psi$. O algoritmo a seguir resolveria o décimo problema de HILBERT.

Liste todas as deduções corretas e examine a última fórmula, pare o processo quando aparecer ψ ou $\neg\psi$. O processo termina pois alguma das duas fórmulas é dedutível , deve haver uma dedução que termina em ψ ou $\neg\psi$. Se é ψ a que aparece, a equação $P(x) = 0$ é solúvel. Se é $\neg\psi$, a equação não é solúvel . Assim temos encontrado um algoritmo que soluciona o décimo problema de HILBERT!! , isso contradiz o teorema 2.11. Por conseguinte não existe um tal sistema Γ.

Então se existe um sistema consistente que deduz Todas as verdades da aritmética ele conseguiria dizer se dada uma equação diofantina ela tem ou não tem solução nos inteiros , mas isso significaria que o Décimo problema de Hilbert é solúvel nos inteiros , portanto um absurdo já que sabemos que o décimo problema não é solúvel e portanto não existe tal sistema axiomático consistente.

5 CONCLUSÃO

É Importante perceber que a insolubilidade do 10º problema de Hilbert não dá informações sobre a existência de soluções para qualquer equação Diofantina específica, limita-se a garantir que não existe um algoritmo único para testar todas as classes de equações Diofantinas. 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.

REFERÊNCIA

CHURCH, A. An unsolvable problem of elementary number theory. American Journal of Mathematics, v. 58, p. 345-363, out. 1936.

COOK, S. Computability theory. [s.l.] : University of Toronto, 2008. Disponível em: http://www.cs.toronto.edu/~toni/Courses/438/Mynotes/page54. pdf Acesso em 19 jun 2018.

DAVIS, M. Arithmetical problems and recursively enumerable predicates. Journal of Symbolic Logic, v. 18, p. 33-41, jan. 1953.

DAVIS, M. Hilbert's tenth problem is unsolvable. The American Mathematical Monthly, v. 80, p. 233-269, nov. 1973.

PUTNAM, H. Reduction of Hilbert tenth problem. Journal of Symbolic Logic, v. 23, p. 183-187, fev. 1958.

GODEL, K. Uber formal unentscheidbare satze der principia mathematica und verwandter systeme. Monatshefte fur Mathematik und Physik, v. 38, p. 173-198, out. 1931.

MATIYASEVICH, Y. Hilbert's tenth problem. Cambridge, Mass. : Mit Press, 1993.

ROBINSON, J. Existential definability in arithmetic. Transactions of the American Mathematical Society, v. 72, p. 437-449, nov. 1952.

SANTOS, J. Introdução à teoria dos números. Rio de Janeiro : IMPA, 2010. Coleção Matemática Universitária.

TURING, A. On computable number with an application to the Entscheidungs problem. Proceedings of the London Mathematical Society, v. 42, p. 230-265, fev. 1936.