MARCELO FERREIRA

O Décimo Problema de Hilbert

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2010

MARCELO FERREIRA

O Décimo Problema de Hilbert

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica

Orientador(a): Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2010

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU – MG, Brasil

F383d Ferreira, Marcelo, 1981-
O décimo problema de Hilbert [manuscrito] / Marcelo Ferreira. - 2010.
74 f. il.

Orientador: Victor Gonzalo Lopez Neumann.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Geometria algébrica - Teses. 2. Riemann-Hilbert, Problemas de - Teses. I. Neumann, Victor Gonzalo Lopez. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 514.16

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO(A): Marcelo Ferreira

NÚMERO DE MATRÍCULA: 93805

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: O Décimo Problema de Hilbert

ORIENTADOR(A): Prof. Dr. Victor Gonzalo Lopez Neumann

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 27 de Agosto de 2010, às 10h00min, pela seguinte Banca Examinadora:

Prof. Dr. Hemar Teixeira Godinho
Universidade de Brasília - UnB

Prof. Dr. Cícero Fernandes de Carvalho
Universidade Federal de Uberlândia-MG

Prof. Dr. Victor Gonzalo Lopez Neumann
Universidade Federal de Uberlândia-MG
(orientador)

Uberlândia - MG, 27 de agosto de 2010.

Dedicatória

Dedico esta dissertação a minha família (o que inclui a família de minha esposa) e a minha amada esposa, sem os quais jamais teria concluído este trabalho.

Agradecimentos

Agradeço primeiramente a Deus, fonte de toda sabedoria, por ter me dado a oportunidade de conhecer um pouco mais desta bela ciência - A MATEMÁTICA. Agradeço a minha esposa, que com sua firmeza e amor, foi fundamental em todas as etapas deste trabalho. Agradeço a minha família que sempre acreditou em mim e isto fez toda a diferença. Finalizo, agradeçendo ao professor Victor Gonzalo Lopez Neumann, um orientador completo e ao professor Edson Agustini , um coordenador dotado de grande sensibilidade, aos dois, serei sempre grato.

FERREIRA, Marcelo *O Décimo Problema de Hilbert.* 2010. 44 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho apresentamos uma demonstração da insolubilidade do Décimo Problema de Hilbert, que investiga a existência de um método para determinar se dada uma equação Diofantina qualquer podemos determinar se esta tem ou não uma solução. Começamos desenvolvendo alguns tópicos de teoria de números, que serão úteis em vários momentos, nesta parte demonstramos apenas os resultados principais. Em um segundo momento, passamos ao estudo das equações Diofantinas bem como das funções Diofantinas, que permeiam nossos resultados. Em seguida, demonstramos uma série de lemas que servem de base para mostrarmos que a função exponencial é Diofantina. A partir daí, passamos a definição do importante conceito de função recursiva e então demonstramos que uma função ser recursiva é equivalente a ser Diofantina. Finalmente, demonstramos o Teorema da Universalidade que servirá de base para a demonstração da insolubilidade do Décimo Problema de Hilbert.

Palavras-chave: (Equações Diofantinas, Funções Recursivas, Função Exponencial).

FERREIRA, Marcelo *Hilbert's Tenth Problem.* 2010. 44 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work we present a proof that the Hilbert's Tenth Problem is unsolvable. This problem is to give a computing algorithm which will tell of a given polynomial Diophantine equation with integer coefficients whether or not it has a solution in integers. We start developing some topics of basic number theory, that will be useful at some time. In this part we prove only main results. After that, we study Diophantine equation as well as Diophantine functions. Then, we prove a serie of lemas that will be useful to proof that the exponential function is Diophantine. From there, we define the concept of recursive function and prove that a function is Diophantine if and only if it is recursive. Finally we prove the Universality Theorem. We use this last theorem to proof that the Hilbert's Problem is unsolvable.
Keywords: (Diophantine Equations, Recursive Functions, Exponential Function).

Sumário

Introdução

Em 1900, David Hilbert proferiu sua famosa conferência intitulada "Probleme Mathematische"antes do segundo congresso internacional de matemáticos.

Este documento contém 23 problemas, ou, mais precisamente, 23 grupos de problemas relacionados, que deixaram o século XIX para serem resolvidos no século XX .

O Décimo Problema é sobre equações Diofantinas. Estas equações receberam este nome, como uma homenagem a um dos maiores matemáticos da Grécia antiga, Diophantus de Alexandria, que formulou e resolveu muitas dessas equações. Informações completas sobre Diophantus de Alexandria podem ser obtidas em [8].

O enunciado do Décimo Problema de Hilbert é o seguinte: Dada uma equação Diofantina com coeficientes inteiros em um número qualquer de variáveis, é possível elaborar um processo que decida, através de um número finito de operações, se a equação tem soluções inteiras.

Na proposta do Décimo Problema de Hilbert estamos interessados apenas na existência das soluções e não na obtenção explícita destas soluções.

Hoje nós lemos as palavras "conceber um processo"no sentido de encontrar um algoritmo. Quando os problemas de Hilbert foram propostos, não havia nenhuma noção matematicamente rigorosa para o conceito de algoritmo.

A falta de tal noção não era em si um obstáculo para a solução do Décimo Problema de Hilbert, porque para qualquer algoritmo específico, ficou claro que uma possível generalização deste método poderia resolver o problema correspondente.

A primeira grande contribuição foi dada em 1931 por Kurt Godel em seu celebrado artigo [9], outros lógicos como Alonzo Church, ver [10] e Alan Turing, ver [11], [12] e [13], contribuíram na formulação rigorosa para a noção de computabilidade; isso possibilitou o estabelecimento do que seria um algoritmo insolúvel, isto é, a impossibilidade de existir um algoritmo com certas propriedades.

Logo em seguida, os primeiros exemplos de algoritmos insolúveis foram encontrados, primeiro na lógica matemática, em seguida em outros ramos da matemática.

A teoria da computabilidade produziu todas as ferramentas para enfrentar o Décimo Problema de Hilbert. Uma série de artigos nesta direção apareceram na década de 1950, graças aos esforços de Martin Davis, nos trabalhos [14] e [15], e deste juntamente com Hilary Putnam, ver [16].

Contribuições essenciais também foram dadas pela matemática Julia Robinson que inicialmente se concentrou na prova de que a função exponencial é Diofantina, e isto decorre de uma Hipótese que ficou conhecida na época como Hipótese de Julia Robinson, alguns de seus trabalhos estão destacados em [18], [19] e [20]. Detalhes sobre a história de Julia Robinson podem ser obtidos na referência [17].

Mas, a peça chave na solução 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 isto culminou com a negativa da solução do Décimo Problema de Hilbert em 1970, isto é, o algoritmo procurado não existe. A produção intelectual de Yuri é vasta, destacamos os seguintes trabalhos [1], [2] e [3]. Neste caso, como em muitos outros problemas cuja solução era aguardada, as técnicas desenvolvidas para a resolução do Décimo Problema de Hilbert são de valor independente por que tem outras aplicações.

Algumas aplicações são impressionantes, e de um modo geral, as outras aplicações que foram surgindo são talvez, ainda mais importantes do que a própria solução do problema.

O principal resultado técnico advindo da insolubilidade do Décimo Problema de Hilbert é a incrível implicação de que a classe dos conjuntos Diofantinos e idêntica à classe dos conjuntos recursivamente enumeráveis.

Outro corolário deste mesmo resultado que não usa uma terminologia especial é : É possível exibir explicitamente um polinômio a coeficientes inteiros tal que o conjunto dos valores assumidos por ele, quando suas variáveis são inteiras é exatamente o conjunto dos números primos. Este polinômio foi obtido por Jones, Sato, Wada e Wiens em 1976, tem grau 25 e 26 indeterminadas, e pode ser encontrado em [21].

Este trabalho se baseou no artigo [4] de Martin Davis, que habilmente sintetizou resultados obtidos por ele, Julia Robinson e Yuri Matiyasevich.

No Capítulo 1, compilamos alguns resultados de teoria de números que serão utilizados nas demonstrações, destaco que apesar da complexidade do problema, utilizamos basicamente, as noções de divisibilidade, a teoria de congruências e o princípio de indução finita. Dois resultados que merecem destaque são: O Teorema do Resto Chinês e o Teorema de Lagrande (todo número positivo e soma de quatro quadrados). Aqui utilizamos como referências [5], [6] e [7].

No Capítulo 2, definimos os importantes conceitos de equação Diofantina e de função Diofantina, dando também exemplos de ambos. Utilizando o Teorema de Lagrande mostramos que será suficiente investigarmos a existência do algoritmo procurado pelo Décimo Problema de Hilbert no conjunto dos números naturais e não no conjunto dos inteiros, como na proposta original do problema. Nesta parte as referências principais foram [1] e [4].

No Capítulo 3, temos como objetivo inicial, mostrar que a função exponencial é Diofantina, nesta tarefa, enunciamos e demonstramos 24 lemas que ulitizam a Equação de Pell. Em seguida, apresentamos um sistema com doze equações Diofantinas que servem de base para concluírmos que a função exponencial é Diofantina. Esta informação é importante pois a partir dela, mostramos que várias outras funções são Diofantinas. A partir daí, definimos o conceito de função recursiva, e então demonstramos um dos resultados centrais deste trabalho, que uma função é Diofantina se, e somente se, é recursiva. Em seguida, criamos uma enumeração para os polinômios com coeficientes inteiros positivos e utilizando esta enumeração, definimos a sequência de conjuntos que incluem todos os conjuntos Diofantinos de dimensão 1. Provamos então o Teorema da Universalidade, que será fundamental para demonstrarmos o resultado principal deste trabalho: O DÉCIMO PROBLEMA DE HILBERT É INSOLÚVEL.

Marcelo Ferreira
Uberlândia-MG, 27 de Agosto de 2010.

Capítulo 1

Tópicos de Teoria de Números

Nesta seção enunciaremos alguns resultados da teoria de números que serão necessários na compreensão de algumas demonstrações.

Definição 1.1 (Princípio da Boa Ordem) *Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.*

Definição 1.2 (Princípio de Indução Finita) *Seja B um subconjunto dos inteiros positivos. Se B possui as seguintes propriedades*

(i) $1 \in B$

(ii) $k+1 \in B$ *sempre que* $k \in B$

então B contém todos os inteiros positivos.

1.1 Divisibilidade

Definição 1.3 *Se a e b, são inteiros, dizemos que a divide b, denotando por $a \mid b$, se existir um inteiro c tal que $b = ac$.*

Se a não divide b escrevemos $a \nmid b$.

Proposição 1.1 *Se a, b, c são inteiros tais que $a \mid b$ e $b \mid c$ então $a \mid c$.*

Demonstração.
Por definição, existem inteiros k, l tais que $b = ak$ e $c = bl$. Logo

$$c = bl = (ak)l = a(kl)\,,$$

ou seja $a \mid c$. ■

Proposição 1.2 *Se a, b, c, m, n são inteiros tais que $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração.
Se $c \mid a$ e $c \mid b$ então existem k e l inteiros, tais que $a = kc$ e $b = lc$. Multiplicando estas equações respectivamente por m e n teremos, $ma = mkc$ e $nb = nlc$. Somando membro a membro obtemos $ma + nb = (mk + nl)c$, de onde concluímos que $c \mid (ma + nb)$. ■

Teorema 1.1 *A divisibilidade tem as seguintes propriedades:*

(i) $n \mid n$,

(ii) $d \mid n \Rightarrow ad \mid an$,

(iii) $ad \mid an \ e \ \ a \neq 0 \Rightarrow d \mid n$,

(iv) $1 \mid n$,

(v) $n \mid 0$,

(vi) $d \mid n \ e \ n \neq 0 \Rightarrow |d| \leq |n|$,

(vii) $d \mid n \ \ e \ \ n \mid d \Rightarrow |d| = |n|$,

(viii) $d \mid n \ \ e \ \ d \neq 0 \Rightarrow \ (\frac{n}{d}) \mid n$.

Demonstração.

(i) Como $n = n \cdot 1$, segue da definição que $n \mid n$.

(ii) Se $d \mid n$, então existe k inteiro tal que, $n = k \cdot d$, logo $a \cdot n = k \cdot a \cdot d$, o que implica que $ad \mid an$.

(iii) Como $ad \mid an$, existe k inteiro tal que, $an = k \cdot ad$, como $k \neq 0$, $n = k \cdot d$, o que implica que $d \mid n$.

(iv) Como $n = n \cdot 1$, segue da definição que $1 \mid n$.

(v) Como $0 = 0 \cdot n$, segue que $n \mid 0$.

(vi) Se $d \mid n$ e $n \neq 0$, existe $k \neq 0$ e inteiro tal que, $n = k \cdot d$, como $\mid n \mid = \mid k \mid \cdot \mid d \mid$ e $\mid k \mid \geq 1$, segue que $\mid d \mid \leq \mid n \mid$.

(vii) Se $d \mid n$ e $n \mid d$, existem k, l inteiros tais que $n = k \cdot d$ e $d = l \cdot n$, daí, $n = k \cdot l \cdot n$, logo $k = l = 1$ ou $k = l = -1$, o que implica que $\mid d \mid = \mid n \mid$.

(viii) Se $d \mid n$, existe k inteiro tal que $n = k \cdot d$, logo n/d é um número inteiro. Como $(n/d) \cdot d = n$, segue da definição que $(n/d) \mid n$.

■

Teorema 1.2 (Algoritmo da Divisão) *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r\,, \ \ com \quad 0 \leq r < b\,,$$

onde q é chamado de quociente e r de resto da divisão de a por b.

Demonstração.

Como $b > 0$, existe q satisfazendo:

$$qb \leq a < (q+1)b\,.$$

Isto implica $0 \leq a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de um outro par q_1 e r_1 verificando:

$$a = q_1 b + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b\,.$$

Disto temos $(qb + r) - (q_1 b + r_1) = 0$ o que implica que $b(q - q_1) = r_1 - r \Rightarrow b \mid (r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$, ou seja, $r_1 = r$. Logo, $q_1 b = qb \Rightarrow q_1 = q$, uma vez que $b \neq 0$. ■

1.2 Máximo Divisor Comum

Definição 1.4 *O máximo divisor comum de dois números a e b (com a ou b diferente de zero), denotado por (a, b), é o maior inteiro que divide a e b.*

Teorema 1.3 (Teorema de Bézout) *Seja d o máximo divisor comum de a e b então existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$.*

Demonstração.

Seja B o conjunto de todas as combinações lineares $\{na + mb\}$ onde m e n são inteiros. Este conjunto contém claramente números negativos, positivos e também o zero. Vamos escolher n_0 e m_0 tais que $c = n_0a + m_0b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c \mid a$ e $c \mid b$. Como as demonstrações são similares, mostraremos apenas que $c \mid a$. A prova é por contradição. Suponha que $c \nmid a$. Neste caso, pelo algoritmo da divisão, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in B$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ é o menor elemento positivo de B. Logo $c \mid a$ e de forma análoga se prova que $c \mid b$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e , portanto, $c = n_0a + m_0b = n_0k_1d + m_0k_2d = d(n_0k_1 + m_0k_2)$ o que implica que $d \mid c$. Pelo Teorema 1.1 (vi), temos $d \leq c$ (ambos positivos) e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = n_0a + m_0b$. ■

Proposição 1.3 *Para todo inteiro positivo t, $(ta, tb) = t(a, b)$*

Demonstração.

Pelo Teorema 1.3, (ta, tb) é o menor valor positivo de $mta + ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $ma + nb$. Logo $(ta, tb) = t \cdot (a, b)$. ■

Proposição 1.4 *Se $c > 0$ e a e b são divisíveis por c, então*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)\,.$$

Demonstração.

Como a e b são divisíveis por c, temos que a/c e b/c são inteiros. Basta, então, substituir na Proposição 1.3, "a"por a/c e "b"por b/c tomando $t = c$. ■

Corolário 1.1 *Se $(a, b) = d$, temos que* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Teorema 1.4 *Para a, b, x inteiros, temos $(a, b) = (a, b + ax)$.*

Demonstração.

Seja $d = (a, b)$ e $f = (a, b+ax)$. Pelo Teorema 1.3 existem inteiros n_0 e m_0 tais que $d = n_0a+m_0b$ e como esta expressão pode ser escrita como $d = a(n_0 - xm_0) + (b+ax)m_0$ concluímos pela Proposição 1.2 que o máximo divisor f de a e $b + ax$ é divisor de d. Tendo mostrado que $f \mid d$, mostraremos, a seguir, que $d \mid f$.

Pela Proposição 1.2, $d \mid (b + ax)$ e todo divisor comum de a e $b + ax$ é um divisor de f. Tendo assim provado que $d \mid f$ concluímos que $d = f$, uma vez que ambos são positivos. ■

Teorema 1.5 *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração.

Como $(a, b) = 1$, pelo Teorema 1.3, existem inteiros n_0, m_0 tais que

$$n_0a + m_0b = 1\,.$$

Multiplicando-se os dois lados desta igualdade por c temos: $n_0(ac) + m_0(bc) = c$.

Como $a \mid ac$ e por hipótese $a \mid bc$, então pela Proposição 1.2, $a \mid c$. ■

Teorema 1.6 *Sejam a, b inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração.
Pelo Teorema 1.4, da relação $a = qb + r$, obtemos $(a, b) = (b, a - qb) = (b, r)$. ■

Teorema 1.7 (O Algoritmo de Euclides) *Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2\,, && 0 < r_2 < r_1\,,\\
r_1 &= q_2 r_2 + r_3\,, && 0 < r_3 < r_2\,,\\
&\vdots && \vdots\\
r_j &= q_{j+1} r_{j+1} + r_{j+2}\,, && 0 < r_{j+2} < r_{j+1} \qquad (0 \leq j \leq n-1)\,,\\
&\vdots && \vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n\,, && 0 < r_n < r_{n-1}\,,\\
r_{n-1} &= q_n r_n\,, && \text{onde } r_{n+1} = 0\,.
\end{aligned}$$

Então o último resto não nulo r_n, satisfaz $(a, b) = r_n$.

Demonstração.
Comecemos aplicando o Teorema 1.2 para dividir $r_0 = a$ por $r_1 = b$ obtendo $r_0 = q_1 r_1 + r_2$, em seguida dividimos r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como, a cada passo o resto é sempre menor do que o anterior, e estamos lidando com números inteiros positivos, é claro que após um número finito de aplicações do Teorema 1.2, teremos resto nulo.

Temos, pois , a seguinte sequência de equações:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2\,, && 0 < r_2 < r_1\,,\\
r_1 &= q_2 r_2 + r_3\,, && 0 < r_3 < r_2\,,\\
&\vdots && \vdots\\
r_j &= q_{j+1} r_{j+1} + r_{j+2}\,, && 0 < r_{j+2} < r_{j+1} \qquad (0 \leq j \leq n-1)\,,\\
&\vdots && \vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n\,, && 0 < r_n < r_{n-1}\,,\\
r_{n-1} &= q_n r_n + 0\,.
\end{aligned}$$

A última destas equações nos diz, pelo Teorema 1.6, que o máximo divisor comum de r_n e r_{n-1} é r_n . A penúltima, que este número é igual a (r_{n-1}, r_{n-2}) e, prosseguindo desta maneira teremos, por repetidas aplicações do Teorema 1.6, a sequência:

$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_1, r_2) = (r_0, r_1) = (a, b)$.

Portanto o máximo divisor comum de a e b é o último resto não-nulo da sequência de divisões descrita. ■

1.3 Números Primos

Definição 1.5 *Um número inteiro n $(n > 1)$ possuindo somente dois divisores positivos n e 1 é chamado primo.*

Se $n > 1$ não é primo, dizemos que n é composto.

Proposição 1.5 *Se $p \mid ab$, p é primo, então $p \mid a$ ou $p \mid b$.*

Demonstração.
Se $p \nmid a$, então $(a, p) = 1$ o que implica, pelo Teorema 1.6, que $p \mid b$. ■

Teorema 1.8 (Teorema Fundamental da Aritmética) *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração.
Ver [5], Teorema 1.9 ■

1.4 Mínimo Múltiplo Comum

Definição 1.6 *O mínimo múltiplo comum de dois inteiros não nulos a e b é o menor inteiro positivo que é divisível por a e b. Vamos denotá-lo por $[a, b]$.*

Proposição 1.6 *Se $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$ e $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n}$, onde $p_1, p_2, \ldots, p_n$ são os primos que ocorrem nas fatorações de a e b, então*

$$[a, b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} p_3^{\max\{a_3,b_3\}} \cdots p_n^{\max\{a_n,b_n\}} .$$

Demonstração.
Ver [5], Proposição 1.5 ■

Proposição 1.7 *Para a e b inteiros não nulos temos $(a, b) \cdot [a, b] = a \cdot b$*

Demonstração.
Ver [5], Teorema 1.16 ■

Teorema 1.9 *Seja b um inteiro positivo maior que 1. Então todo inteiro positivo n pode ser representado de maneira única da seguinte forma:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 ,$$

onde $k \geq 0$, $a_k \neq 0$ e $0 \leq a_i < b$, para $i = 0, 1, 2, \ldots, k$.

Demonstração.
Ver [5], Teorema 1.17 ■

1.5 Congruências

Definição 1.7 *Se um inteiro m não nulo divide $a - b$ dizemos que a é congruente a b módulo m e escrevemos $a \equiv b \pmod{m}$. Se $a - b$ não é divisível por m dizemos que a não é congruente a b módulo m e neste caso escrevemos $a \not\equiv b \pmod{m}$*

Teorema 1.10 *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ então:*

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ka \equiv kb \pmod{m}$, $\forall\ k \in \mathbb{Z}$

(iv) $ac \equiv bd \pmod{m}$

(v) $a^k \equiv b^k \pmod{m}$, $\forall\ k \in \mathbb{Z}$

(vi) *Se $(k, m) = d$ então* $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$

Demonstração.
Ver [5], [7] ■

Definição 1.8 *Um conjunto A de números inteiros é um sistema completo de restos módulo n, se todo número inteiro for congruente módulo n com um, e somente um, elemento de A.*

1.6 Teorema do Resto Chinês

O nome deste teorema se deve ao fato de que na antiguidade os matemáticos chineses já o conheciam.

Em sua demonstração utilizaremos os dois resultados seguintes :

Teorema 1.11 *Sejam a, b inteiros e $m_1, \ldots, m_k$ inteiros positivos.*
Se $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, então $a \equiv b \pmod{[m_1, m_2, \ldots, m_r]}$, onde $[m_1, m_2, \ldots, m_r]$ é o mínimo múltiplo comum de $m_1, m_2, \ldots, m_r$.

Demonstração.

Ver [5], Teorema 2.6 ■

Teorema 1.12 *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \pmod{m}$ não possui nenhuma solução e se $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração.

Ver [5], Teorema 2.8 ■

Teorema 1.13 (Teorema do Resto Chinês) *Se $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ para $i \neq j$ e c_i inteiro, então o sistema*

$$\begin{aligned} a_1 x &\equiv c_1 \pmod{m_1}, \\ a_2 x &\equiv c_2 \pmod{m_2}, \\ a_3 x &\equiv c_3 \pmod{m_3}, \\ &\vdots \\ a_r x &\equiv c_r \pmod{m_r}, \end{aligned}$$

possui solução e a solução é única módulo m, onde $m = m_1 \cdot m_2 \cdots m_r$.

Demonstração.

Do fato de $(a_i, m_i) = 1$, o Teorema 1.12 nos diz que $a_i x \equiv c_i \pmod{m_i}$ possui uma única solução que denotamos por b_i. Se definirmos $y_i = m/m_i$, onde, $m = m_1 \cdot m_2 \cdots m_r$, teremos $(y_i, m_i) = 1$, uma vez que $(m_i, m_j) = 1$ para $i \neq j$. Novamente, o teorema anterior nos garante que cada uma das congruências $y_i x \equiv 1 \pmod{m_i}$ possui uma única solução que denotamos por $\overline{y_i}$. Logo,

$$y_i . \overline{y_i} \equiv 1 \pmod{m_i}, i = 1, 2, \ldots, r.$$

Afirmamos que o número x dado por

$$x = b_1 y_1 \overline{y_1} + b_2 y_2 \overline{y_2} + \cdots + b_r y_r \overline{y_r}\,.$$

é uma solução simultânea para nosso sistema de congruências. De fato

$$\begin{aligned} a_i x &= a_i b_1 y_1 \overline{y_1} + a_i b_2 y_2 \overline{y_2} + \cdots + a_i b_i y_i \overline{y_i} + \cdots + a_i b_r y_r \overline{y_r} \\ &\equiv a_i b_i y_i \overline{y_i} \pmod{m_i} \equiv a_i b_i \equiv c_i \pmod{m_i}, \end{aligned}$$

uma vez que y_i é divisível por m_i, para $i \neq j$, $y_i \overline{y_i} \equiv 1 \pmod{m_i}$ e b_i é solução de $a_i x \equiv c_i \pmod{m_i}$.

Mostraremos agora que esta solução é única módulo m.

Se $\overline{x}$ é uma outro solução para nosso sistema, então $a_i \overline{x} \equiv c_i \equiv a_i x \pmod{m_i}$ e sendo $(a_i, m_i) = 1$ obtemos $\overline{x} \equiv x \pmod{m_i}$.

Logo $m_i \mid (\overline{x} - x), i = 1, 2, \ldots, r$. Mas, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1 \cdot m_2 \cdots m_r\,.$$

Portanto pelo Teorema 1.11 , $m_1 \cdot m_2 \cdots m_r \mid (\overline{x} - x)$, ou seja, $\overline{x} \equiv x \pmod{m}$, o que conclui a demonstração. ■

1.7 Soma de Quatro Quadrados

A demonstração do Teorema de Lagrange utiliza algumas definições e resultados que enunciaremos a seguir:

Definição 1.9 (Resíduos Quadráticos) *Sejam a e m inteiros com $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m se a congruência $x^2 \equiv a \pmod{m}$ tiver solução. Caso $x^2 \equiv a \pmod{m}$ não tenha solução dizemos que a não é um resíduo quadrático módulo m ou que a é um resíduo não-quadrático.*

Teorema 1.14 *Seja p um primo ímpar. Dentre os números $1, 2, \ldots, p-1$, $(p-1)/2$ são resíduos quadráticos e $(p-1)/2$ não são.*

Demonstração.
Ver [5], Teorema 5.5 ■

Teorema 1.15 *Para p primo, a congruência $x^2 \equiv -1 \pmod{p}$ tem solução se, e somente se, $p = 2$ ou $p \equiv 1 \pmod{4}$.*

Demonstração.
Ver [5], Teorema 5.6 ■

Definição 1.10 *Para p um número primo ímpar e a um inteiro não-divisível por p, definimos o Símbolo de Legendre $\left(\frac{a}{p}\right)$ por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático de } p \\ -1, & \text{se } a \text{ não é um resíduo quadrático de } p \end{cases}$$

Teorema 1.16 *O Símbolo de Legendre é uma função completamente multiplicativa de a, isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

para a e b inteiros não-divisíveis por p.

Demonstração.
Ver [5], Teorema 5.8. ■

Teorema 1.17 *Para p um primo ímpar, temos*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod{4} \\ -1, & \text{se } p \equiv 1 \pmod{4} \end{cases}$$

Demonstração.
Ver [5], Teorema 5.9. ■

Teorema 1.18 *Para todo primo p existem inteiros, a, b, c não todos nulos, tais que a congruência seguinte se verifica $a^2 + b^2 + c^2 \equiv 0 \pmod{p}$.*

Demonstração.
Para o caso $p = 2$ tomamos $a = b = 1$ e $c = 0$. Se $p \equiv 1 \pmod{4}$ tomamos $b = 1, c = 0$ e a como uma solução de $x^2 \equiv -1 \pmod{p}$, a existência deste a é garantida pelo Teorema 1.15. Se $p \equiv 3 \pmod{4}$ tomamos $c = 1$ e mostramos a existência de solução para a congruência

$$a^2 + b^2 \equiv -1 \pmod{p}$$

sabemos pleo Teorema 1.14, que para um p primo ímpar, temos $(p-1)/2$ resíduos quadráticos e $(p-1)/2$ resíduos não-quadráticos dentre os números $1, 2, \ldots, p-1$. Seja, pois, d o menor resíduo positivo não-quadrático módulo p. Como 1 é resíduo quadrático, $d \geq 2$. Logo, pelos Teoremas 1.16 e 1.17

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = (-1)(-1) = 1\,.$$

Isso nos diz que $-d$ é resíduo quadrático módulo p, ou seja, a congruência $x^2 \equiv -d \pmod{p}$ possui solução. Seja b tal que $b^2 \equiv -d \pmod{p}$. Precisamos achar um a tal que $a^2 \equiv d-1 \pmod{p}$. Mas esta congruência claramente possui solução uma vez que $d \geq 2, d-1 \leq d$ e d é o menor resíduo não-quadrático positivo módulo p. ■

Utilizaremos também a identidade seguinte:

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(r^2+s^2+t^2+v^2) = \\ &= (ar+bs+ct+dv)^2 + (as-br-cv+dt)^2 + (at+bv-cr-ds)^2 + (av-bt+cs-dr)^2.\end{aligned} \tag{1.1}$$

Esta identidade mostra que o produto de números possuindo representação como soma de quatro quadrados pode também ser representado como soma de quatro quadrados. Feita esta observação, só resta mostrar que todo primo pode ser representado desta forma.

Teorema 1.19 (Lagrange) *Todo inteiro positivo possui representação como soma de quatro quadrados.*

Demonstração.

Mostremos que todo número primo possui esta representação.

Seja p um número primo ímpar (para o número primo 2 temos, $2 = 1^2 + 1^2 + 0^2 + 0^2$). Pelo Teorema 1.18, existem inteiros a, b e c tais que

$$a^2 + b^2 + c^2 \equiv 0 \pmod{p}\,. \tag{1.2}$$

Esta congruência pode ser reescrita como

$$a^2 + b^2 + c^2 + d^2 = Mp\,, \tag{1.3}$$

onde M é um inteiro e $d = 0$.

A equação (1.3) e o princípio da Boa Ordem nos garantem a existência de um menor inteiro m satisfazendo (1.3), isto é,

$$a^2 + b^2 + c^2 + d^2 = mp\,. \tag{1.4}$$

Como em (1.2) estamos trabalhando módulo p e a, b e c estão elevados ao quadrado podemos tomar a, b e c no intervalo $[0, \frac{p}{2})$ em (1.2) e (1.3). Logo,

$$mp = a^2 + b^2 + c^2 + d^2 < 4(\frac{p}{2})^2 = p^2$$

o que implica que $m < p$.

Para concluir a demonstração será suficiente provarmos que $m = 1$.

Vamos mostrar que a suposição $m > 1$, nos leva à obtenção de um inteiro $0 \leq m' < m$ o qual fornecerá uma representação para $m'p$ como soma de quatro quadrados, o que contradiz a forma como m foi escolhido.

Separamos em dois casos: m ímpar e m par. Seja $m > 1$ e m ímpar. Na equação

$$a^2 + b^2 + c^2 + d^2 = mp \tag{1.5}$$

podemos escolher a_1, b_1, c_1 e d_1 no intervalo $\left[0, \frac{m}{2}\right)$ satisfazendo às equações

$$\begin{aligned}a_1 &\equiv a \pmod{m}\,,\\ b_1 &\equiv b \pmod{m}\,,\\ c_1 &\equiv c \pmod{m}\,,\\ d_1 &\equiv d \pmod{m}\,.\end{aligned}$$

Desta forma temos

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv 0 \pmod{m},$$

o que nos garante a existência de $m' \geq 0$ tal que

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = mm'. \tag{1.6}$$

Como os inteiros a_1, b_1, c_1 e d_1 são todos menores que $\frac{m}{2}$ temos que $m' < m$. A suposição $m' = 0$ nos leva a uma contradição pois $m' = 0$ então $a_1 = b_1 = c_1 = d_1 = 0$ e portanto, $a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$ o que implica $m^2 \mid mp$. Como $m^2 \mid mp$ implica que $m \mid p$ temos uma contradição, pois $1 < m < p$.

Logo, $m' \neq 0$. De (1.5), (1.6) e (1.1) temos

$$\begin{aligned} mpm'm &= m^2pm' \\ &= (a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) \\ &= (aa_1 + bb_1 + cc_1 + dd_1)^2 + (ab_1 - ba_1 - cd_1 + dc_1)^2 + \\ &\quad (ac_1 + bd_1 - ca_1 - db_1)^2 + (ad_1 - bc_1 + cb_1 - da_1)^2. \end{aligned} \tag{1.7}$$

Como $a \equiv a_1, b \equiv b_1, c \equiv c_1$ e $d \equiv d_1 \pmod{m}$ e $a^2 \equiv aa_1, b^2 \equiv bb_1, c^2 \equiv cc_1$ e $d^2 \equiv dd_1 \pmod{m}$ vemos que as quatro expressões que estão elevadas ao quadrado do lado direito da última igualdade acima são múltiplos de m.

Portanto existem inteiros $\overline{a}, \overline{b}, \overline{c}$ e $\overline{d}$ tais que (1.7) pode ser reescrita como

$$m^2pm' = (\overline{a}m)^2 + (\overline{b}m) + (\overline{c}m)^2 + (\overline{d}m)^2$$

ou seja, $pm' = \overline{a}^2 + \overline{b}^2 + \overline{c}^2 + \overline{d}^2$ onde $m' < m$.

Nos resta mostrar que no caso m par também podemos encontrar $\overline{m} < m$ tal que $\overline{m}p$ é soma de quatro quadrados.

Para m par, os inteiros a, b, c e d devem ser todos pares, dois pares e dois ímpares ou todos ímpares.

Em qualquer um destes três casos podemos escolher a, b, c e d satisfazendo $a \equiv b \pmod{2}$ e $c \equiv d \pmod{2}$ o que nos permite escrever

$$p\frac{m}{2} = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2$$

Portanto, tomando $\overline{m} = \frac{m}{2} < m$, obtemos uma expressão para $\overline{m}p$ como soma de quatro quadrados. Pelas observações feitas anteriormente, concluímos que $m = 1$, ou seja, o primo p pode ser expresso como soma de quatro inteiros sendo cada um deles um quadrado. ■

Capítulo 2

Equações Diofantinas

O objetivo principal deste capítulo é introduzir dois conceitos, o de conjunto Diofantino e o de função Diofantina, pois estes são necessários a compreensão do Décimo Problema de Hilbert. Em seguida, estabeleceremos algumas propriedades e daremos alguns exemplos que elucidarão estes conceitos.

2.1 Equações Diofantinas

Uma equação Diofantina é uma equação da forma:

$$D(x_1, \ldots, x_m) = 0\,, \tag{2.1}$$

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

$$D_L(x_1, \ldots, x_m) = D_R(x_1, \ldots, x_m)\,, \tag{2.2}$$

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

2.2 Sistema de Equações Diofantinas

Lema 2.1 *Um sistema constituido de k equações Diofantinas*

$$\begin{aligned} D_1(x_1, \ldots, x_m) &= 0 \\ &\vdots \\ D_k(x_1, \ldots, x_m) &= 0 \end{aligned} \tag{2.3}$$

tem como solução os inteiros $x_1, \ldots, x_m$ se, e somente se, a equação Diofantina

$$D_1^2(x_1, \ldots, x_m) + \cdots + D_k^2(x_1, \ldots, x_m) = 0 \tag{2.4}$$

tem a mesma solução.

Demonstração.

Primeiramente, suponha que o sistema é satisfeito, ou seja, $D_i^2(x_1, \ldots, x_m) = 0$ para $1 \leq i \leq k$, e então é evidente que:

$$D_1^2(x_1, \ldots, x_m) + \ldots + \ D_k^2(x_1, \ldots, x_m) = 0\,.$$

Reciprocamente, se $\sum_{i=1}^{k} D_i^2(x_1, \ldots, x_m) = 0$, como $D_i^2(x_1, \ldots, x_m) \geq 0$ para $1 \leq i \leq k$, segue que $D_i(x_1, \ldots, x_m) = 0$ para $1 \leq i \leq k$. ■

Com este resultado reduzimos um sistema de equações Diofantinas a uma única equação Diofantina.

A transformação inversa também é possível, isto é, transformar a equação:

$$D(x_1, \ldots, x_m) = 0 \tag{2.5}$$

em um sistema de equações Diofantinas

$$\begin{aligned} D_1(x_1, \ldots, x_m, y_1, \ldots, y_m) &= 0 \\ &\vdots \\ D_k(x_1, \ldots, x_m, y_1, \ldots, y_m) &= 0 \end{aligned} \tag{2.6}$$

onde $y_1, \ldots, y_m$ são novas variáveis no sistema.

Uma possível razão para transformar a equação (2.5) no sistema (2.6) pode ser a obtenção de um sistema constituido de equações de grau menor.

É fácil ver que qualquer equação Diofantina pode ser transformada num sistema de equações constituído de equações de duas formas:

$$\alpha = \beta + \gamma \tag{2.7}$$

$$\alpha = \beta\gamma \tag{2.8}$$

onde α, β, γ são números particulares ou dependem das variáveis $x_1, \ldots, x_m, y_1, \ldots, y_m$.

Exemplo: Considere a seguinte equação Diofantina

$$4x^3y - 2x^2z^3 - 3y^2x + 5z = 0 \tag{2.9}$$

Primeiro vamos transpor os termos negativos obtendo a equação

$$4x^3y + 5z = 2x^2z^3 + \ 3y^2 \tag{2.10}$$

A seguir introduziremos 14 novas variáveis e obtemos o sistema equivalente:

$$\begin{array}{llll} p_1 = 4x, & p_2 = p_1x, & p_3 = p_2x, & p_4 = p_3y; \\ q_1 = 5z; & & & \\ r_1 = 2x, & r_2 = r_1x, & r_3 = r_2z, \quad r_4 = r_3z, & r_5 = r_4z; \\ s_1 = 3y, & s_2 = s_1y, & s_3 = s_2x; & \\ t_1 = p_4 + q_1, & u_1 = r_5 + s_3, & t_1 = u_1. & \end{array} \tag{2.11}$$

onde a variável t_1 corresponde ao lado esquerdo da equação inicial e u_1 ao lado direito da equação inicial.

Finalmente, utilizando o Lema 2.1, obtemos uma equação de grau 4 independentemente do grau da equação inicial.

Então para resolver o 10^o Problema de Hilbert será suficiente decidir se uma equação de grau 4 tem ou não solução.

2.3 Soluções nos Números Naturais

Em seu 10^o problema, Hilbert falou sobre as soluções nos inteiros.

Algumas vezes uma solução inteira é evidente. Por exemplo, a equação

$$(x+1)^3 + (y+1)^3 = (z+1)^3 \tag{2.12}$$

tem infinitas soluções da forma $x = z$ e $y = -1$.

Por outro lado, a obtenção de soluções não-negativas x, y e z para a equação (2.12) não é trivial.

Desse modo, para uma equação Diofantina particular, o problema de decidir 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 2.2 *A equação Diofantina $D(x_1, \ldots, x_m) = 0$ tem uma solução em inteiros não-negativos se, e somente se, o sistema*

$$\begin{aligned} &D(x_1, \ldots, x_m) = 0 \\ &x_1 = y_{1,1}^2 + y_{1,2}^2 + y_{1,3}^2 + y_{1,4}^2 \\ &\qquad\vdots \\ &x_m = y_{m,1}^2 + y_{m,2}^2 + y_{m,3}^2 + y_{m,4}^2 \end{aligned} \tag{2.13}$$

tem uma solução nos inteiros.

Demonstração.

Considere $(x_1, \ldots, x_m)$ uma solução em inteiros não-negativos da equação $D(x_1, \ldots, x_m) = 0$. Pelo Teorema 1.15, podemos expressar cada x_j $(1 \leq j \leq m)$ como soma de quatro quadrados, dando uma solução ao sistema (2.13).

Reciprocamente, qualquer solução do sistema (2.13) em números inteiros inclui a solução $(x_1, \ldots, x_m)$ em inteiros não-negativos da equação $D(x_1, \ldots, x_m) = 0$. ■

Da seção 2.2, o sistema (2.13) pode ser simplificado na equação :

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

que tem solução inteira se e somente se a equação original tem solução inteira não-negativa.

Desse modo, nós mostramos 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.

Chamaremos os inteiros não-negativos de números naturais, mas não consideraremos o 0 (zero) como número natural, desta forma, os números considerados são números naturais diferentes de zero, a menos que seja especificado o contrário.

2.4 Família de Equações Diofantinas

Uma família de equações Diofantinas é uma relação da forma:

$$D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{2.14}$$

onde D é um polinômio com coeficientes inteiros com respeito a todas as variáveis $a_1, \ldots, a_n, x_1, \ldots, x_m$ sendo $a_1, \ldots, a_n$ os parâmetros e $x_1, \ldots, x_m$ as incógnitas.

Uma família de equações Diofantinas não é um sistema infinito de equações por que as incógnitas não precisam satistazer todas as equações simultaneamente, como deve acontecer no sistema.

Famílias de equações Diofantinas são também chamadas de equações paramétricas. Para equações paramétricas precisamos distinguir o grau da equação com respeito a suas variáveis.

Para diferentes valores de parâmetros podemos obter equações que tem solução, bem como equações que não tem.

2.5 Conjuntos Diofantinos

Uma equação paramétrica Diofantina como em (2.14), define o conjunto $\mathbb{M}$ formado de n-uplas de valores de parâmetros $a_1, \ldots, a_n$ para os quais existem incógnitas $x_1, \ldots, x_m$ satisfazendo (2.14), isto é:

$$\langle a_1, \ldots, a_n \rangle \in \mathbb{M} \;\Leftrightarrow \exists\, x_1, \ldots, x_m \; [D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0]\,. \tag{2.15}$$

O número n é chamado de dimensão $\mathbb{M}$ e a equivalência (2.15) é chamada de representação Diofantina de $\mathbb{M}$.

Conjuntos que têm representação Diofantina são chamados conjuntos Diofantinos.

Todo conjunto Diofantino tem várias representações Diofantinas.

Neste trabalho o problema usual de equações Diofantinas será abordado de uma forma diferente.

Em vez de dar uma equação e procurar uma solução, começaremos com um conjunto e procuraremos a equação Diofantina correspondente.

2.6 Propriedades dos Conjuntos Diofantinos

A seguir mostraremos duas importantes propriedades dos conjuntos Diofantinos.

1 - A união de dois conjuntos Diofantinos de mesma dimensão é também Diofantino.

De fato, se

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

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

são representações Diofantinas de dois conjunto, então a equação

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

é uma representação Diofantina de sua união.

2- A interseção de dois conjuntos de mesma dimensão é também um conjunto Diofantino, para isto defina a equação:

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

2.7 Exemplos de Conjuntos Diofantinos

1. Os números que não são potências de 2:
$$x \in S \ \Leftrightarrow \ (\exists\ y, z)\ [x = y(2z + 1)].$$
2. Os números compostos:
$$x \in S \ \Leftrightarrow \ (\exists\ y, z)\ [x = (y + 1)(z + 1)].$$
3. A relação de ordem dos números inteiros positivos, isto é, o conjunto $\{\langle x, y\rangle \ | \ x < y\}$:
$$x \ < y \Leftrightarrow \ (\exists\ z)\ [x + z = y].$$
e o conjunto $\{\langle x, y\rangle \ | \ x \leq y\}$:
$$x \leq y \Leftrightarrow \ (\exists\ y, z)\ [x + z - 1 = y].$$
4. A relação de divisibilidade, considerando o conjunto $\{\langle x, y\rangle \ | \ x \mid y\}$:
$$x \mid y \Leftrightarrow \ (\exists\ z)\ [xz = y].$$

Os exemplos 1 e 2 sugerem que outros conjuntos podem ser considerados, como por exemplo: o conjunto dos números que são potências de 2 e o conjunto dos números primos. Veremos que estes conjuntos realmente são Diofantinos, mas isto não é trivial. Consideremos ainda o seguinte exemplo:

5. O conjunto W formado pelas ternas $\langle x, y, z\rangle$ para os quais $x \mid y$ e $x < z$:
$$x \mid y \Leftrightarrow (\exists\ u)\ [y = xu] \ \text{ e } \ x < z \Leftrightarrow \ (\exists\ v)\ [z = x + v],$$
ou equivalentemente:
$$\langle x, y, z\rangle \in W \Leftrightarrow (\exists\ u, v)[(y - xu)^2 + (z - x - v)^2 = 0]$$

2.8 Terminologia Lógica

Muitas vezes, é mais fácil usar, em vez da linguagem dos conjuntos, uma linguagem essencialmente equivalente, de propriedades e relações.

Por exemplo, ao invés de dizer que o conjunto de números pares é Diofantino, pode-se dizer que a propriedade de um número ser par é Diofantina.

Mais formalmente, nós dizemos que uma propriedade P dos números naturais é uma propriedade Diofantina se o conjunto dos números tendo esta propriedade é Diofantino.

O que pode se representado por uma equivalência da seguinte forma:

$$P(a) \Leftrightarrow (\exists\ x_1, \ldots, x_m)\ [D(a, x_1, \ldots, x_m) = 0]$$

chamada de representação Diofantina da propriedade P. Onde $P(a)$ indica que a satisfaz a propriedade P.

A equivalência da forma:

$$R(a_1, \ldots a_n) \Leftrightarrow (\exists\ x_1, \ldots, x_m)\ [D(a_1, \ldots a_n, x_1, \ldots, x_m) = 0]$$

é chamada de representação Diofantina da relação R. Onde $R(a_1, \ldots a_n)$ indica que a n-upla $(a_1, \ldots, a_n)$ é um elemento da relação $R \subseteq \mathbb{N}^n$, onde $\mathbb{N}$ é o conjunto de números naturais.

Ao invés de união de conjuntos, nesta terminologia, utilizamos o conectivo lógico *ou*. Em outras palavras, se R_1 e R_2 são relações Diofantinas (ou propriedades) então a relação (ou propriedade) R constituída pelas n-uplas $(a_1, \ldots, a_n)$ satisfazendo

$$R(a_1, \ldots a_n) \Leftrightarrow R_1(a_1, \ldots a_n) \vee R_2(a_1, \ldots a_n)$$

também é Diofantina.

Similarmente, para a interseção de conjuntos, temos nesta linguagem o conectivo lógico e. Assim, a equivalência da forma

$$R(a_1, \ldots a_n) \Leftrightarrow R_1(a_1, \ldots a_n) \wedge R_2(a_1, \ldots a_n)$$

pode ser considerada uma generalização da representação da relação Diofantina R desde que mostremos que as relações R_1 e R_2 são Diofantinas.

Funções Diofantinas

O termo função indicará funções de $\mathbb{N}^r$ em $\mathbb{N}$.

Uma função é chamada de função Diofantina se seu gráfico é um conjunto Diofantino.

Correspondentemente, a representação Diofantina de uma função F é uma equivalência da forma

$$a = F(b_1, \ldots b_n) \ \Leftrightarrow (\exists\ x_1, \ldots, x_m)\ [D(a, b_1, \ldots b_n, x_1, \ldots, x_m) = 0] \tag{2.16}$$

onde D é um polinômio com coeficientes inteiros.

Podemos tratar também equações com a seguinte forma:

$$P(t_1, \ldots, t_k) = 0 \tag{2.17}$$

onde P é um polinômio com coeficientes inteiros e $t_1, \ldots, t_k$ são termos Diofantinos, isto é, expressões construídas a partir de números naturais particulares, variáveis, os símbolos de "+", "-" , ".", e os símbolos para funções Diofantinas.

Como quando passamos da equação (2.9) para (2.11), a equação (2.17) pode ser transformada em um sistema equivalente consistindo em equações da forma (2.7) e (2.8) e da forma

$$\alpha = F(\beta_1, \ldots, \beta_n) \tag{2.18}$$

onde F é uma função Diofantina e α e $\beta_1, \ldots, \beta_n$ são variáveis ou números naturais particulares.

Além disso, podemos substituir cada equação da forma (2.18) por uma equação da forma (2.16) com a substituído por α e $b_1, \ldots b_n$ substituído por $\beta_1, \ldots, \beta_n$ e também $x_1, \ldots, x_m$ substituídos por novas variáveis que ainda não tinham sido utilizadas.

O sistema resultante pode ser reduzido a uma única equação equivalente da forma (2.17)

Exemplos de Funções Diofantinas

Uma importante função Diofantina esta associada com os números triangulares, que são os números da forma:

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

Esta função é crescente e para cada inteiro positivo z, existe um único $n \geq 0$, tal que

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

Assim, cada z, é representado de forma única da seguinte forma:

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

ou de forma equivalente

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

Se escrevermos $x = L(z),\ y = R(z)$, temos a seguinte função $P(x, y) = T(x + y - 2) + y$. Note que $L(z), R(z)$ e $P(x, y)$ são funções Diofantinas uma vez que:

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

$$x = L(z) \Leftrightarrow (\exists y)\ [2z = (x + y - 2)(x + y - 1) + 2y]$$

$$y = R(z) \Leftrightarrow (\exists x)\ [2z = (x + y - 2)(x + y - 1) + 2y]$$

A função $P(x, y)$ estabelece uma bijeção entre o 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 $(L(z), R(z))$. Note que $L(z) \leq z$ e $R(z) \leq z$.

O teorema a seguir é uma coletânea dos resultados vistos acima.

Teorema 2.1 (Teorema das Funções de Emparelhamento) *Existem funções Diofantinas $P(x, y)$, $L(z)$, $R(z)$ tais que:*

1 - Para todo x, y, $L(P(x, y)) = x$, $R(P(x, y)) = y$, e

2 - Para todo z, $P(L(z), R(z)) = z$, $L(z) \leq z$, $R(z) \leq z$.

Outra função Diofantina que nos será muito útil esta relacionada ao Teorema do Resto Chinês. Defina a função $S(i, u)$ da seguinte forma:

$$S(i, u) = w,$$

onde w é o único inteiro positivo para o qual:

$$w \equiv L(u) \pmod{1 + i \cdot R(u)} \quad \text{e} \quad w \leq 1 + iR(u)\,.$$

Aqui, w é resto da divisão euclidiana de $L(u)$ por $1 + iR(u)$.

Teorema 2.2 (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 $a_1, \ldots, a_n$, existe um número u tal que $S(i, u) = a_i$ para $1 \leq i \leq n$.

Demonstração.

Primeiro vamos mostrar que $S(i,u)$ definida acima é uma função Diofantina.

Temos que $w = S(i,u)$ se e somente se o seguinte sistema de equações tem solução:

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

Isto ocorre pois pela discussão conduzida no teorema das funções de emparelhamento, a primeira função é equivalente a $x = L(u)$ e $y = R(u)$.

Então somando os quadrados das três equações prova-se que $S(i,u)$ é Diofantina.

Como $S(i,u) \leq L(u)$ e $L(u) \leq u$ segue que $S(i,u) \leq u$. Finalmente, sejam $a_1, \ldots, a_n$ uma sequência de números. Escolha y 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, se $d \mid 1+iy$ e $d \mid 1+jy$, $i<j$, então $d \mid [j(1+iy) - i(1+jy)]$, isto é, $d \mid j-i$, de modo que $d \leq n$, mas isto é impossível, exceto se $d = 1$, pois $d \mid y$.

Sendo assim, podemos aplicar o Teorema do Resto Chinês para obtermos um número x tal que:

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

Sendo $u = P(x,y)$, tal que $x = L(u)$ e $y = R(u)$.Então para $i = 1, 2, \ldots, n$ teremos:

$a_i \equiv L(u) \pmod{1+iR(u)}$ e $a_i < y = R(u) < 1+iR(u)$. Mas por definição $a_i = S(i,u)$. ■

Uma impressionante caracterização dos conjuntos Diofantinos de inteiros positivos é dada por:

Teorema 2.3 *Um conjunto S de inteiros positivo é Diofantino se e somente se existe um polinômio P tal que S é precisamente o conjunto dos inteiros positivos na imagem da função definida por P.*

Demonstração.

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

$$x \in S \Leftrightarrow (\exists\, x_1, \ldots, x_m)[Q(x, x_1, \ldots, x_m) = 0].$$

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

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

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

$$x \in S \Leftrightarrow (\exists\, x_1, \ldots, x_m)\ [P(x_1, \ldots, x_m) = x]\,.$$

Defina $R(x, x_1, \ldots, x_m) = x - P(x_1, \ldots, x_m)$. Então:

$$x \in S \Leftrightarrow (\exists\, x_1, \ldots, x_m)\ [R(x, x_1, \ldots, x_m) = 0]\,,$$

logo o conjunto S é Diofantino. ■

Capítulo 3

O Décimo Problema de Hilbert é Insolúvel

3.1 A Função Exponencial é Diofantina

O objetivo desta seção é mostrar que a função exponencial $h(n,k) = n^k$ é Diofantina. Isto é necessário pois esta função servirá de base para mostrarmos que outras funções importantes também são Diofantinas.

Para isto 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.

A Equação de Pell é dada por:

$$x^2 - dy^2 = 1,\ x, y \in \mathbb{Z},$$

onde tomaremos $d = a^2 - 1$, $a > 1$.

São soluções triviais desta equação:

$$x = 1 \text{ e } y = 0,$$

$$x = a \text{ e } y = 1.$$

Mais informações sobre a Equação de Pell podem ser obtidas em [6].

Lema 3.1 *Não existem inteiros x, y, que satisfaçam a Equação de Pell para os quais*

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

Demonstração.

Sejam x, y satisfazendo a inequação $1 < x + y\sqrt{d} < a + \sqrt{d}$ e também a Equação de Pell. Logo,

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

esta igualdade e a inequação implicam que $1 > x - y\sqrt{d} > a - \sqrt{d}$, o que é equivalente a:

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

Adicionando as duas inequações temos que: $0 < 2y\sqrt{d} < 2\sqrt{d}$, ou seja, $0 < y < 1$, o que é uma contradição. ■

Lema 3.2 *Sejam x, y e x', y' inteiros, que satistaçam a Equação de Pell. Tomando*

$$x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d})\,.$$

Então x'' e y'' satisfazem a Equação de Pell.

Demonstração.
Observe que

$$x'' - y''\sqrt{d} = (x - y\sqrt{d})(x' - y'\sqrt{d})\,.$$

Então:

$$\begin{aligned}(x'')^2 - d(y'')^2 &= (x'' + y''\sqrt{d})(x'' - y''\sqrt{d}) \\ &= [(x + y\sqrt{d})(x' + y'\sqrt{d})][(x - y\sqrt{d})(x' - y'\sqrt{d})] \\ &= (x^2 - dy^2)((x')^2 - d(y')^2) = 1\,.\end{aligned}$$

■

Definição 3.1 *$x_n(a)$ e $y_n(a)$ para $n \geq 0$, $a > 1$, são definidas por $x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$.*

Quando o contexto permitir a dependência em relação a a não será explicitada e escreveremos apenas x_n e y_n.

Lema 3.3 *x_n e y_n satisfazem a Equação de Pell*

Demonstração.
Utilizaremos indução.
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 $y_1(a) = 1$, que solução trivial da Equação de Pell.
Suponha que o lema seja verdadeiro para $n - 1$. Logo,

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

satisfazem a Equação de Pell, utilizando o Lema 3.2 e a hipótese de indução. ■

Lema 3.4 *Sejam x, y soluções não negativas da Equação de Pell.*
Então para algum n, $x = x_n$ e $y = y_n$.

Demonstração.
Inicialmente note que $x + y\sqrt{d} \geq 1$. Por outro lado, $(a + \sqrt{d})^n$ tende ao infinito. Portanto existe um $n \geq 0$, tal que

$$(a + \sqrt{d})^n \leq x + y\sqrt{d} < (a + \sqrt{d})^{n+1}$$

Se ocorre a igualdade o resultado esta provado, caso contrário:

$$x_n + y_n\sqrt{d} < x + y\sqrt{d} < (x_n + y_n\sqrt{d})(a + \sqrt{d})$$

Como $(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = 1$ (pois x_n e y_n satisfazem a Equação de Pell), então o número $x_n - y_n\sqrt{d} > 0$ (caso contrário, $x_n + y_n\sqrt{d} < 0$, uma contradição). Então:

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

Logo,

$$1 < (x_n - y_n\sqrt{d})(x + y\sqrt{d}) < a + \sqrt{d}\,.$$

Mas isto contradiz os Lema 3.1 e 3.2. ■

Lema 3.5 *$x_{m\pm n} = x_m x_n \pm d y_n y_m$ e $y_{m\pm n} = x_n y_m \pm x_m y_n$.*

Demonstração.

$$\begin{aligned} x_{m+n} + y_{m+n}\sqrt{d} &= (a+\sqrt{d})^{m+n} \\ &= (x_m + y_m\sqrt{d})(x_n + y_n\sqrt{d} \\ &= (x_m x_n + d y_n y_m) + (x_n y_m + x_m y_n)\sqrt{d}\,. \end{aligned}$$

Portanto,

$$\begin{aligned} x_{m+n} &= x_m x_n + d y_n y_m \\ &\text{e} \\ y_{m+n} &= x_n y_m + x_m y_n\,. \end{aligned}$$

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

$$\begin{aligned} x_{m-n} + y_{m-n}\sqrt{d} &= (x_m + y_m\sqrt{d})(x_n - y_n\sqrt{d}) \\ &= (x_m x_n - d y_n y_m) + (x_n y_m - x_m y_n)\sqrt{d}\,. \end{aligned}$$

Portanto,

$$\begin{aligned} x_{m-n} &= x_m x_n - d y_n y_m \\ &\text{e} \\ y_{m-n} &= x_n y_m - x_m y_n\,. \end{aligned}$$

■

Lema 3.6 *$y_{m\pm1} = a y_m \pm x_m$ e $x_{m\pm1} = a x_m \pm d y_m$.*

Demonstração.
Tome $n = 1$ no Lema 3.5. ■

Lema 3.7 *$(x_n, y_n) = 1$.*

Demonstração.
Se $d \mid x_n$ e $d \mid y_n$, então $d \mid x_n^2 - d y_n^2 = 1$. ■

Lema 3.8 *$y_n \mid y_{nk}$.*

Demonstração.
Vamos utilizar indução e o Lema 3.5. O lema é obviamente verdadeiro para $k = 1$.
Suponha que seja verdadeiro para $k = m$, ou seja, $y_n \mid y_{nm}$.
Do Lema 3.5 temos que, $y_{n(m+1)} = x_n\, y_{nm} + x_{nm}\, y_n$.
Como $y_n \mid x_{nm} y_n$ e pela hipótese de indução $y_n \mid x_n y_{nm}$, segue que $y_n \mid x_n y_{nm} + x_{nm}\, y_n$, ou seja, $y_n \mid y_{n(m+1)}$.
Portanto o lema é válido para $k = m + 1$, o que conclui a prova por indução. ■

Lema 3.9 *$y_n \mid y_t$ se, e somente se, $n \mid t$.*

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 3.5 temos que, $y_t = x_r\, y_{nq} + x_{nq}\, y_r$. Do Lema 3.8 $y_n \mid y_{nq}$ e por hipótese $y_n \mid y_t$, como $x_{nq} y_r = y_t - x_{nq} y_r$ segue que $y_n \mid x_{nq}\, y_r$.
Mas $(y_n, x_{nq}) = 1$, (se $d \mid y_n$ e $d \mid x_{nq}$, pelo Lema 3.8 $d \mid y_{nq}$, e como $(x_{nq}, y_{nq}) = 1$ pelo Lema 3.7, segue que $d \mid 1$, ou seja, $d = 1$). Portanto $y_n \mid y_r$, e daí $y_n \le y_r$.
Por outro lado, $n > r$, e pelo Lema 3.6 teríamos $y_n > y_r$, uma contradição.
Reciprocamente, se $n \mid t$, então $t = nk$, pelo Lema 3.8 $y_n \mid y_{nk}$, ou seja, $y_n \mid y_t$. ■

Lema 3.10 *$y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}, \quad \forall\ k \in \mathbb{Z},\ k \ge 1$.*

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:

$$(x_n + y_n\sqrt{d})^k = \sum_{j=0}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) x_n^{k-j} y_n^j d^{\frac{j}{2}} =$$
$$= \left(\begin{array}{c} k \\ 0 \end{array} \right) x_n^k + \left(\begin{array}{c} k \\ 1 \end{array} \right) x_n^{k-1} y_n d^{\frac{1}{2}} + \left(\begin{array}{c} k \\ 2 \end{array} \right) x_n^{k-2} y_n^2 d + \left(\begin{array}{c} k \\ 3 \end{array} \right) x_n^{k-3} y_n^3 d^{\frac{3}{2}} + \ldots + \left(\begin{array}{c} k \\ k \end{array} \right) y_n^k d^{\frac{k}{2}}$$

desta igualdade concluímos que:

$$y_{nk} = \sum_{\substack{j=1 \\ j \text{ ímpar}}}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) x_n^{k-j} y_n^j d^{\frac{j-1}{2}} = k x_n^{k-1} y_n + \sum_{\substack{j=3 \\ j \text{ ímpar}}}^{k} \left(\begin{array}{c} k \\ j \end{array} \right) x_n^{k-j} y_n^j d^{\frac{j-1}{2}}.$$

Mas para $j \geq 3$, os termos desta expansão são todos congruentes a zero $\pmod{y_n^3}$.
Então $y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}$. ■

Lema 3.11 *$y_n^2 \mid y_{ny_n}$.*

Demonstração.
Utilizando $k = y_n$ no Lema 3.10 obtemos $y_{ny_n} \equiv y_n^2 x_n^{y_n - 1} \pmod{y_n^3}$ e desta congruência temos que:

$$y_{ny_n} = (y_n)^3 t + y_n^2 x_n^{y_n - 1} = y_n^2 (y_n t + x_n^{y_n - 1}),$$

de onde concluímos que $y_n^2 \mid y_{ny_n}$. ■

Lema 3.12 *$y_n^2 \mid y_t$ então $y_n \mid t$.*

Demonstração.
Como $y_n^2 \mid y_t$, segue que $y_n \mid y_t$ e pelo Lema 3.9, $n \mid t$. Seja $t = nk$.
Do Lema 3.10 temos que, $k x_n^{k-1} y_n = y_{nk} - u(y_n)^3$ e como $y_n^2 \mid y_{nk}$ e $y_n^2 \mid (y_n)^3$ concluímos que $y_n^2 \mid k x_n^{k-1} y_n$, ou ainda, $y_n \mid k x_n^{k-1}$. Mas pelo Lema 3.7, $(x_n, y_n) = 1$.
Então $y_n \mid k$, e como $t = nk$, segue que $y_n \mid t$. ■

Lema 3.13 *$x_{n+1} = 2ax_n - x_{n-1}$ e $y_{n+1} = 2ay_n - y_{n-1}$.*

Demonstração.
Do Lema 3.6 temos:

$$x_{n+1} = ax_n + dy_n \quad \text{e} \quad y_{n+1} = ay_n + x_n,$$

$$x_{n-1} = ax_n - dy_n \quad \text{e} \quad y_{n-1} = ay_n - x_n,$$

e então:

$$x_{n+1} + x_{n-1} = 2ax_n \Rightarrow x_{n+1} = 2ax_n - x_{n-1}.$$

$$y_{n+1} - y_{n-1} = 2ay_n \Rightarrow y_{n+1} = 2ay_n - y_{n-1}.$$

■

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 3.14 *$y_n \equiv n \pmod{a-1}$.*

Demonstração.

Utilizaremos indução.

Para $n = 0$ e $n = 1$ a congruência é trivialmente satisfeita. Vamos supor que o lema é verdadeiro para $k \leq n$. Então $y_n \equiv n \pmod{a-1}$ e $y_{n-1} \equiv n-1 \pmod{a-1}$. Mas como $a \equiv 1 \pmod{a-1}$, segue das propriedades de congruência que $2ay_n \equiv 2n \pmod{a-1}$ e $-y_{n-1} \equiv -(n-1) \pmod{a-1}$, logo: $2ay_n - y_{n-1} \equiv 2n - (n-1) = n+1 \pmod{a-1}$.

Pelo Lema 3.13, $y_{n+1} = 2ay_n - y_{n-1}$, portanto $y_{n+1} \equiv n+1 \pmod{a-1}$, o que conclui a prova. ■

Lema 3.15 *Se* $a \equiv b \pmod{c}$, *então* $\forall\ n,\ x_n(a) \equiv x_n(b) \pmod{c}$ *e* $y_n(a) \equiv y_n(b) \pmod{c}$.

Demonstração.

Vamos provar que $x_n(a) \equiv x_n(b) \pmod{c}$. Utilizaremos indução. Para $n = 0$ e $n = 1$ a congruência é trivialmente satisfeita. Vamos supor que o lema é verdadeiro para $k \leq n$.

Em particular, $x_n(a) \equiv x_n(b) \pmod{c}$ e $x_{n-1}(a) \equiv x_{n-1}(b) \pmod{c}$. Destas duas congruências temos que:

$$2ax_n(a) - x_{n-1}(a) \equiv 2ax_n(b) - x_{n-1}(b) \pmod{c},$$

e pelo Lema 3.13 concluímos que $x_{n+1}(a) \equiv x_{n+1}(b) \pmod{c}$ o que conclui a prova.

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

Lema 3.16 *Quando* n *é par,* y_n *é par e quando* n *é ímpar,* y_n *é ímpar.*

Demonstração.

Considerando $y_{n+1} = 2ay_n - y_{n-1} \equiv y_{n-1} \pmod{2}$:

Se n é par, então $y_n \equiv y_0 = 0 \pmod{2}$, o que implica que y_n é par.

Se n é ímpar, então $y_n \equiv y_1 = 1 \pmod{2}$, o que implica que y_n é ímpar. ■

Lema 3.17 $x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$.

Demonstração.

Utilizaremos indução.

Para $n = 0$, temos $x_0 - y_0(a-y) = 1 = y^0$ e para $n = 1$, temos $x_1 - y_1(a-y) = y = y^1$. Suponha que o lema seja verdadeiro para $k \leq n$.

Pelo Lema 3.13 temos que : $x_{n+1}(a) - y_{n+1}(a)(a-y) = 2a[x_n - y_n(a-y)] - [x_{n-1} - y_{n-1}(a-y)]$, mas pela hipótese de indução,

$x_n - y_n(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$ e $-[x_{n-1} - y_{n-1}(a-y)] \equiv -y^{n-1} \pmod{2ay - y^2 - 1}$. Portanto:

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

e daí,

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

Mas $2ay - 1 \equiv y^2 \pmod{2ay - y^2 - 1}$. Logo,

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

o que conclui a prova. ■

Lema 3.18 $\forall\ n,\ \ y_{n+1} > y_n \geq n$.

Demonstração.

Pelo Lema 3.6 , $y_{n+1} > y_n$.

Resta provar que $y_n \geq n$. Utilizaremos indução.

Se $n = 0$, o lema é verdadeiro, pois $y_0 = 0 \geq 0$.

Suponha que o lema seja verdadeiro para n, ou seja, $y_n \geq n$.

Temos que $y_{n+1} > y_n \quad \Rightarrow y_{n+1} \geq y_n + 1$, e pela hipótese de indução $y_{n+1} \geq n + 1$, o que conclui a prova. ■

Lema 3.19 $\forall\ n, \quad a^n \leq x_n(a) < x_{n+1}(a)$ *e* $x_n(a) \leq (2a)^n$.

Demonstração.

Para $n = 0$, as desigualdades se verificam, pois $x_0 = 1$ e $x_1 = a > 1$. Por indução, suponha o Lema válido para n e provemos que ele é válido para $n + 1$.

Pelo Lema 3.6

$$x_{n+1} = ax_n + dy_n \geq ax_n$$

e por indução temos

$$a^{n+1} = a \cdot a^n \leq ax_n \leq x_{n+1}\,.$$

Como $a > 1$,

$$a^{n+1} \leq x_{n+1} < ax_{n+1} \leq x_{n+2}\,.$$

Pelo Lema 3.13

$$x_{n+1} = 2ax_n - x_{n-1} \leq 2ax_n\,.$$

Como por indução $x_n \leq (2a)^n$, temos

$$x_{n+1} \leq 2ax_n \leq 2a \cdot (2a)^n = (2a)^{n+1}\,.$$

■

Lema 3.20 $x_{2n\pm j} \equiv -x_j \pmod{x_n}$.

Demonstração.

Pelas fórmulas de adição do Lema 3.5 temos que:

$$\begin{aligned} x_{2n+j} &= x_{n+(n+j)} = x_n x_{n+j} + dy_n y_{n+j}\,, \\ x_{n+j} &= x_n x_j + dy_j y_n\,, \\ y_{n+j} &= x_j y_n + x_n y_j\,. \end{aligned}$$

Então,

$$x_{2n+j} = x_n x_n x_j + dy_n(y_n x_j + x_n y_j) + dy_n x_n y_j\,.$$

A partir desta igualdade temos:

$$x_{2n+j} \equiv dy_n^2 x_j \pmod{x_n}\,.$$

Mas $dy_n^2 = x_n^2 - 1$, logo $x_{2n+j} \equiv (x_n^2 - 1)x_j \equiv -x_j \pmod{x_n}$.

De forma análoga prova-se que $x_{2n-j} \equiv -x_j \pmod{x_n}$. ■

Lema 3.21 $x_{4n\pm j} \equiv x_j \pmod{x_n}$.

Demonstração.

Pelo Lema 3.20, $x_{4n\pm j} \equiv -x_{2n\pm j} \equiv x_j \pmod{x_n}$. ■

Lema 3.22 *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.

Primeiro suponha que x_n é ímpar e seja $q = \dfrac{x_n - 1}{2}$. Então os números

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

formam um sistema completo de restos módulo x_n.

Pelo Lema 3.19, $1 = x_0 < x_1 < \ldots < x_{n-1}$. Usando o Lema 3.6, $x_{n-1} \leq \dfrac{x_n}{a} \leq \dfrac{x_n}{2}$, assim $x_{n-1} \leq q$.

Também pelo Lema 3.20 os números $x_{n+1}, x_{n+2}, \ldots, x_{2n-1}, x_{2n}$ são congruentes módulo x_n a respectivamente:

$$-x_{n-1}, -x_{n-2}, \ldots, -x_1, -x_0 = -1.$$

Deste modo os números $x_0, x_1, \ldots, x_{2n}$ são mutuamente incongruentes módulo x_n. O que prova o resultado.

A seguir suponha que x_n é par e seja $q = \dfrac{x_n}{2}$. Neste caso, os números

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

formam um sistema completo de restos módulo x_n(pois $-q \equiv q \pmod{x_n}$). Como acima $x_{n-1} \leq q$. Assim, o resultado segue como acima, exceto se $x_{n-1} = q = \dfrac{x_n}{2}$, de modo que pelo Lema 3.13, $x_{n+1} \equiv -q \pmod{x_n}$ e se $i = n-1$ e $j = n+1$ nosso resultado seria falso. Mas do Lema 3.6, $x_n = ax_{n-1} + dy_{n-1}$, e desse modo $x_n = 2x_{n-1}$ implica $a = 2$ e $y_{n-1} = 0$, isto é, $n = 1$. Assim, o resultado pode falhar somente quando $a = 2,\ n = 1,\ i = 0$ e $j = 2$. ■

Lema 3.23 *Seja* $x_j \equiv x_i \pmod{x_n}$, $n > 0,\ 0 < i \leq n,\ 0 \leq j < 4n$, *então* $j = i$ *ou* $j = 4n - i$.

Demonstração.

Primeiro suponha que $j \leq 2n$. Então pelo Lema 3.22, $j = i$, exceto se o caso excepcional ocorrer. Se $i > 0$, então isto só pode acontecer se $j = 0$. Mas então $i = 2 > 1 = n$, uma contradição.

Por outro lado, seja $j > 2n$ e considerando $j' = 4n - j$, temos $0 < j' < 2n$. Do Lema 3.21,

$$x_{j'} \equiv x_j \equiv x_i \pmod{x_n}.$$

Novamente $j' = i$, exceto se o caso excepcional do Lema 3.22 ocorrer, mas isto esta fora de questão pois, $i, j' > 0$ ■

Lema 3.24 *Seja* $0 < i \leq n$ *e* $x_j \equiv x_i \pmod{x_n}$ *então* $j \equiv \pm i \pmod{4n}$.

Demonstração.

Escrevendo $j = 4nq + j',\ \ 0 \leq j' < 4n$. Então pelo Lema 3.21, $x_i \equiv x_j \equiv x_{j'} \pmod{x_n}$.

E pelo Lema 3.23, $i = j'$ ou $i = 4n - j'$.

Se $i = 4n - j'$, como $j = 4nq + j'$ segue que:

$$i + j = 4n(q+1) \equiv 0 \pmod{4n}, \text{ então } j \equiv -i \pmod{4n}.$$

Se $i = j'$, como $j = 4nq + j'$ segue que:

$$j - i = 4nq \equiv 0 \pmod{4n}, \text{ então } j \equiv i \pmod{4n}.$$

■

Lema 3.25 *Se* $a > y^k$, *então* $2ay - y^2 - 1 > y^k$.

Demonstração.

Defina $g(y) = 2ay - y^2 - 1$. Então $g(1) = 2a - 2 \geq a$, pois $a \geq 2$.

Para $1 \leq y < a$, $g'(y) = 2a - 2y > 0$, ou seja, a função $g(y)$ é crescente para $1 \leq y < a$.

Logo, $g(y) \geq a$ para $1 \leq y < a$. Então para $a > y^k \geq y$, segue que:

$$2ay - y^2 - 1 \geq a > y^k.$$

■

Estes lemas serão necessários 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 3.1 *Dados a, x, k, $a > 1$, o sistema de (I)-(VIII) tem solução nos argumentos restantes $y, u, v, s, t, b, r, p, q, c, d, e$ se, e somente se, $x = x_k(a)$.*

Demonstração.

Primeiramente consideremos dadas as soluções de (I)-(VIII).

De (V), $b > a > 1$. Pelo Lema 3.4 concluímos apartir de (I), (II) e (III) que existem $i, j, n > 0$ tais que:

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

De (IV), $y \leq v$ e então $i \leq n$. As equações (V) e (VI) produzem as seguintes congruências:

$$b \equiv a \pmod{x_n(a)} \quad \text{e} \quad x_i(a) \equiv x_j(b) \pmod{x_n(a)}$$

e do Lema 3.15, também temos: $x_j(b) \equiv x_j(a) \pmod{x_n(a)}$.

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

A partir desta congruência o Lema 3.24 fornece que:

(1) $j \equiv \pm i \pmod{4n}$.

Da equação (IV) deduz-se que $(y_i(a))^2 \mid y_n(a)$ e do Lema 3.12 $y_i(a) \mid n$, daí (1) implica:

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

Da equação (V), $b \equiv 1 \pmod{4y_i(a)}$, e do Lema 3.14 segue que:

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

Da equação (VII):

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

Combinando (2), (3) e (4) obtemos:

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

A equação (VIII) produz $k \leq y_i(a)$ e do Lema 3.18 $i \leq y_i(a)$, ou seja, $2y_i(a) < k \pm i \leq 2y_i(a)$, mas $4y_i(a) \mid k \pm i$, então k=i.

Assim,

$$x = x_i(a) = x_k(a)\,.$$

Reciprocamente, seja $x = x_k(a)$. Assim, $y = y_k(a)$ satistaz (I). Considere $m = 2ky_k(a)$ e seja $u = x_m(a)$ e $v = y_m(a)$. Então (II) é satisfeita.

Pelo Lema 3.11, $y_k^2 \mid y_{ky_k}$, mas $ky_k \mid m$, pelo Lema 3.9, $y_{ky_k} \mid y_m$. Portanto $y_k^2 \mid y_m$, isto é, $y_k^2 \mid v$. Com isto podemos escolher r satisfazendo (IV).

Além disso, como m é par, pelo Lema 3.16, v é par e como u e v satisfazem (II) segue que u é ímpar. Pelo Lema 3.7, $(u, v) = 1$. Portanto, $(u, v4y) = 1$, 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 3.9, $y_k \mid y_m$, 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 :

$$\begin{aligned} b_0 &\equiv 1 \pmod{4y} \text{ e} \\ b_0 &\equiv a \pmod{u}\,, \end{aligned}$$

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

A equação (III) é satisfeita, definindo, $s = x_k(b)$ e $t = y_k(k)$. Assim, $b > a$, $s = x_k(b) > x_k(a) = x$.

Pelo Lema 3.15 e utilizando (V), $s \equiv x \pmod{u}$. Assim, c pode ser escolhido de forma a satisfazer (VI). Pelo Lema 3.18, $y_k \geq k$, ou seja, $t \geq k$ e pelo Lema 3.14, $y_k = t \equiv k \pmod{b-1}$ e assim, usando (V), $t \equiv k \pmod{4y}$.

Podemos então escolher d satisfazendo a equação (VII).

Pelo Lema 3.18 novamente, $y \geq k$, então (VIII) pode ser satisfeito tomando $e = y - k + 1$. ■

O Teorema 3.1 implica que o conjunto

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

é Diofantino, basta utilizar o Lema 2.1 para reduzir o sistema de equações Diofantinas (I)-(VIII).

Corolário 3.1 *A função $g(z, k) = x_k(z + 1)$ é Diofantina.*

Incluindo ao sistema (I)-(VIII) a equação $a = z + 1$ (*)

Pelo teorema anterior, o sistema (*), (I)-(VIII) tem solução se, e somente 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 inclua 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 teorema.

Lema 3.26 *$m = n^k$ se, e somente se, as equações (I)-(XII) tem uma solução nos argumentos restantes.*

Demonstração.

Suponha que (I)-(XII) é satisfeito. De, (XI), $w > 1$. Assim $(w-1)z > 0$ e por (XII) $a > 1$. Assim, aplicando o Teorema 3.1 segue que:

$$x = x_k(a) \text{ e } y = y_k(a).$$

Por (IX),

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

e pelo Lema 3.17,

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

Destas duas congruências concluímos que $m \equiv n^k \pmod{2an - n^2 - 1}$

A equação (XI) implica que $k, n < w$.

De (XII) e do Lema 3.4, para algum j, $a = x_j(w)$ e $(w-1)z = y_j(w)$. Do Lema 3.14, $y_j(w) \equiv j \pmod{w-1}$ e como $y_j(w) \equiv 0 \pmod{w-1}$ concluímos que

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

e daí $j \geq w-1$, pois $w-1 \mid j$. Do Lema 3.19, $a \geq w^1 \geq w^{w-1} > n^{w-1} \geq n^k$.

Agora de (X), $m < 2an - n^2 - 1$, e do Lema 3.25, $n^k < 2an - n^2 - 1$.

Como m e n^k são congruentes e ambos são menores do que $2an - n^2 - 1$, eles devem ser iguais.

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

Seja $a = x_{w-1}(w)$ tal que $a > 1$. Do Lema 3.14,

$y_{w-1}(w) \equiv w - 1 \pmod{w-1}$ e como $w - 1 \equiv 0 \pmod{w-1}$ segue que:

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

Assim, podemos escrever $y_{w-1}(w) = z(w-1)$, e desse modo (XII) é satisfeita tomando,

$$x_{w-1} = a$$
$$\text{e}$$
$$y_{w-1} = z(w-1)$$

.

A equação (XI) pode ser satisfeita definindo $h = w - n$ e $l = w - k$.

Como anteriormente, $a > n^k$ e novamente pelo Lema 3.25,

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

Então a equação (X) pode ser satisfeita. Definindo $x = x_k(a)$ e $y = y_k(a)$, o Lema 3.17 nos permite definir f tal que:

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

de forma que (IX) é satisfeita. Finalmente, o sistema (I)-(VIII) pode ser satisfeito pelo Teorema 3.1. ■

O Lema 3.26 implica que o conjunto

$$N = \{\langle m, n, k\rangle \mid m = n^k\}$$

é Diofantino, basta utilizar o Lema 2.1 para reduzir o sistema de equações Diofantinas (I)-(XII). E esta conclusão implica diretamente no resultado mais importante desta seção que enunciamos no teorema abaixo.

Teorema 3.2 *A função exponencial $h(n,k) = n^k$ é Diofantina.*

3.2 A Linguagem dos Predicados Diofantinos

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

Como por exemplo, seja $h(u,v,w) = u^{v^w}$.

Mostremos que h é Diofantina.

Temos que:

$$y = u^{v^w} \Leftrightarrow (\exists\ z)(y = u^z\ \wedge\ z = v^w)\,,$$

onde " $\wedge$ " é o símbolo lógico para "*e*". Usando o Teorema 3.2, existe um polinômio P tal que:

$$y = u^z\ \Leftrightarrow (\exists\ r_1,\ldots,r_n)\ [P(y,u,z,r_1,\ldots,r_n) = 0]\,,$$

$$z = v^w\ \Leftrightarrow (\exists\ s_1,\ldots,s_n)\ [P(z,v,w,s_1,\ldots,s_n) = 0]\,.$$

Então,

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

Este procedimento é perfeitamente generalizável.

Expressões que já são conhecidas por gerar conjuntos Diofantinos podem ser combinadas livremente utilizando os operadores lógicos " $\wedge$ " e "$\exists$", a expressão resultante será novamente um conjunto Diofantino. Estas expressões são chamadas de predicados Diofantinos.

Nesta linguagem é permitido o uso dos símbolos lógicos " $\vee$ " para "*ou*", assim

$$(\exists\ r_1,\ldots,r_n)\ [P_1 = 0]\ \vee (\exists\ s_1,\ldots,s_m)\ [P_2 = 0] \Leftrightarrow (\exists\ r_1,\ldots,r_n,s_1,\ldots,s_m)\ [P_1\cdot P_2 = 0]\,.$$

Três importantes funções Diofantinas são dadas por:

Teorema 3.3 *As seguintes funções são Diofantinas:*

(1)
$$f(n,k) = \binom{n}{k}$$

(2)
$$g(n) = n!$$

(3)
$$h(a,b,y) = \prod_{k=1}^{y}(a+bk)$$

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

$$[\alpha] \le \alpha < [\alpha] + 1\,.$$

Lema 3.27 *Para* $0 < k \le n$, $u > 2^n$ *temos que*

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

Demonstração.

$$(u+1)^n = \sum_{i=0}^{n}\binom{n}{i}u^i\,,$$

então

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

onde

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

Então S é um inteiro e

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

Assim,

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

o que prova o resultado. ■

Lema 3.28 *Para $0 < k \leq n$, $u > 2^n$ temos que*

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

Demonstração.

No Lema 3.27 todos os termos da soma para os quais $i > k$ são divisíveis por u, logo congruentes a zero $\pmod{u}$.

■

Lema 3.29 *$f(n,k) = \binom{n}{k}$ é Diofantina.*

Demonstração.

Como

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

o Lema 3.28 determina que $\binom{n}{k}$ é o único inteiro positivo congruente a $\left[\frac{(u+1)^n}{u^k}\right] \pmod{u}$ e menor que u.

Desse modo,

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

Para ver que $\binom{n}{k}$ é Diofantina, é suficiente notar que cada expressão acima separada por "$\wedge$" é um predicado Diofantino, $v = 2^n$ é claramente Diofantino pelo Teorema 3.2.

A inequação $u > v$ é claramente Diofantina pois $u > v \Leftrightarrow (\exists\, x)\ (u = v + x)$. Também,

$$z \equiv w \pmod{u} \wedge\ z < u \Leftrightarrow (\exists\, x,y)\ (w = z + (x-1)u \ \wedge\ u = z + y).$$

Finalmente,

$$w = \left[\frac{(u+1)^n}{u^k}\right] \Leftrightarrow (\exists\, x,y,t)\ (t = u+1 \ \wedge\ x = t^n \ \wedge\ y = u^k \ \wedge\ w \leq \frac{x}{y} < w+1),$$

e

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

■

Lema 3.30 *Se* $r > (2x)^{x+1}$, *então* $x! = \left[r^x / \binom{r}{x}\right]$.

Demonstração.

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

Então,

$$\left[r^x / \binom{r}{x}\right] = r^x \cdot \frac{x!(r-x)!}{r!} = r^x \cdot \frac{x!.(r-x)!}{r \cdot (r-1) \cdots (r-x+1)(r-x)!} = \frac{r^x.x!}{r \cdot (r-1) \cdots (r-x+1)} =$$
$$= x! \left\{ \frac{1}{(1-\frac{1}{r}) \cdots (1-\frac{(x-1)}{r})} \right\} < x! \frac{1}{(1-\frac{x}{r})^x}$$

Agora,

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

Mas,

$$r > (2x)^{x+1} \Rightarrow \frac{x}{r} < \frac{1}{2 \cdot (2x)^x} < \frac{1}{2}.$$

Então

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

e,

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

Assim,

$$\frac{r^x}{\binom{r}{x}} < x! + \frac{2x}{r} \cdot x! \cdot 2^x = x! + \frac{2^{x+1}x}{r} \cdot x! < x! + \frac{2^{x+1}x^{x+1}}{r},$$

pois $x \cdot x! < x^{x+1}$.

Mas,

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

Portanto,

$$\left[r^x / \binom{r}{x}\right] < x! + 1.$$

Como

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

segue que,

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

O que conclui a prova do lema. ■

Lema 3.31 *$n!$ é uma função Diofantina.*

Demonstração.

$m = n! \Leftrightarrow (\exists\, r, s, t, u, v)\ \{s = 2n+1\ \wedge\ t = n+1\ \wedge\ r = s^t\ \wedge\ u = r^n\ \wedge\ v = \binom{r}{n} \wedge mv \leq u < (m+1)v\}$. ■

Lema 3.32 *Seja $bq \equiv a \pmod m$. Então,*

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

Demonstração.

$$b^y \cdot y!\binom{q+y}{y} = \frac{b^y \cdot y! \cdot (q+y)!}{y! \cdot q!} = \frac{b^y \cdot (q+y)!}{q!} = \frac{b^y \cdot (q+y) \cdot (q+y-1) \cdots (q+1) \cdot q!}{q!} =$$

$$= b^y \cdot (q+y) \cdot (q+y-1) \cdots (q+1) = (bq+yb) \cdot (bq+(y-1)b) \cdots (bq+b),$$

e como $bq \equiv a \pmod m$, segue que:

$$(bq+yb) \cdot (bq+(y-1)b) \cdots (bq+b) \equiv (a+yb) \cdot (a+(y-1)b) \cdots (a+b) \pmod m.$$

E isto prova o resultado. ■

Lema 3.33 *$h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ é uma função Diofantina.*

Demonstração.

No Lema 3.32, escolha $m = b(a+by)^y + 1$. Então $(m,b) = 1$ e $m > \prod_{k=1}^{y}(a+bk)$. Logo, existe um valor de q para o qual a congruência $bq \equiv a \pmod m$ tem solução. Daí, $\prod_{k=1}^{y}(a+bk)$ é o único número menor que m que é congruente módulo m a $b^y y!\binom{q+y}{y}$, isto é,

$$\begin{aligned} z = \prod_{k=1}^{y}(a+bk) \quad \Leftrightarrow \quad & (\exists\, m,p,q,r,s,t,u,v,w,x) \\ & \Big\{\ r = a+by \quad \wedge \quad s = r^y \quad \wedge \quad m = bs+1 \\ & \wedge \quad bq = a+mt \quad \wedge \quad u = b^y \quad \wedge \quad v = y! \quad \wedge \quad z < M \\ & \wedge \quad w = q+y \quad \wedge \quad x = \binom{w}{y} \quad \wedge \quad z+mp = uvx\ \Big\} \end{aligned}$$

Utilizando as expressões anteriores para a função exponencial, para $v = y!$ e para $x = \binom{w}{y}$ nós obtemos o resultado. ■

A afirmação do Teorema 3.3 está provada pelos Lemas 3.29, 3.31 e 3.33.

3.3 Quantificadores Limitantes

A linguagem de predicado Diofantinos usa $\wedge, \vee$ e $\exists$. Outros operadores lógicos usados são:

$\sim$ para "não"

$(\forall x)$ para "para todo x"

$\rightarrow$ para "se..., então..."

Porém, o uso de qualquer uma dessas expressões pode levar a expressões que definem conjuntos que não são Diofantinos.

Mais duas classes de quantificadores mereçem destaque, são elas:

Quantificadores limitantes existenciais:

"$(\exists\ y)_{\leq\ x} \ldots$" que significa "$(\exists\ y)\ (y \leq x\ \wedge \ldots)$"

Quantificadores limitantes universais:

"$(\forall\ y)_{\leq\ x} \ldots$" que significa "$(\forall\ y)\ (y > x \vee \ldots)$"

Estas operações podem ser utilizadas juntamente com a linguagem de predicados Diofantinos, isto é, os conjuntos definidos pelas expressões desta linguagem extendida ainda são Diofantinos.

Teorema 3.4 *Se P é um polinômio, os conjuntos*

$$R = \{\langle y, x_1, \ldots, x_n\rangle \mid\ (\exists\ z)_{\leq\ y}\ (\exists\ y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$

$$e$$

$$S = \{\langle y, x_1, \ldots, x_n\rangle \mid\ (\forall z)_{\leq\ y}\ (\exists\ y_1, \ldots, y_m)[P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$

são Diofantinos.

Que R é Diofantino é trivial. A saber,

$$\langle y, x_1, \ldots, x_n\rangle \in R \Leftrightarrow (\exists\ z, y_1, \ldots, y_m)(z \leq y\ \wedge\ P = 0).$$

Para provar a outra metade do teorema precisamos dos dois lemas seguintes.

Lema 3.34

$$(\ \forall k)_{\leq\ y}\ (\exists\ y_1, \ldots, y_m)\ [P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$
$$\Leftrightarrow$$
$$(\exists\ u)(\ \forall k)_{\leq\ y}(\exists\ y_1, \ldots, y_m)_{\leq\ u}\ [P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0]$$

Demonstração.

Comecemos supondo que o lado esquerdo é verdadeiro para $y, x_1, \ldots, x_n$ dados.

Então para cada $k = 1, 2, \ldots, y$ existem números definidos por $y_1^{(k)}, \ldots, y_m^{(k)}$ para os quais

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

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

$$u = \max\ \{{y_j}^{(k)} \mid j = 1, 2, \ldots, m; k = 1, 2, \ldots, y\}.$$

Segue que o lado direito da equivalência é igualmente verdadeiro.

A recíproca é trivial. ■

Lema 3.35 *Seja* $Q(y,u,x_1,\ldots,x_n)$ *um polinômio com as propriedades:*

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

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

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

Então,

$$(\ \forall k)_{\leq\ y}\ (\exists\ y_1,\ldots,y_m)\ \ [P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m)=0]$$
$$\Leftrightarrow$$
$$(\exists\ c,t,a_1,\ldots,a_m)[1+ct=\prod_{k=1}^{y}(1+kt)$$
$$\wedge\ t=Q(y,u,x_1,\ldots,x_n)!\ \wedge\ 1+ct\ \Big|\ \prod_{k=1}^{y}(a_1-j)$$
$$\wedge\ldots\wedge\ 1+ct\ \Big|\ \prod_{k=1}^{y}(a_m-j)$$
$$\wedge\ P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)\equiv 0 \pmod{1+ct}.$$

Demonstração.

Mostremos primeiro a volta. Para cada $k=1,2,3,\ldots,y$, seja p_k um fator primo de $1+kt$.

Seja $y_i^{(k)}$ o resto da divisão de a_i por p_k ($k=1,2,\ldots,y$; $i=1,2,\ldots,m$).

Disto segue que para cada k,i :

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

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

Para demonstrar (a), note que $p_k \mid 1+kt,\ 1+kt \mid 1+ct$ e $1+ct \mid \prod_{j=1}^{u}(a_i-j)$, isto é,

$p_k \mid \prod_{j=1}^{u}(a_i-j)$. Assim, p_k é primo, $p_k \mid a_i-j$ para algum $j=1,2,\ldots,u$. Isto é:

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

Uma vez que $t=Q(y,u,x_1,\ldots,x_n)!$, (2) implica que todo divisor de $1+kt$ deve ser maior que $Q(y,u,x_1,\ldots,x_n)$.

Assim $p_k > Q(y,u,x_1,\ldots,x_n)$ e de (1), $p_k > u$. Portanto, $j \leq u \leq p_k$.

Uma vez que $y_i^{(k)}$ é o resto da divisão de a_i por p_k, também $y_i^{(k)} < p_k$.

Assim, $y_i^{(k)} = j$.

Para demonstrar (b), primeiro note que $1+ct \equiv 1+kt \equiv 0 \pmod{p_k}$.

Portanto,

$$k+kct \equiv c+kct \equiv 0 \pmod{p_k},$$

isto é,

$$k \equiv c \pmod{p_k}.$$

Nós já tínhamos obtido $y_i^{(k)} \equiv a_i \pmod{p_k}$.

Desse modo,

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

Finalmente,

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

Isto prova (b) e completa a primeira parte da demonstração.

Reciprocamente, suponha que, $P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)}) = 0$, para cada $k = 1,2,\ldots,y$, onde cada $y_j^{(k)} \leq u$.

Nós fixamos $t = Q(y,u,x_1,\ldots,x_n)!$, e uma vez que $\prod_{k=1}^{y}(1+kt) \equiv 1 \pmod{t}$, existe c tal que:

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

Agora, é exigido que para $1 \leq k < l \leq y$, $(1+kt, 1+lt) = 1$.

Se $p \mid 1+kt$ e $p \mid 1+lt$, então $p \mid l-k$, assim, $p < y$. Uma vez que $Q(y,u,x_1,\ldots,x_n) > y$ isto implica que $p \mid t$ que é impossível.

Desse modo os números $1+kt$ são primos entre si e o Teorema Chinês do Resto pode ser aplicado para produzir, para cada i, $1 \leq i \leq m$, um número a_i tal que:

$$a_i \equiv y_i^{(k)} \pmod{1+kt}, \quad k = 1,2,\ldots,y$$

Como acima, $k \equiv c \pmod{1+ct}$. Assim, para cada k nós temos

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

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:

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

Finalmente,

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

isto é,

$1+kt \mid a_i - y_i^{(k)}$ e como $1 \leq y_i^{(k)} \leq u$, $1+kt \mid \prod_{j=1}^{u}(a_i - j)$.

E novamente, como os números $1+kt$ são relativamente primos entre si, $1+ct \mid \prod_{j=1}^{u}(a_i - j)$. ■

Demonstração do Teorema 3.4.

Agora é fácil completar a prova do Teorema 3.4 usando os Lema 3.34 e 3.35.

Primeiro encontre um polinômio Q satisfazendo (1), (2), (3) no Lema 3.35

Isto é fácil de fazer. Escreva:

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

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

para cada c_r positivo ou negativo.

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

Então (1), (2) e (3) do Lema 3.35 é trivialmente satisfeito. Desse modo,

$$(\forall k)_{\leq y} \ \ (\exists\, y_1, y_2, \ldots, y_m)\ [P(y,k,x_1,\ldots,x_n,y_1,\ldots,y_m) = 0]$$

é equivalente a

$$\begin{aligned}
&(\exists\, u,c,t,a_1,\ldots,a_m)\ \Big[1 + ct = \prod_{j=1}^{y}(1+kt) \\
&\wedge\, t = Q(y,u,x_1,\ldots,x_n)!\ \wedge\ 1+ct \ \Big|\ \prod_{j=1}^{u}(a_1 - j) \\
&\wedge\ \ldots\ \wedge\ 1+ct \ \Big|\ \prod_{j=1}^{u}(a_m - j) \\
&\wedge\, P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m) \equiv 0 \pmod{1+ct}\ \Big],
\end{aligned}$$

que por sua vez, é equivalente a

$$
\begin{aligned}
&(\exists\, u, c, t, a_1, \ldots, a_m, e, f, g_1, \ldots, g_m, h_1, \ldots, h_n, l) \\
&\Big[e = 1 + ct \ \wedge\ e = \prod_{k=1}^{y} (1 + kt) \ \wedge\ f = Q(y, u, x_1, \ldots, x_n) \\
&\wedge\, t = f! \ \wedge\ g_1 = a_1 - u - 1 \ \wedge\ g_2 = a_2 - u - 1 \ \wedge \ldots \wedge\ g_m = a_m - u - 1 \\
&\wedge\, h_1 = \prod_{k=1}^{u} (g_1 + k) \ \wedge\ h_2 = \prod_{k=1}^{u} (g_2 + k) \\
&\wedge\ \ldots \wedge\ h_m = \prod_{k=1}^{u} (g_m + k) \ \wedge\ \ e \mid h_1 \ \wedge\ \ e \mid h_2 \ \wedge\ \ldots \wedge\ e \mid h_m \\
&\wedge\, l = P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_n) \ \wedge\ \ e \mid l \ \Big] .
\end{aligned}
$$

E este último predicado é Diofantino pelo Teorema 3.3. ■

3.4 Funções Recursivas

Utilizando a versão extendida da linguagem de Predicados Diofantinos, os quantificadores limitantes e o Teorema da Sequência de Números, podemos mostrar que vários conjuntos são Diofantinos.

Veja alguns exemplos:

(i) O conjunto dos números primos:

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

Outra definição Diofantina dos números primos é:

$$x \in \mathbb{P} \Leftrightarrow x > 1 \wedge ((x-1)!, x) = 1 \Leftrightarrow x > 1 \wedge (\exists y, z, u, v)\, [y = x - 1 \wedge z = y! \wedge (uz - vx)^2 - 1] .$$

Pelo Teorema 2.3, existe um polinômio P tal que: Um inteiro positivo é primo se, e somente se, é um elemento da imagem da função definida por P.

Em 1971, Yuri Matiyasevich mostrou que com 24 variáveis, o grau do polinômio seria 37, mas tal polinômio não foi dado explicitamente.

Somente em 1976 um polinômio foi determinado explicitamente por Jones, Sato, Wada e Wins, tem grau 25 e 26 variáveis, e pode ser encontrado em [21].

Evidente somos tentados a diminuir o número de variáveis, a reduzir o grau do polinômio, ou fazer ambas as coisas. Mas há um preço a pagar. Se o número de variáveis é reduzido, o grau do polinômio aumente, ou vice-versa. No mesmo ano, Jones, Sato, Wada e Wins determinaram o recorde, que foi um polinômio de grau 5 e de 42 variáveis. Não se sabe qual seria o número mínimo de variáveis, mas sabe-se que não pode ser 1 ou 2. Entretanto, Jones mostrou que existe um polinômio representando os números primos tendo grau inferior ou igual a 5. Mais informações sobre tais polinômios podem ser obtidas em [22].

(ii) A função $g(y) = \prod_{k=1}^{y} (1 + k^2)$.

Aqui nós usamos o Teorema da Sequência de Números para codificar a sequência $g(1), g(2), \ldots, g(y)$ por um único número u, isto é,

$$S(i, u) = g(i)\ ; i = 1, 2, \ldots, y$$

Desse modo,

$z = g(y) \Leftrightarrow (\exists\, u)\, \{S(1, u) = 2 \wedge (\forall k)_{\leq\, y}\, [\, k = 1 \vee (S(k, u) = (1 + k^2) \cdot S(k - 1, u))] \wedge z = S(y, u)\}$

$\Leftrightarrow\ (\exists\, u)\, \{S(1, u) = 2 \wedge (\forall k)_{\leq\, y}\, [\, k = 1 \vee (\exists = a, b, c)\, (a = k - 1 \wedge b = S(a, u) \wedge c = S(k, u) \wedge c = (1 + k^2)b)] \wedge z = S(y, u)\}$.

A força destes métodos pode ser testada ao considerar a classe de todas as funções computáveis ou recursivas.

Estas são as funções que podem ser computadas por um programa finito ou máquina que tenha uma grande quantidade de tempo e memória disponível.

Existem várias definições rigorosas destas classes. Uma das mais simples é a seguinte:

As funções recursivas são aquelas que podem ser obtidas a partir das funções iniciais:

$$c(x) = 1; \quad S(x) = x + 1; \quad U_i^n(x_1, \ldots, x_n) = x_i, \quad 1 \leq i \leq n; \quad S(i, u).$$

Aplicando iterativamente as três operações: composição, recursão primitiva e minimização definidas abaixo:

Composição define a função:

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

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

Recursão primitiva define a função $h(x_1, \ldots, x_n, z)$ que satisfaz as equações:

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

a partir das funções f, g dadas. Quando $n = 0$, f torna-se uma constante e h é obtida diretamente de g.

Minimização define a função:

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

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

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

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

Abaixo temos uma lista de algumas funções recursivas.

(1) $x + y$ é recursiva.

Considere $g(u, v, w) = S(U_2^3(u, v, w))$ e $f(x) = S(x) = x + 1$.
Então pela recursão primitiva $h(x, t) = x + t$.

(2) $x.y$ é recursiva.

Considere $h(x, y) = x + y$ e $g(t, v, x) = U_2^3(t, v, x) + U_3^3(t, v, x)$ e $f(x) = U_1^1(x) = x \cdot 1$,
nós obtemos $h(x, t) = x \cdot t$.

(3) Para cada k fixado, a função constante $c_k(x) = k$ é recursiva.

Isto é evidente uma vez que $c_1(x)$ é uma das funções iniciais e $c_{k+1}(x) = c_k(x) + c(x)$.

(4) Alguns polinômios $P(x_1, \ldots, x_n)$ com coeficientes inteiros positivos são recursivos.

Uma vez que algumas desta funções podem ser expressadas por uma iteração finita de adição e mutiplicação de variáveis e $c(x)$.

Por exemplo:

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

Assim, (1), (2), (3) e composições dão o resultado.

Agora enunciaremos um dos resultados centrais deste trabalho:

Teorema 3.5 *Uma função é Diofantina se, e somente se, é recursiva.*

Demonstração.

Inicialmente, suponha que f é Diofantina e escreva:

$$y = f(x_1, \ldots, x_n) \Leftrightarrow \ (\exists\ t_1, \ldots, t_m)\ [\ P(x_1, \ldots, x_n, y, t_1, \ldots, t_m) = Q(x_1, \ldots, x_n, y, t_1, \ldots, t_m)],$$

onde P e Q são polinômios com coeficientes inteiros e positivos. Então pelo Teorema da Sequência de Números:

$$\begin{aligned} f(x_1, \ldots, x_n) &= S(1, \min_u[\ P(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u)) \\ &= Q(x_1, \ldots, x_n, S(1,u), S(2,u), \ldots, S(m+1,u))])\,. \end{aligned}$$

Uma vez que P, Q e $S(i,u)$ são recursivas e utilizando a minimização e composição, concluímos que f é recursiva.

Para provar a recíproca, basta mostrar que as funções Diofantinas são fechadas para as operações de composição, recursão primitiva e minimização, já que no Teorema 2.2 mostramos que $S(i,u)$ é Diofantina e as outras funções iniciais são trivialmente Diofantinas.

Faremos isto a seguir:

Composição:

Se $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$, onde $f, g_1, \ldots, g_m$ são Diofantinas então h também é uma vez que

$$\begin{gathered} y = h(x_1, \ldots, x_n) \Leftrightarrow \\ (\exists\ t_1, \ldots, t_m)\ [t_1 = g_1(x_1, \ldots, x_n)\ \wedge\ \ldots \wedge\ t_m = g_m(x_1, \ldots, x_n)\ \wedge\ y = f(t_1, \ldots, t_m)]. \end{gathered}$$

Recursão primitiva:

Se

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, t+1) &= g(t, h(x_1, \ldots, x_n, t), x_1, \ldots, x_n), \end{aligned}$$

e f, g são Diofantinas, então usando o Teorema da Sequência de Números para codificar os números $h(x_1, \ldots, x_n, 1), h(x_1, \ldots, x_n, 2), \ldots, h(x_1, \ldots, x_n, z)$:

$$\begin{gathered} y = h(x_1, \ldots, x_n, z) \Leftrightarrow \\ (\exists\ u)\ \{(\exists\ v)\ [v = S(1,u)\ \wedge\ v = f(x_1, \ldots, x_n)] \\ \wedge\ (\forall\ t)_{\leq\ z}\ [\ (t = z)\ \vee\ (\exists\ v)\ (v = S(t+1,u) \\ \wedge\ v = g(t, S(t,u), x_1, \ldots, x_n))]\ \wedge\ y = S(z,u)\}. \end{gathered}$$

e assim, utilizando o Teorema 3.4, h é Diofantina.

Minimização:

Se

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

onde f, g são Diofantinas, então h também é, uma vez que:

$$y = h(x_1, \ldots, x_n) \Leftrightarrow (\exists\ z)\ [z = f(x_1, \ldots, x_n, y)\ \wedge\ z = g(x_1, \ldots, x_n, y)]\ \wedge$$

$$(\forall\ t)_{\leq\ y}\ [\ (t = y)\ \vee (\exists\ u, v)\ (u = f(x_1, \ldots, x_n, t) \wedge v = g(x_1, \ldots, x_n, t)\ \wedge\ (u < v\ \vee v < u)].$$

■

3.5 O Conjunto Diofantino Universal

Nesta seção daremos uma enumeração explícita de todos os conjuntos Diofantinos de inteiros positivos.

Qualquer polinômio a coeficientes inteiros e positivos pode ser construído a partir do número 1 e de um alfabeto fixado $x_0, x_1, x_2, \ldots$ de variáveis, utilizando adições e multiplicações sucessivas.

As funções abaixo geram todos os polinômios com coeficientes inteiros e positivos, estas dependem das funções de emparelhamento descritas no Teorema 2.1.

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

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 esteja incluidas (É claro que P_i geralmente não depende de todas estas variáveis).

Finalmente, seja

$$D_n = \{x_0 \mid (\exists\, x_1, \ldots, x_n)\ [\ P_{L(n)}(x_0, x_1, \ldots, x_n) = P_{R(n)}(x_0, x_1, \ldots, x_n)]\}.$$

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

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. Além disso,

Teorema 3.6 (Teorema da Universalidade)

O conjunto $\{\langle n, x\rangle \mid x \in D_n\}$ *é Diofantino.*

Demonstração.

Mais uma vez utilizando o Teorema da Sequência de Números afirmamos que:

$$x \in D_n$$

é equivalente a

$$(\exists\, u) \quad \{S(1,u) = 1 \ \wedge\ S(2,u) = x \ \wedge\ (\forall\, i)_{\leq\, n}\ [S(3i,u) = S(L(i),u) + S(R(i),u)]$$

$$\wedge\ (\forall\, i)_{\leq\, n}\ [S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)] \ \wedge\ S(L(n),u) = S(R(n),u)\}.$$

É claro que o predicado no lado direito desta equivalência é Diofantino, por isso é necessário apenas verificar a afirmação:

Seja $x \in D_n$ para x e n dados. Então existem números $t_1, \ldots, t_n$ tais que:

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

Escolha u, pelo Teorema da Sequência de Números, de modo que:

$$S(j,u) = P_j\ (x, t_1, \ldots, t_n), \ \ j = 1, 2, \ldots, 3n+2. \tag{3.1}$$

Então em particular $S(2,u) = x$ e $S(3i-1,u) = t_{i-1};\ i = 2, 3, \ldots, n+1$. Desse modo o lado direito da equivalência é verdadeiro.

Reciprocamente, seja o lado direito verdadeiro para x e n dados.
Seja $t_1 = S(5,u), t_2 = S(8,u), \ldots, t_n = S(3n+2,u)$.

Então, (3.1) deve ser verdadeiro. Uma vez que, $S(L(n),u) = S(R(n),u)$, devemos ter:

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

tal que $x \in D_n$. ■

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

$$V = \{n \ \mid\ n \notin D_n\}.$$

Teorema 3.7 *V não é Diofantino.*

Demonstração.
Esta é uma simples aplicação do método de diagonalização de Cantor. Se V fosse Diofantino, então para algum i fixado, $V = D_i$. Logo,

$$i \in V \Leftrightarrow i \in D_i \qquad \text{e} \qquad i \in V \Leftrightarrow i \notin D_i,$$

uma contradição. ■

Teorema 3.8 *A função $g(n, x)$ definida por:*

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

não é recursiva.

Demonstração.
Se g fosse recursiva, então seria Diofantina. Afirmamos:

$$y = g(n,x) \Leftrightarrow (\exists\ y_1, \ldots, y_m)\ [P(n, x, y, y_1, \ldots, y_m) = 0].$$

Mas disto segue que:

$$\begin{aligned} V &= \{x \mid x \in D_x\} = \{x \mid g(x,x) = 1\} \\ &= \{x \mid (\exists\ y_1, \ldots, y_m)\ \ [P(x, x, 1, y_1, \ldots, y_m) = 0]\}, \end{aligned}$$

o que contradiz o Teorema 3.7. ■

Teorema 3.9 *O Décimo problema de Hilbert é insolúvel.*

Demonstração.
Usando o Teorema da Universalidade, sabemos que:

$$\text{O conjunto } \{\langle n, x\rangle \mid x \in D_n\} \text{ é Diofantino.}$$

Logo, existe uma equação diofantina P, de parâmetros x, n e variáveis $z_1, \ldots, z_k$ tal que:

$$x \in D_n \Leftrightarrow\ (\exists\ z_1, \ldots, z_k)\ [P(n, x, z_1, \ldots, z_k) = 0].$$

Suponha que exista um algoritmo para testar se uma equação Diofantina possui soluções inteiras positivas, isto é, o algoritmo procurado pelo Décimo Problema de Hilbert. Então para x e n dados, este algoritmo poderia ser usado para testar se a equação

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

tem solução, isto é, se $x \in D_n$ ou não. Desse modo o algoritmo calcula a função $g(n, x)$. Uma vez que as funções recursivas são apenas aquelas para as quais existe um algoritmo de computação, $g(n, x)$ seria recursiva, mas isto contraria o Teorema 3.8. Logo o Décimo problema de Hilbert é insolúvel. ■

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.

3.6 Grau e Dimensão de um Conjunto Diofantino

É natural associar a cada conjunto Diofantino uma dimensão e um grau, isto é, a dimensão de S é o menor n para o qual o polinômio P existe para que :

$$S = \{x \mid \exists\ (y_1, \ldots, y_n)\ [P(x, y_1, \ldots, y_n) = 0]\}, \tag{3.2}$$

e o grau de S é o menor grau dos polinômios P satisfazendo a equação (3.2) (Permitindo que n seja tão grande quanto se queira).

Agora é fácil ver que:

Teorema 3.10 *Cada conjunto Diofantino tem grau menor ou igual a quatro.*

Demonstração.

O grau de P satisfazendo (3.2) pode ser reduzido através da introdução da variáveis adicionais z_j satisfazendo as equações da forma

$$\begin{aligned} z_j &= y_i y_k, \\ z_j &= y_i^2, \\ z_j &= x y_i^2, \\ z_j &= x^2. \end{aligned}$$

Por sucessivas substituições destas equações dentro de P, seu grau pode ser reduzido para 2.

Além disso, a equação é equivalente a um sistema de equações simultâneas de grau 2. Somando os quadrados obtemos uma equação de grau 4. ■

Um resultando interessante e surpreendente é dado pelo seguinte teorema:

Teorema 3.11 *Existe um inteiro m tal que todo conjunto Diofantino tem dimensão $\leq m$.*

Utilizando os argumentos vistos neste trabalho produziríamos um número em torno de 50, porém, Matiyacevic e Júlia Robinson mostraram que $m = 14$ é suficiente.

Um exemplo interessante é dado pela sequência de conjuntos Diofantinos

$$S_q = \{x \mid\ (\exists\ y_1, y_2, \ldots, y_q)\ [x = (y_1 + 1) \ldots (y_q + 1)]\}.$$

Para $q = 2$, o conjunto S_2 é formado pelos números naturais que podem ser escritos como produto de dois fatores maiores que 1, ou seja, S_2 é o conjunto de números compostos. Assim, S_3, seria o conjunto de números compostos com no mínimo três fatores primos (não necessariamente distintos). É interessante observar que pelo Teorema 3.11, o conjunto Diofantino S_q é de dimensão menor ou igual a 14, mesmo para grandes valores de q.

3.7 Conjuntos Recursivamente Enumeráveis

Neste capítulo enunciaremos um resultado que nos ajudará a decidir se um conjunto dado é ou não é Diofantino.

Definição 3.2 *Um conjunto S de n-uplas de inteiros positivos é chamado recursivamente enumerável, se existem funções recursivas $f(x, x_1, \ldots, x_n)$ e $g(x, x_1, \ldots, x_n)$ tais que:*

$$S = \{\langle x_1, \ldots, x_n\rangle \mid\ (\exists\ x)[f(x, x_1, \ldots, x_n)\ = g(x, x_1, \ldots, x_n)]\}.$$

Teorema 3.12 *Um conjunto S é Diofantino se, e somente se, é recursivamente enumerável.*

Demonstração.

Se S é Diofantino, existem polinômios P, Q com coeficientes inteiros e positivos tais que:

$$\begin{gathered}\langle x_1, \ldots, x_n\rangle \in S \\ \Leftrightarrow \\ (\exists\ y_1, y_2, \ldots, y_m)[\ P(x_1, \ldots, x_n,\ y_1, y_2, \ldots, y_m) = Q(x_1, \ldots, x_n,\ y_1, y_2, \ldots, y_m)] \\ \Leftrightarrow \\ (\exists\ u)\ [\ P(x_1, \ldots, x_n,\ S(1,u), \ldots, S(m,u)) = Q(x_1, \ldots, x_n,\ S(1,u), \ldots, S(m,u))],\end{gathered}$$

portanto S é recursivamente enumerável.

Reciprocamente, se S é recursivamente enumerável, então existem funções recursivas:

$$f(x, x_1, \ldots, x_n) \quad \text{e} \quad g(x, x_1, \ldots, x_n),$$

tais que:

$$\begin{gathered}\langle x_1, \ldots, x_n\rangle \in S \\ \Leftrightarrow \\ (\exists\ x)\ [f(x, x_1, \ldots, x_n)\ = g(x, x_1, \ldots, x_n)] \\ \Leftrightarrow \\ (\exists\ x, z)\ [z = f(x, x_1, \ldots, x_n)\ \wedge\ z = g(x, x_1, \ldots, x_n)].\end{gathered}$$

Então pelo Teorema 3.5, S é Diofantino. ■

Referências Bibliográficas

[1] Matiyasevich, Yuri, Hilbert's Tenth Problem, The MIT Press, London, 1993.

[2] Matiyasevich, Yuri, Enumerable sets are Diophantine(Russian), Dokl. Akad. Nauk SSSR,191(1970) 279-282.

[3] Matiyasevich, Yuri, Diophantine representation of enumerable predicates(Russian), Izv. Akad. Nauk SSSR. Ser. Mat.35(1971) 3-30.

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

[5] Santos, J.P.O., Introdução à Teoria de Números, Coleção Matemática Universitária, SBM., Rio de Janeiro, 2000.

[6] Landau, E.G.H., Teoria Elementar dos Números, Coleção Clássicos da Matemática, Editora Ciência Moderna, Rio de Janeiro, 2002.

[7] Burton, D.M., Elemetary Number Theory, Fifth Edition, McGraw-Hill Higher Education, 2002.

[8] Heath, T. L., Diophantos of Alexandria: A Study in the History of Greek Algebra, Cambridge: Cambridge University Press, 1885, 1910.

[9] Godel, Kurt, Uber formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme I,Monatsh. Math. und Physik, 38(1931) 173-198.

[10] Church, Alonzo, An unsolvable problem of elementary number theory. American Journal of Mathematics, 58:345-363.

[11] Turing, A.M., On computable numbers, whith an application to the Entscheidungsproblem.Proceedings of the London Mathematical Society. Second Series, 42(1936):230-265.

[12] Turing, A.M., On computable numbers, whith an application to the Entscheidungsproblem. A correction Proceedings of the London Mathematical Society. Second Series, 43(1937):544-546.

[13] Turing, A.M., Systems of logic based on ordinals. Proceedings of the London Mathematical Society. Second Series, 45(1939):161-228.

[14] Davis, Martin, Arithmetical problems and recursively enumerable predicates, J. Symbolic Logic, 18(1953):33-41

[15] Davis, Martin, Computability and Unsolvability, McGraw Hill, New York, 1958.

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

[17] Reid, Constance, Julia: A Life in Mathematics, The Mathematical Association of America, 1997.

[18] Robinson, Julia, Existential definability in arithmetic. Transactions of the American Mathematical Society, 72(3):437-449.

[19] Robinson, Julia, Diophantine decision problems.In W.J. LeVeque, editor, Studies in Number Theory, volume 6 of Studies in Mathematics, pages 76-116. Mathematical Association of America.

[20] Robinson, Julia, Hilbert's Tenth Problem. In 1969 Number Theory Institute, volume 20 of proceedings of Symposia in Pure Mathematics, pages 191-194, Providence, Rhode Island. American Mathematical Society.

[21] Jones, J.P., Sato, D., Wada, H. e Wiens, D., Diophantine representation of the set of prime numbers. Amer. Math. Monthly, 83. 1976, 449-464.

[22] Ribenboim, Paulo, Números Primos: Mistérios e Recordes. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2001.