Problemas Indecidíveis

Diana de Castro Lobo

Problemas Indecidíveis

Diana de Castro Lobo

Dissertação para a obtenção do Grau de **Mestre em Matemática**

Área de Especialização em **Computação**

Júri

Presidente:	Jorge Manuel Senos da Fonseca Picado
Orientador:	Alexander Kovacec
Vogal:	Olga Maria da Silva Azenhas

Data: Setembro de 2013

Resumo

Este trabalho pretende explicar tanto quanto possível em linguagem não excessivamente técnica o que se entende por um problema indecidível. De seguida, menciona o Problema da Correspondência de Post (PCP) que foi provado como sendo indecidível por Emil Post em 1936. Com base neste resultado, prova-se pormenorizadamente que a questão de se um semigrupo (sob multiplicação) formado por um conjunto finito de matrizes inteiras 3×3 contém a matriz nula é um problema indecidível. Na terceira e mais volumosa parte, a prova da indecibilidade do famoso décimo problema de Hilbert é apresentada com base na "simples" exposição de Martin Davis.

Palavras Chave: algoritmo, diofantina, indecidibilidade, mortalidade, recursividade

Abstract

This work aims to explain as far as possible what an unsolvable problem is, in a not exceedingly technical language. Next, the Post Correspondence Problem (PCP) is referred, a problem which was proved unsolvable by Emil Post in 1936. Based on this result, it is proved in detail that whether or not a finitely generated semigroup (under multiplication) of 3×3 integer matrices contains the null matrix is unsolvable. In the third and larger part, the proof of the unsolvability of Hilbert's famous tenth problem is presented, based on the "simple" exposition made by Martin Davis.

Keywords: algorithm, diophantine, mortality, recursivity, unsolvability

Agradecimentos

Em primeiro lugar não posso deixar de agradecer ao meu orientador, Alexander Kovacec, que muito me ensinou na Matemática para além do tema desta Dissertação e me apoiou ao longo do tempo em que a elaborei. Aos meus pais, o meu obrigado sincero por tudo o que fizeram por mim e pelas ferramentas que me deram e que fizeram de mim o que sou hoje. Espero um dia poder dar aos meus filhos uma pequena parcela do que me foi dado. À minha família, Hugo e Aline, avós, tios, primas: obrigada por me terem apoiado sempre, quando foi mais difícil para mim e por rirem comigo quando é mais fácil. Obrigada ao Jason e aos seus inesgotáveis conhecimentos de LaTeX, e ao Eduardo, fulcral nas minhas dúvidas pontuais da matemática que eu já não recordava. Obrigada aos que releram a minha tese à procura de gralhas, trabalho aborrecido e meritório, o João foi impecável nisso. Aos meus amigos que ao longo dos anos se mantêm a meu lado e nos meus momentos piores tentaram manter-se e manter-me à tona e me fazerem soltar gargalhadas, o meu muito obrigada. Obrigada Maria, Eduarda, Madalena, minhas Amoras, João, Pedro, André, Juliana, Rita, Carolina, Joana. Obrigada aos meus amigos de matemática, são para a vida. Obrigada às pessoas a quem agradeci nos rascunhos que fiz nas últimas semanas ao adormecer e que se calhar esqueci de pôr aqui. Por último, um obrigado especial à pessoa para quem eu devia ser o exemplo e, no fundo, acabou por o ser para mim, o meu irmão Diogo.

"I would thank you from the bottom of my heart, but for you my heart has no bottom. "

Autor desconhecido

A todos, obrigada.

Conteúdo

Capítulo 1

Introdução

1.1. O que é um problema indecidível?

Um dos grandes contributos da Lógica Moderna para o avanço da Matemática é a clarificação da noção intuitiva de "método efectivo" (ou "algoritmo") através de máquinas de Turing, ou conceitos essencialmente equivalentes como o cálculo lambda e funções recursivas, e a possibilidade de demonstrar que certos problemas como o "Décimo Problema" de Hilbert (Paris 1900) - conceber um método uniforme e efectivo que permita decidir para dada uma equação diofantina qualquer se ela tem ou não solução - são insolúveis (ou indecidíveis) no sentido pretendido. No presente trabalho vai mostrar-se também que a questão de se um semigrupo formado por um conjunto finito de matrizes inteiras 3×3 contém a matriz nula é um problema indecidível.

Para compreendermos o que se entende por "um problema indecidível" precisamos da noção de um "método efectivo" ou "algoritmo". Uma formalização rigorosa pode ser dada por uma "máquina de Turing"; no entanto, um exemplo bem conhecido é o "algoritmo euclideano" para calcular o máximo divisor comum de dois inteiros positivos m e n. Uma forma muito simples deste algoritmo é dado desta forma:

1. Se $m > n$: define $m := m - n$ e volta para 1.
2. Se $n > m$: define $n := n - m$ e volta para 1.
3. Se $m = n$ escreve 'o máximo divisor dos inteiros dados é m' e pára.

Se este algoritmo arrancar com $(18, 8)$, por exemplo, vai produzir sucessivamente os seguintes pares (m, n) de inteiros: $(18, 8), (10, 8), (2, 8), (2, 6), (2, 4), (2, 2)$; de seguida vai imprimir 2, e parar.

Este algoritmo, que de momento calcula uma função, pode ser convertido num algoritmo de decisão da coprimalidade de dois números inteiros m e n. Basta substituir a linha 3 por

3': Se $m = n = 1$ escreve 'os inteiros dados são primos entre si'.

3": Se $m = n \neq 1$ escreve 'os inteiros dados não são primos entre si'.

Existe então um algoritmo que permite decidir para todo o par de inteiros positivos se são ou não primos entre si. Diz-se que "O problema da coprimalidade é decidível". Mais geralmente, diz-se de uma forma sucinta - mas um pouco enganadora - que "um problema P é decidível" se existir um algoritmo que decida toda a instância do problema P.

De um algoritmo de decisão para um problema P exige-se que páre, seja qual for a instância do problema com que for "alimentado".

A "indecidibilidade de um problema P", que se provará à frente para certos problemas de números inteiros, afirma então a não-existência de um método mecânico que permita decidir todas as instâncias de P. É preciso, no entanto, ter presente que isto não impede que pelo menos certas instâncias do problema P possam ser decididas, normalmente por truques ou ideias particulares, típicas da mente humana e, por isso, não mecanizáveis.

Assim, ao dizer coisas como "a hipótese de Riemann sobre os zeros da função ζ pode ser não decidível" (já ouvida de bocas de matemáticos) a impressão deixada é de que não foi entendido o conceito da decidibilidade: a palavra "Indecidibilidade (de P)", como é aqui usada neste trabalho, expressa a impotência de resolver por um algoritmo (método efectivo ou mecânico) todas as instâncias de uma classe P de problemas; não diz nada sobre a solubilidade de um problema individual, quer por meio de um contra-exemplo, quer por uma prova tradicional.

De uma perspectiva "filosófica", em particular em linha com a "inteligência artificial" de que tanto se fala há já umas décadas, podemos dizer que a comprovada existência de problemas indecidíveis contribui de forma pessimista para o debate sobre se "ter ideias" é algo que possamos alguma vez esperar de computadores como os conhecemos; e se "ser inteligente" é algo que é programável. Este pessimismo no plano tecnológico, no entanto, é algo que deveria ser visto como positivo pela maior parte dos seres humanos. Ao ser humano não deveria agradar a perspectiva de ser um dia - também a nível intelectual - substituído por máquinas.

Na secção 2.1 define-se o Problema da Correspondência de Post e enuncia-se formalmente a sua indecidibilidade algorítmica, como base para a prova da indecidibilidade do problema da mortalidade em semigrupos matriciais. Já o capítulo 3 é dedicado exclusivamente ao décimo problema de Hilbert e à prova da sua indecidibilidade.

Capítulo 2

A Mortalidade em Semigrupos de Matrizes

2.1. O problema da correspondência de Post

Se A for um alfabeto (i.e. um conjunto de símbolos ditos "letras"), então define-se por A^* *linguagem* sobre A, ou seja, a família de todas as palavras com letras em A. Note-se que A^* forma naturalmente um semigrupo, sendo a operação binária '$\cdot$' sobre A^* simplesmente a concatenação de palavras: se todos os a_i, a'_j, com $i = 1, \ldots, k$, $j = 1, \ldots, k'$, são letras de A, então $a_1 a_2 \ldots a_k \cdot a'_1 a'_2 \ldots a'_{k'} = a_1 a_2 \ldots a_k a'_1 a'_2 \ldots a'_{k'}$, ou seja, a concatenação de palavras não será indicada por nenhum símbolo especial, mas simplesmente por justaposição.

Sejam então Σ^* e Δ^* semigrupos sobre os alfabetos Σ e Δ.

Um *morfismo* $h : \Sigma^* \to \Delta^*$ é uma aplicação tal que, para palavras $w_1, w_2 \in \Sigma^*$ quaisquer, se tem a equação $h(w_1 w_2) = h(w_1)h(w_2)$.

Então, uma *instância* do *Problema da Correspondência* de Post (PCP) é um par de morfismos (h, g), $h, g : \Sigma^* \to \Delta^*$. Diz-se que w é *solução* de (h, g) se $h(w) = g(w)$.

Teorema 1. O PCP é indecídivel, isto é, não há um método efectivo para, dada uma instância do PCP, decidir se esta tem solução. Na verdade, mesmo o caso particular do PCP em que Δ tem apenas duas letras é também indecidível.

Neste trabalho vamos assumir como conhecido este teorema, cuja prova se baseia em outros longos artigos de Alonzo Church sobre o cálculo lambda.

2.2. Mortalidade em semigrupos de matrizes inteiras 3×3

Um semigrupo $S = (S, \cdot)$ é *gerado* por um *conjunto gerador* $S' \subseteq S$ se todo o $s \in S$ pode ser escrito como produto na forma $s = s'_1 s'_2 \cdots s'_m$ com $s'_i \in S'$. S é *finitamente gerado* se existir um conjunto gerador finito.

Se escolhermos uma família finita de matrizes inteiras 3×3 qualquer e considerarmos todos os produtos matriciais, definimos desta forma um subsemigrupo finitamente gerado do semigrupo de matrizes inteiras 3×3. O semigrupo diz-se *mortal* se contiver a matriz nula.

Provar-se-á ao longo desta secção o seguinte teorema, que é o resultado principal deste capítulo:

Teorema 2. O problema da mortalidade de semigrupos de matrizes inteiras 3×3 é indecidível.

Por outras palavras, não existe um algoritmo que, dado um qualquer conjunto finito de matrizes $M_1, M_2, ..., M_n$, determine a existência de um conjunto de índices $i_1, \ldots, i_k$ tal que $M_{i_1}M_{i_2}\cdots M_{i_k} = 0$.

Para provarmos este teorema, comecemos por tomar como alfabetos Γ, Δ, com $\Gamma = \{a_1, a_2, a_3\}$ e $\Delta = \{a_1, a_2\}$ e definamos $\sigma : \Gamma^* \to \mathbb{N}$ por

$$\sigma(\text{palavra vazia}) = 0, \text{ e } \sigma(a_{i_1}\ldots a_{i_k}) = \sum_{j=1}^{k} i_j 3^{k-j}.$$

Em primeiro lugar, temos que

Lema. A função σ é injectiva.

Prova: Supondo que os valores de duas palavras em Σ^* sob a aplicação σ são iguais, chega-se a uma igualdade da forma $\sum_{j=1}^{k} i_j 3^{k-j} = \sum_{j=1}^{l} h_j 3^{l-j}$, com os $i_j, h_j \in \{1,2,3\}$. Sem perda de generalidade, podemos supor $k \geq l$. A igualdade pode ser então escrita na forma

$$0 = \sum_{s=0}^{k-1} i_{k-s}3^s - \sum_{s=0}^{l-1} h_{l-s}3^s = \sum_{s=l}^{k-1} i_{k-s}3^s + \sum_{s=0}^{l-1}(i_{k-s} - h_{l-s})3^s.$$

Ora, note-se que todo o $i_{k-s} - h_{l-s} \in \{-2, -1, 0, 1, 2\}$, pelo que o segundo somatório é em módulo menor ou igual a $\sum_{s=0}^{l-1} 2\cdot 3^s = 3^l - 1 < 3^l$. Se fosse $k-1 \geq l$, o primeiro somatório seria maior ou igual a 3^l. Por isso a soma não poderia ser nula. Logo $k = l$ e $\sum_{s=0}^{k-1}(i_{k-s} - 1)3^s = \sum_{s=0}^{k-1}(h_{k-s} - 1)3^s$. Temos assim aqui a igualdade de representações tri-ádicas. Esta implica que os coeficientes das potências 3^s sejam iguais, ou seja, $i_j = h_j$ para $j = 1, 2, ..., k$. □

Tomemos duas palavras $u = a_{i_1}\ldots a_{i_k}, v = a_{j_1}\ldots a_{j_l} (= a_{i_{k+1}}\ldots a_{i_{k+l}}) \in \Gamma^*$.

Tem-se

$$\begin{aligned}
\sigma(uv) &= \sigma(a_{i_1}\dots a_{i_k}a_{j_1}\dots a_{j_l}) \\
&= \sigma(a_{i_1}\dots a_{i_k}a_{i_{k+1}}\dots a_{i_{j+k}}) \\
&= \sum_{j=1}^{k+l} i_j 3^{k+l-j} \\
&= \sum_{j=1}^{k} i_j 3^{k+l-j} + \sum_{j=k+1}^{k+l} i_j 3^{k+l-j} \\
&= 3^l \sum_{j=1}^{k} i_j 3^{k-j} + \sum_{j=1}^{l} i_{j+k} 3^{l-j} = 3^{|v|}\sigma(u) + \sigma(v).
\end{aligned}$$

Portanto, para duas palavras u, v em Γ^*, $\sigma(uv) = 3^{|v|}\sigma(u) + \sigma(v)$.

Usemos a aplicação σ para definir $\gamma_1 : \Gamma^* \times \Gamma^* \to \mathbb{N}_0^{3\times 3}$ por

$$\gamma_1(u,v) = \begin{bmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{bmatrix}.$$

Esta aplicação que obtivemos tem a seguinte propriedade:

Lema. γ_1 é morfismo injectivo.

Prova: Por σ ser injectiva, γ_1 é injectiva. Ora calculamos

$$\begin{aligned}
\gamma_1(u_1,u_2,v_1,v_2) &= \begin{bmatrix} 3^{|u_1|+|u_2|} & 0 & 0 \\ 0 & 3^{|v_1|+|v_2|} & 0 \\ \sigma(u_1u_2) & \sigma(v_1v_2) & 1 \end{bmatrix} \\
&= \begin{bmatrix} 3^{|u_1|+|u_2|} & 0 & 0 \\ 0 & 3^{|v_1|+|v_2|} & 0 \\ 3^{|u_2|}\sigma(u_1)+\sigma(u_2) & 3^{|v_2|}\sigma(v_1)+\sigma(v_2) & 1 \end{bmatrix} \\
&= \begin{bmatrix} 3^{|u_1|} & 0 & 0 \\ 0 & 3^{|v_1|} & 0 \\ \sigma(u_1) & \sigma(v_1) & 1 \end{bmatrix} \begin{bmatrix} 3^{|u_2|} & 0 & 0 \\ 0 & 3^{|v_2|} & 0 \\ \sigma(u_2) & \sigma(v_2) & 1 \end{bmatrix} \\
&= \gamma_1(u_1,v_1)\gamma_1(u_2,v_2).
\end{aligned}$$

Mostrámos assim que $\gamma_1(u_1,u_2,v_1v_2) = \gamma_1(u_1,v_1)\gamma_1(u_2,v_2)$. Verifica-se então que γ_1 é também morfismo e, consequentemente, é um morfismo injectivo. □

Através das matrizes

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ e } A^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

definimos a aplicação γ por $\gamma : \Gamma^* \times \Gamma^* \ni (u, v) \overset{\gamma}{\mapsto} A\gamma_1(u, v)A^{-1} \in \mathbb{Z}^{3\times 3}$. É evidente que γ é morfismo injectivo.

Então, para $u, v \in \Gamma^*$, tem-se

$$\begin{aligned} \gamma(u,v) &= \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 3^{|u|+\sigma(u)} & \sigma(v) & 1 \\ 3^{|u|} & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 3^{|u|+\sigma(u)-\sigma(v)} & * & * \\ * & * & * \\ * & * & * \end{bmatrix} \end{aligned}$$

Em particular, obtém-se

$$(\gamma(u, v))_{11} = 3^{|u|} + \sigma(u) - \sigma(v) \ .$$

O Teorema que provaremos em seguida, uma versão simplificada do Teorema 2, fala apenas da posição $(1, 1)$ de uma matriz do semigrupo. Não obstante, este resultado é um passo importantíssimo para a conclusão do nosso resultado principal.

Teorema 3. O problema de se um semigrupo finitamente gerado de matrizes em $\mathbb{Z}^{3\times 3}$ conter uma matriz com a entrada $(1, 1)$ nula é indecidível.

Prova: Seja $\Sigma^* \overset{h,g}{\to} \Delta^*$ uma instância do PCP com $\Delta = \{a_2, a_3\}$. Para $a \in \Sigma$ definam-se as matrizes $N_a = \gamma(h(a), g(a))$ e $N'_a = \gamma(h(a), a_1 g(a))$ e seja S o semigrupo gerado por essas matrizes. Uma matriz $M \in S$ tem então a forma $M = M_{b_1} \cdots M_{b_n}$, com $M_{b_i} = N_{b_i}$ ou N'_{b_i}, e define uma palavra $w = b_1 \cdots b_n \in \Sigma^*$. Como γ é um morfismo, obtém-se

$$M = \gamma(h(b_1), \dot{g}(b_1)) \ldots \gamma(h(b_n), \dot{g}(b_n)) = \gamma(h(w), \dot{g}(b_1) \ldots \dot{g}(b_n))$$

onde cada $\dot{g}(b_i)$ é $g(b_i)$ ou $a_1 g(b_i)$ conforme se $M_{b_i} = N_{b_i}$ ou N'_{b_i}.

Pondo $v = \dot{g}(b_1) \cdots \dot{g}(b_n)$, notamos que $v \in \Gamma^* = (\{a_1\} \cup \Delta)^*$ e obtemos por (1),

$M_{11} = 3^{|h(w)|} + \sigma(h(w)) - \sigma(v) = \sigma(a_1 h(w)) - \sigma(v)$. Então, pela injectividade de σ, $M_{11} = 0 \iff a_1 h(w) = v$. Neste caso, como $h(w) \in \Delta^*$, v tem um a_1 só no início. Então, $v = a_1 g(b_1) \dots g(b_n) = a_1 g(w)$. Das duas representações de v tiramos a conclusão de que $h(w) = g(w)$, ou seja, w é solução da instância (h, g).

Reciprocamente, se w for solução desta instância, o argumento mostra como construir uma matriz $M \in S$ que tem $M_{11} = 0$.

Reflectindo sobre o que foi feito, concluímos: uma qualquer instância do PCP permite definir um semigrupo finitamente gerado de matrizes 3×3 com entradas inteiras; este semigrupo tem uma matriz M com entrada $(1, 1)$ nula sse a instância do PCP tem uma solução; portanto, se houvesse um método efectivo para resolver o problema do enunciado, ter-se-ia um método efectivo para resolver o PCP, que é indecidível. □

Lema. Seja S um semigrupo de matrizes inteiras 3×3 finitamente gerado, e seja R o semigrupo gerado por $S \cup \{B\}$, onde $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Então $0 \in R$ se e só se $M_{11} = 0$ para algum $M \in S$.

Prova: Por cálculo matricial elementar vê-se que para toda a matriz $M \in \mathbb{Z}^{3\times3}$, se tem $(BMB)_{ij} = \begin{cases} M_{11} & \text{se } (i,j) = (1,1) \\ 0 & \text{se } (i,j) \neq (1,1) \end{cases}$.

Se existir $M \in R$ tal que $M_{11} = 0$ então, naturalmente, $0 = BMB \in R$.

Por outro lado, notando que $B^2 = B$, se $0 \in R$, então, sem perda de generalidade, $0 = BM_1BM_2B \cdots BM_nB = (BM_1B)(BM_2B) \dots (BM_nB)$, com certas $M_i \in S$. Como resultado das observações acima, a entrada (1,1) desta matriz é o produto das entradas (1,1) dos factores: tem-se então

$$0 = (BM_1B)_{11}(BM_2B)_{11} \cdots (BM_nB)_{11} = (M_1)_{11} \cdots (M_n)_{11}.$$

Assim $(M_i)_{11} = 0$, para algum i. Ou seja, $0 \in R$ implica $M_{11} = 0$, para algum $M \in S$. □

Prova do teorema principal (**Teorema 2.**):

Se houvesse um método efectivo para decidir se a matriz nula pertence a um semigrupo finitamente gerado de matrizes inteiras 3×3, então, em particular, poder-se-ia decidir tal questão para o semigrupo R do lema anterior. Mas, por esse mesmo lema, ter-se-ia um método efectivo para decidir se S possui uma matriz com a entrada

$(1,1)$ nula que, pelo Teorema 3 é um problema indecidível. □

Capítulo 3

O Décimo Problema de Hilbert

Em 1900, no Congresso Internacional de Matemáticos, David Hilbert apresentou uma lista de problemas que ele achava de grande importância para a Matemática no início do século XX. Mais tarde, estendeu-a um pouco, obtendo uma lista que constava de 23 problemas em aberto e cuja análise levou a grandes desenvolvimentos em várias áreas. Neste momento, algumas das questões foram resolvidas, outras há que aguardam solução e ainda outras têm um enunciado algo vago: são antes incentivos para programas de investigação de que não se pode declarar de forma clara se já terminaram ou não.

Em interpretação moderna, com o seu décimo problema, Hilbert desejava saber se existiria um algoritmo que decidisse, dada uma equação diofantina qualquer, se esta teria ou não soluções inteiras. Esse problema provou-se indecidível por Matyasevic, em 1970, completando espaços em branco nas provas conjuntas de Julia Robinson, Martin Davis e Hilary Putnam.

De notar que uma solução definitivamente negativa só pode ser dada após clarificação da noção de um algoritmo. Nos tempos de Hilbert esta noção ainda não existia e será a razão pela qual nos termos originais a existência de um método para resolver equações não é posta em causa. O enunciado do décimo problema é o mais curto de todos:

"Dada uma equação diofantina com variáveis quaisquer e coeficientes inteiros: pede-se um método através do qual se pode decidir num número finito de passos se a equação é solúvel em números inteiros."

Notemos a diferença entre as formulações moderna e a de Hilbert: este fala de um método como dependente da equação, enquanto que na formulação mais exacta falamos de um método que dê para todas as equações.

3.1. Equações diofantinas

Uma **equação diofantina** (na sua forma normal) é uma equação polinomial da forma $P(x_1, \ldots, x_n) = 0$, sendo P um polinómio com coeficientes inteiros, em que para as incógnitas só se admitem valores inteiros.

Ao longo deste texto, admitimos apenas inteiros positivos como incógnitas.

O que veremos é que não existe um algoritmo que decida se uma equação diofantina tem soluções positivas. No entanto, tal é suficiente para responder à questão de Hilbert, devido ao Teorema de Lagrange. Este teorema diz que qualquer inteiro positivo pode ser escrito como soma de quatro quadrados perfeitos. Se houvesse um algoritmo de teste de soluções inteiras para equações diofantinas, poder-se-ia testar uma equação diofantina polinomial $P(x_1, \ldots, x_n) = 0$ em relação às suas soluções inteiras positivas, testando $\tilde{P}(p_1, \ldots, p_n, q_1, \ldots, q_n, r_1, \ldots, r_n, s_1, \ldots, s_n) = P(1+p_1^2+q_1^2+r_1^2+s_1^2, \ldots, 1+p_n^2+q_n^2+r_n^2+s_n^2)$ em relação às suas soluções inteiras.

(Nota: Aqui existem somas de cinco números por se quererem apenas inteiros positivos - o que não inclui o zero.)

Definição. Um subconjunto S de $\mathbb{N}^n$ diz-se **diofantino** se existir um polinómio $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$, onde m pode ser nulo, de coeficientes inteiros tal que $(x_1^*, \ldots, x_n^*) \in S$ se e só se existem inteiros positivos $y_1, \ldots, y_m$ tais que

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

Assim sendo, podemos escrever

$$(x_1^*, \ldots, x_n^*) \in S \Leftrightarrow \exists (y_1 \ldots, y_n)(P(x_1^*, \ldots, x_n^*, y_1, \ldots, y_m) = 0)$$

isto é,

$$S = \{(x_1^*, \ldots, x_n^*) : \exists (y_1 \ldots, y_n)(P(x_1^*, \ldots, x_n^*, y_1, \ldots, y_m) = 0)\}$$

Definição. Uma função f com n argumentos diz-se **diofantina** se o seu grafo for diofantino, isto é, se $\{(x1, \ldots, x_n) : y = f(x_1, \ldots, x_n)\}$ for um conjunto diofantino.

Ao longo deste trabalho daremos vários exemplos de funções e conjuntos diofantinos, sobretudo na secção 3.5. No entanto, uma função diofantina importante será deduzida a partir dos números triangulares:

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

Sendo $T(n)$ uma função crescente, para cada inteiro z há um único número não negativo n tal que $T(n) < z \leq T(n+1) = T(n) + n + 1$.

Isto significa que z é unicamente representável como sendo

$$z = T(n) + y, \text{ com } y \leq n + 1$$

ou, de forma equivalente,

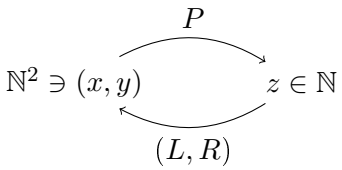
$$z = T(x + y - 2) + y, \text{ com } x, y \in \mathbb{Z}^+.$$

Assim sendo, escreve-se $x = L(z)$, $y = R(z)$ (respectivamente, **L**eft e **R**ight, como veremos a seguir) e $z = P(x, y)$.

Estas três funções L, R e P são diofantinas, já que:

$$\begin{aligned} z = P(x, y) &\Leftrightarrow 2z = (x + y - 2)(x - +y - 1) + 2y \\ x = L(z) &\Leftrightarrow (\exists y)[2z = (x + y - 2)(x - +y - 1) + 2y] \\ y = R(z) &\Leftrightarrow (\exists x)[2z = (x + y - 2)(x - +y - 1) + 2y]. \end{aligned}$$

Estas funções demonstram uma bijecção entre o conjunto dos pares de naturais e o próprio conjunto de naturais, isto é, P é uma função que transforma pares de $\mathbb{N}^2$ em elementos de $\mathbb{N}$. Por outro lado, cada elemento $z \in \mathbb{N}$ é mapeado num par de naturais $(L(z), R(z))$, respectivamente a parte esquerda e direita de z. Esquematicamente,



O que foi atrás descrito serve de prova ao seguinte

Teorema 1.1. Existem funções $P(x, y)$, $L(z)$ e $R(z)$ tais que

- para todo x, y, $L(P(x, y)) = x$ e $R(P(x, y)) = y$ e
- para todo z, $P(L(z), R(z)) = z$, $L(z)$, $R(z) \leq z$.

Eis uma tabela dos primeiros valores destas funções:

z	1	2	3	4	5	6	7	8	9	10
$L(z)$	1	2	1	3	2	1	4	3	2	1
$R(z)$	1	1	2	1	2	3	1	2	3	4

Outra função diofantina muito útil está relacionada com o Teorema Chinês dos Restos. Relembrando, este teorema diz-nos que para $a_1, \ldots, a_n$ inteiros positivos quaisquer e $m_1, \ldots, m_n$ tais que para $i \neq j$, m_i e m_j são primos entre si, existe x tal

que

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_n \bmod m_n \end{aligned}$$

Mais, o conjunto das soluções das congruências é dado por $x + m_1 m_2 \cdots m_n \mathbb{Z}$, de onde vemos que existe uma solução positiva.

Defina-se a função $\mathbb{N}^2 \ni (i,u) \stackrel{S}{\to} S(i,u) = w \in \mathbb{N}$, requerendo-se que w seja o único inteiro positivo tal que

$$\begin{aligned} w &\equiv L(u) \bmod 1 + iR(u) \\ w &\leq 1 + iR(u). \end{aligned}$$

Vemos então que w é o menor inteiro positivo que é resto da divisão inteira de $L(u)$ por $1 + iR(u)$.

Dado o que acabámos de descrever, podemos então provar o seguinte teorema.

Teorema 1.2. Existe uma função diofantina $S(i,u)$ tal que

- $S(i,u) \leq u$
- para cada sequência $a_1, \ldots, a_n$ existe um número u tal que

$$S(i,u) = a_i, \text{ para } 1 \leq i \leq n$$

Prova: Em primeiro lugar, vejamos que a função $S(i,u)$ como foi definida atrás é diofantina. Para isso, e como $x = L(u)$ e $y = R(u)$ é equivalente a $2u = (x+y-2)(x+y-1) + 2y$ (vide discussão do teorema anterior), $w = S(i,u)$ se e só se o seguinte sistema de equações tem solução em (x,y,z,v).

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

Podemos reescrever a primeira equação na forma $(2u-(x+y-2)(x+y-1)+2y)^2 = 0$ e proceder de forma análoga com as outras duas equações. As três equações têm solução sse a soma dos quadrados - que resulta num polinómio Q - tem a propriedade de que existam (x,y,z,v) tal que $Q(i,u,v,w,x,y,z) = 0$. (Este método será explicado mais detalhadamente na secção 3.4.) Isto mostra que S é diofantina.

Ora, a segunda equação (ou, mais correctamente, o segundo conjunto de equações - devido à iteração de i) demonstra que $S(i,u) \leq L(u)$ e, consequentemente, $S(i,u)$ é menor ou igual a u, tal como imposto pela primeira parte do teorema.

Seja então $a_1, \ldots, a_n$ uma sequência de números quaisquer. Escolha-se y como sendo maior que cada número da sequência e divísivel pelos naturais até n. Então os números $1+y, 1+2y, \ldots, 1+ny$ são dois a dois primos entre si (já que se $d|1+iy$ e $d|1+jy$, então $d|j-i$, $j > i$ e, portanto, $d \leq n-1$; mas nesse caso, $d|y$, logo, como $d|1+jy-jy$, $d=1$) e, assim sendo, o Teorema Chinês dos Restos pode ser aplicado para obter um número x tal que

$$\begin{aligned} x &\equiv a_1 \bmod 1+y \\ &\vdots \\ x &\equiv a_n \bmod 1+ny \end{aligned}$$

Faça-se $u = P(x,y)$ de modo a que $x = L(u)$ e $y = R(u)$. Então, para $i = 1, 2, \ldots, n$

$$a_i \equiv L(u) \bmod 1 + iR(u)$$

e $a_i < y = R(u) < 1 + iR(u)$. Mas então, por definição, $a_i = S(i,u)$. □

3.2. 24 lemas importantes

A indecidibilidade do décimo problema de Hilbert foi originalmente provada em dois passos. O primeiro foi tomado por Martin Davis, H. Putnam e Julia Robinson, ao usarem uma função exponencial para provar um certo teorema que envolvia conjuntos recursivamente enumeráveis. Neste trabalho, no entanto, não se enveredou por este caminho, optando-se antes pelas funções recursivas.

O segundo passo foi feito por Yuri Matijasevic ao provar que a função exponencial era ela própria diofantina. Em 1970, Matijasevic usou propriedades da sequência de números de Fibonacci para o fazer, mas, actualmente, propriedades das soluções da equação de Pell formam das provas mais simples de tal resultado.

A subclasse de equações de Pell que usámos é definida por

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geq 0 \\ d = a^2 - 1, & a > 0 \end{cases} \tag{3.1}$$

A descoberta de tal simplificação deve-se a Davis e Putnam. Note-se que a equação

tem as soluções imediatas:

$$x = 1; \quad y = 0$$
$$x = a; \quad y = 1.$$

Lema 2.1. Não há inteiros x, y (positivos, negativos ou nulos) satisfazendo a equação e tais que $1 < x + y\sqrt{d} < a + \sqrt{d}$.

Prova: Provemos este lema por redução ao absurdo: Suponhamos que o par (x, y) é solução inteira da equação de Pell. Então, $(x - y\sqrt{d})(x + y\sqrt{d}) = 1$. A mesma igualdade sucede com o par $(a, 1)$, uma das soluções que vimos inicialmente. Isto é, também $(a - \sqrt{d})(a + \sqrt{d}) = 1$.

Suponhamos que $1 < x + y\sqrt{d} < a + \sqrt{d}$, então, como $(x - y\sqrt{d})(x + y\sqrt{d}) = 1$, tem-se que $(x - y\sqrt{d}) < 1$, o que é equivalente a $-1 < -x + y\sqrt{d}$.

Da mesma forma, $x + y\sqrt{d} < a + \sqrt{d}$ leva a $-x + y\sqrt{d} < -a + \sqrt{d}$.

Somando as duas desigualdades,

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

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

Obtém-se $0 < 2y\sqrt{d} < 2\sqrt{d}$, i.e., $0 < y < 1$, o que é impossível pois y é inteiro. □

Definição De agora em diante, chamaremos uma *l-combinação* a uma expressão $x + y\sqrt{d}$ com x, y inteiros tais que $x^2 - dy^2 = 1$.

Vemos que o *conjugado* $x - y\sqrt{d} = x + (-y)\sqrt{d}$ de uma l-combinação é também l-combinação. Na verdade, no anel $\mathbb{Z}[\sqrt{d}]$ temos a factorização $(x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$.

Na prova do seguinte lema é claro que x, y são definidos de formas únicas por x_1, y_1, x_2, y_2.

Lema 2.2. O produto de l-combinações é ainda uma l-combinação.

Prova: Sejam $x_i + y_i\sqrt{d}$, $i = 1, 2$, l-combinações e $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})$. Para provar este lema precisamos de verificar que $x^2 - y^2 d = 1$.

Ora, $x - y\sqrt{d} = (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d})$. Isto porque, expandindo, $x + y\sqrt{d} =$

$x_1x_2+y_1y_2d^2+(x_1y_2+x_2y_1)\sqrt{d}$, donde $x-y\sqrt{d}=x_1x_2+y_1y_2d^2-(x_1y_2+x_2y_1)\sqrt{d}$ o que origina precisamente a desigualdade já escrita.

Temos então $(x^2-y^2d) = (x_1-y_1\sqrt{d})(x_2-y_2\sqrt{d})(x_1+y_1\sqrt{d})(x_2+y_2\sqrt{d})$, que podemos reorganizar como sendo $(x_1-y_1\sqrt{d})(x_1+y_1\sqrt{d})(x_2-y_2\sqrt{d})(x_2+y_2\sqrt{d})$. Como $x_i+y_i\sqrt{d}$ são l-combinações, $(x_i-y_i\sqrt{d})(x_i+y_i\sqrt{d})=1$, para $i=1,2$, e, daí, concluímos o que desejávamos: $x^2-y^2=1$. □

Recorde-se que $\mathbb{Q}[\sqrt{d}]$ é espaço vectorial sobre $\mathbb{Q}$ com base $\{1,\sqrt{d}\}$. Isto implica que o que vem a seguir está bem definido.

Definição Os inteiros $x_n(a),\ y_n(a)$ estão definidos (de forma única) para $n\geq 0$, $a>1$, por

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

Onde o contexto o permitir, a dependência de a não será explicitamente exibida, escrevendo-se apenas $x_n,\ y_n$.

Lema 2.3. As expressões $x_n+y_n\sqrt{d}$ são l-combinações.

Prova: Prove-se o lema 2.3 por indução:

Para $n=0$, $x_0+y_0\sqrt{d}=(a+\sqrt{d})^0=1$, donde se verifica o resultado. Suponhamos então que $x_n+y_n\sqrt{d}$ é l-combinação.

Então, usando que

$x_{n+1}+y_{n+1}\sqrt{d}=(a+\sqrt{d})^{n+1}=(a+\sqrt{d})^n(a+\sqrt{d})=(x_n+y_n\sqrt{d})(a+\sqrt{d})$, o facto de $(x_n+y_n\sqrt{d})$ ser uma l-combinação e $(a+\sqrt{d})$ ser outra, leva-nos a concluir, pelo lema 2.2, que $x_{n+1}+y_{n+1}\sqrt{d}$ é uma l-combinação. □

Lema 2.4. Seja $x,\ y$ uma solução não negativa de (3.1). Então existe algum n natural, tal que $x=x_n,\ y=y_n$.

Prova: Se $x=1, y=0$, o n procurado é 0. As outras soluções são tais que $x+y\sqrt{d}\neq 1$. Como $(a+\sqrt{d})>1$, $(a+\sqrt{d})^n$ tende para infinito, donde existe um n positivo único tal que $(a+\sqrt{d})^n\leq(x+y\sqrt{d})<(a+\sqrt{d})^{n+1}$.

Se a igualdade se verifica, o lema está provado. Se não, então $x_n+y_n\sqrt{d}<(x+$

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

Mas então, como $(x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = 1$, $(x_n - y_n\sqrt{d}) > 0$, e, assim sendo, $1 < (x_n - y_n\sqrt{d})(x + y\sqrt{d}) < (a + \sqrt{d})$.

Mas $(x_n - y_n\sqrt{d})(x + y\sqrt{d})$ é produto de l-combinações, portanto pelo lema 2.2 é l-combinação. Assim a desigualdade dupla contradiz o Lema 2.1. □

Lema 2.5. $x_{m\pm n} = x_m x_n \pm d y_m y_n$ e $y_{m\pm n} = x_n y_m \pm x_m y_n$, sendo no caso da subtração de indices $m \geq n$.

Prova: Este resultado sai facilmente da definição:

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

Daqui sai que

$$x_{m+n} = x_m x_n + d y_m y_n \text{ e } y_{m+n} = x_n y_m + x_m y_n.$$

Por outro lado, $x_m + y_m\sqrt{d} = (x_{m-n} + y_{m-n}\sqrt{d})(x_n + y_n\sqrt{d})$, portanto

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

Daqui obtém-se o pretendido. □

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

Em particular as funções $m \mapsto x_m$ e $m \mapsto y_m$ são crescentes.

Prova: Basta fazer $n = 1$ no lema anterior. As soluções de (3.1) para n=1 são $x_1 = a$ e $y_1 = 1$. □

Nota: A notação de (x, y) é usada para representar o máximo divisor comum entre x e y.

Lema 2.7. Tem-se $(x_n, y_n) = 1$

Prova: Se $k|x_n$ e $k|y_n$, então $k|(x_n^2 - d y_n^2)$, isto é, $k|1$. □

Lema 2.8. $y_n|y_{nk}$

Prova: Provemos este resultado por indução em k: Se $k = 0$, é óbvio que $y_n|0$.

Suponhamos então que $y_n|y_{nk}$, para qualquer k natural.

Então, por 2.5, $y_{n(k+1)} = y_{nk+n} = x_n y_{nk} + x_{nk} y_n$ que é, por hipótese de indução, divisível por y_n. □

Lema 2.9. $y_n|y_t$ se e só se $n|t$.

Prova: Segundo o lema anterior, bastará provar que se $y_n|y_t$ então $n|t$.

Suponhamos que t não é divisível por n, isto é, $t = nq + r$, com $0 < r < n$.

Então, $y_t = y_{nq+r} \overset{2.5}{=} x_r y_{nq} + x_{nq} y_r$.

Como $y_n|y_{nq}$, y_n terá de dividir também o segundo termo da soma, $x_{nq} y_r$. Mas $k = (x_{nq}, y_n) = 1$. (Se $k|y_n$, k irá dividir y_{nq} por lema 2.8. E como $k|x_{nq}$, pelo lema 2.7 é $k = 1$).

Então $y_n|y_r$. Mas isso é uma contradição, pois por r ser menor que n, $y_r < y_n$ por lema 2.6. □

Lema 2.10. $y_{nk} \equiv k x_n^{k-1} y_n \bmod (y_n)^3$.

Prova: Da definição vem que

$$\begin{aligned} x_{nk} + y_{nk}\sqrt{d} &= (a + \sqrt{d})^{nk} \\ &= (x_n + y_n\sqrt{d})^k \\ &= \textstyle\sum_{j=1}^{k} \binom{k}{j} x_n^{k-j} y_n^j (\sqrt{d})^j. \end{aligned}$$

Ou seja,

$$y_{nk} = \sum_{\substack{j=1 \\ j \text{ ímpar}}}^{k} \binom{k}{j} x_n^{k-j} y_n^j (\sqrt{d})^{j-1}$$

O termo associado a $j = 1$ nesta soma é $k x_n^{k-1} y_n$.

No entanto, y_n^3 divide todos os termos da soma associados a $j > 1$. Daí vem o resultado. □

Lema 2.11. $y_n^2|y_{n_{y_n}}$

Prova: Usando $k = y_n$ no lema anterior, $y_{ny_n} \overset{2.10}{\equiv} y_n^2 x_n^{y_n - 1} \bmod y_n^3$. Logo $y_n^2|y_{ny_n}$. □

Lema 2.12. Se $y_n^2|y_t$, então $y_n|t$.

Prova: Se $y_n^2|y_t$ então $y_n|y_t$ e, portanto, pelo lema 2.9, $n|t$. Seja então $t = nk$. Pelo lema 2.10, y_{nk} é congruente módulo $(y_n)^3$ com $kx_n^{k-1}y_n$ e, portanto, $y_n^2|kx_n^{k-1}y_n$, i.e., $y_n|kx_n^{k-1}$.

Mas, como $(y_n, x_n) = 1$, pelo lema 2.7, $y_n|k$, ou seja, $y_n|t$. □

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

Prova: Pelo lema 2.6,

$$y_{m+1} = ay_m + x_m \quad \text{e} \quad x_{m+1} = ax_m + dy_m$$
$$y_{m-1} = ay_m - x_m \quad \text{e} \quad x_{m-1} = ax_m - dy_m.$$

Então, $y_{m+1} + y_{m-1} = 2ay_m$ e $x_{m+1} + x_{m-1} = 2ax_m$. □

Estas equações, juntamente com os valores iniciais $x_0 = 1,\ x_1 = a,\ y_0 = 0,\ y_1 = 1$, determinam todos os valores de x_n, y_n. Muitas das propriedades à frente são provadas por indução, vendo que o resultado se verifica para os valores de $n = 0,\ 1$ e depois inferidas a partir de $n - 1, n$. Alguns exemplos importantes são apresentados em seguida:

Lema 2.14. Tem-se $y_n \equiv n \bmod a - 1$.

Prova: O resultado prova-se por indução em n : Se $n = 0$, $y_0 = 0$ e se $n = 1$, $y_1 = 1$, portanto a condição inicial é verificada. Suponhamos então que $y_n \equiv n \bmod a - 1$ para n e assumamos uma congruência similar para $n - 1$. Então,

$$\begin{aligned} y_{n+1} \overset{2.13}{=} 2ay_n - y_{n-1} &\equiv 2an - (n-1) \bmod a - 1 \\ &\equiv (2a-1)n + 1 \bmod a - 1 \\ &\equiv 2(a-1)n + n + 1 \bmod a - 1 \\ &\equiv n + 1 \bmod a - 1 \end{aligned}$$

□

Lema 2.15. Se $a \equiv b \bmod c$ então, para todo n, $x_n(a) \equiv x_n(b),\ y_n(a) \equiv y_n(b) \bmod c$.

Prova: Para $n = 0,\ 1$, os valores são iguais, portanto a condição é verificada.

Suponhamos que a afirmação é válida para n e $n-1$ em lugar de n.

$$\begin{aligned} y_{n+1}(a) &\overset{2.13}{=} 2ay_n(a) - y_{n-1}(a) \\ &\equiv 2by_n(b) - y_{n-1}(b) \bmod c \\ &\equiv y_{n+1}(b) \bmod c. \end{aligned}$$

Da mesma forma,

$$\begin{aligned} x_{n+1}(a) &\overset{2.13}{=} 2ax_n(a) - x_{n-1}(a) \\ &\equiv 2bx_n(b) - x_{n-1}(b) \bmod c \\ &\equiv x_{n+1}(b) \bmod c. \end{aligned}$$

□

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

Prova: Para $n = 0$ e $n = 1$ o lema verifica-se, visto que $y_0 = 0$ e $y_1 = 1$. Do lema 2.13 vem que $y_{n+1} = 2ay_n - y_{n-1}$ donde y_{n+1} e y_{n-1} têm a mesma paridade e, portanto, o resultado verifica-se. □

Lema 2.17. Seja $y \geq 1$ inteiro. Então $x_n(a) - y_n(a)(a-y) \equiv y^n \bmod 2ay - y^2 - 1$.

Prova: Primeiramente,

$$x_0 - y_0(a-y) = 1 \equiv y^0 \bmod 2ay - y^2 - 1,$$
$$x_1 - y_1(a-y) = a - a + y = y \equiv y^1 \bmod 2ay - y^2 - 1.$$

Portanto, o resultado é verificado para os valores iniciais de n. Suponhamos que se verifica para n e $n-1$ em lugar de n.

Provemos este lema por indução, usando o lema 2.13 (no que se segue '$\equiv$' significará sempre congruência módulo $2ay - y^2 - 1$):

$$\begin{aligned} x_{n+1} - y_{n+1}(a-y) &\overset{2.13}{=} 2ax_n - x_{n-1} - (2ay_n - y_{n-1})(a-y) \\ &= 2a(x_n - y_n(a-y)) - (x_{n-1} - y_{n-1}(a-y)) \\ &\equiv 2ay^n - y^{n-1} \\ &\equiv y^{n-1}(2ay - 1) \\ &\equiv y^{n-1}y^2 \\ &\equiv y^{n+1} \bmod 2ay - y^2 - 1 \end{aligned}$$

□

Lema 2.18. Para todo o n, $y_{n+1} > y_n \geq n$.

Prova: O lema 2.6 demonstra a primeira desigualdade. Use-se indução na segunda parte: $y_0 = 0$ e $y_1 = 1$ verificam a igualdade. Suponhamos que o resultado é válido para y_n, isto é, $y_n \geq n$. Como a é positivo e x_n e y_n percorrem todas as soluções não negativas da equação de Pell (pelo lema 2.4), então $y_{n+1} \overset{2.6}{=} ay_n + x_n \geq y_n + 1 \geq n+1$, o que prova o pretendido. □

Lema 2.19. Para todo o n, $x_{n+1}(a) > x_n(a) \geq a^n$, $x_n(a) \leq (2a)^n$.

Prova: Pelo lema 2.6, $x_{n+1} > x_n$ e pelo lema 2.13 $x_{n+1} = 2ax_n - x_{n-1}$, portanto, $ax_n \leq x_{n+1} \leq 2ax_n$. Por indução, prove-se que $a^n \leq x_n \leq (2a)^n$:

Para $x_0 = 1$ e $x_1 = a$ o resultado é obviamente válido. Consideremos então válida a hipótese de indução para n qualquer. Novamente pelo lema 2.13, $x_{n+1} = 2ax_n - x_{n-1} \leq 2a(2a)^n - a^{n-1} \leq (2a)^{n+1}$ e, por outro lado, $x_{n+1} \geq ax_n \geq aa^n = a^{n+1}$, o que prova o pretendido, por indução. □

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

Prova: Temos

$$\begin{aligned} x_{2n\pm j} &= x_{n+n\pm j} \\ &\overset{2.5}{=} x_n x_{n\pm j} + dy_n y_{n\pm j} \\ &\equiv dy_n y_{n\pm j} \bmod x_n \\ &\equiv dy_n(y_n x_j \pm x_n y_j) \bmod x_n \\ &\equiv dy_n^2 x_j \bmod x_n \\ &\equiv (x_n^2 - 1)x_j \bmod x_n \qquad \equiv -x_j \bmod x_n, \end{aligned}$$

onde no penúltimo passo usámos que $x_n^2 - dy_n^2 = 1$. □

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

Prova: Note-se que $4n \pm j = 2n + (2n \pm j)$. Então, usando o lema anterior a cada passo das congruências, temos $x_{4n\pm j} \overset{2.20}{\equiv} -x_{2n\pm j} \overset{2.20}{\equiv} x_j \bmod x_n$. □

Lema 2.22. Sejam $x_i \equiv x_j \bmod x_n$, com $i \leq j \leq 2n$ e $n > 0$. Então $i = j$, a não ser que a seja 2, n seja 1, i seja 0 e j seja 2, isto é, $(a, n, i, j) = (2, 1, 0, 2)$.

Prova: Suponhamos que x_n é ímpar e seja $q = \frac{x_n-1}{2}$. Os números $-q, -q+1, \ldots, -1, 0, 1, \ldots, q-1, q$, formam um conjunto completo de resíduos módulo x_n. Pelo lema 2.19,

$$1 = x_0 < x_1 < \cdots < x_{n-1}.$$

Usando o lema 2.6, $x_{n-1} \leq \frac{x_n}{a} \leq \frac{x_n}{2}$, portanto $x_{n-1} \leq q$. Mais ainda, observando que $n + k = 2n - (n - k)$, $k = 1, ..., n$, pelo lema 2.20, os números

$$x_{n+1}, x_{n+2}, \ldots, x_{2n-1}, x_{2n}$$

são congruentes módulo x_n, respectivamente, com

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

Então os números $x_0, x_1, \ldots, x_{2n}$ são incongruentes módulo x_n provando o lema no presente caso em que x_n é impar.

Suponhamos agora que x_n é par e seja $q = \frac{x_n}{2}$. Assim sendo, os números que formam um conjunto de resíduos módulo x_n são

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

(já que $-q \equiv q \bmod x_n$). Como anteriormente, $x_{n-1} \leq q$ e o resultado seguirá como antes, a não ser que $x_{n-1} = q = \frac{x_n}{2}$, de modo que $x_{n+1} \equiv -q \bmod x_n$, caso em que $i = n - 1$, $j = n + 1$ iria contradizer este resultado. Mas, pelo lema 2.6,

$$x_n = ax_{n-1} + dy_{n-1},$$

de modo que $x_n = 2x_{n-1}$ iria implicar $a = 2$, e $y_{n-1} = 0$, i.e, $n = 1$. Então este resultado falha apenas para $a = 2$, $n = 1$, $i = 0$ e $j = 2$. □

Lema 2.23. Sejam $x_i \equiv x_j \bmod x_n$, com $0 < i \leq n$, $0 \leq j < 4n$ e $n > 0$. Então ou $j = i$, ou $j = 4n - i$.

Prova: Suponhamos que $j \leq 2n$. Pelo Lema 2.22, $j = i$ a não ser que seja o caso especial referido no lema. Como $i > 0$, terá de ser $j = 0$, $n = 1$, $i = a = 2$. Mas então, $i = 2 > 1 = n$, o que é impossível, por hipótese.

Suponhamos então que $j > 2n$ e seja $j' = 4n - j$ de forma a que $0 < j' < 2n$. Neste caso, i e j são não nulos, logo não pode surgir a excepção do lema 2.22, o que implica que se tenha $i = j'$, donde se conclui o lema 2.23. □

Lema 2.24. Se $0 < i \leq n$ e $x_j \equiv x_i \bmod x_n$, então $j \equiv \pm i \bmod 4n$.

Prova: Faça-se $j = 4nq + j'$, com $0 \leq j' < 4n$. Pelo lema 2.21, $x_{j'} \equiv x_j \equiv x_i \bmod x_n$. Então, pelo lema 2.23, $j' = i$ ou $j \equiv j' \equiv i \bmod x_n$.

3.3. A função exponencial

Considere-se 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)	$t = k + 4(d-1)y$
$(VIII)$	$y = k + e - 1$

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

Prova: Suponhamos que há uma solução do sistema $I - VIII$. Por V, $b > a > 1$. Então, I, II, III, pelo lema 2.4, implicam a existência de i, j, n positivos tais que

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

Por IV, $y \leq v$, portanto $i \leq n$. As congruências

$$b \equiv a \bmod x_n(a), \quad x_j(b) \equiv x_i(a) \bmod x_n(a)$$

são consequência das equações V e VI e, pelo lema 2.15, obtém-se

$$x_j(b) \equiv x_j(a) \bmod x_n(a)$$

portanto,

$$x_i(a) \equiv x_j(a) \bmod x_n(a).$$

Pelo lema 2.24,

$$j \equiv \pm i \bmod 4n. \tag{3.2}$$

Pela equação IV, $y_i(a)^2 | y_n(a)$, o que, pelo lema 2.12, implica que $y_i(a) | n$, o que, por (3.2) leva a

$$j \equiv \pm i \bmod 4y_i(a). \tag{3.3}$$

Pela equação V, $b \equiv 1 \bmod 4y_i(a)$, o que, pelo lema 2.14, leva a

$$y_j(b) \equiv j \bmod 4y_i(a). \tag{3.4}$$

Devido a VII,

$$y_j(b) \equiv k \bmod 4y_i(a). \tag{3.5}$$

Combinando agora (3.3), (3.4), (3.5), obtém-se

$$k \equiv \pm i \bmod 4y_i(a). \tag{3.6}$$

Pela equação $VIII$, $k \leq y_i(a)$ e, pelo lema 2.18 o mesmo acontece a i, pois $i \leq y_i(a)$.

Como os números $-2y+1, -2y+2 \cdots -1, 0, 1, \ldots, 2y$ formam um conjunto completo de resíduos módulo $4y = 4y_i(a)$, as duas desigualdades anteriores, juntamente com (3.6), implicam a igualdade entre k e i, ou seja, $x = x_i(a) = x_k(a)$, que é que queríamos provar.

Para provar a implicação recíproca, seja $x = x_k(a)$. Faça-se $y = y_k(a)$ de modo a que I se verifique. Seja $m = 2ky_k(a)$ e $u = x_m(a),\ v = y_m(a)$. Assim, a equação II é satisfeita. Pelos lemas 2.9 e 2.11, $y^2|v$. Então basta escolher r de modo a que IV seja verdadeira. Adicionalmente, pelo lema 2.16, v é par portanto u é ímpar. Pelo lema 2.7, $(u, v) = 1$ e, sendo d' um divisor primo de u e $4y$, $d'|y$, pois u é impar e, nesse caso, d' dividiria v, pois $y|v$. Consequentemente, $(u, 4y) = 1$. Assim sendo, pelo Teorema Chinês dos Restos, existe b_0 tal que

$$\begin{aligned} b_0 &\equiv \ \ 1 \bmod 4y \\ b_0 &\equiv \ \ a \bmod u. \end{aligned}$$

Ora $b_0 + 4juy$ é também solução das duas congruências e portanto a equação V fica satisfeita, encontrando-se b, p e q adequados. Para satisfazer a equação III basta fazer $s = x_k(b),\ t = y_k(b)$. Como $b > a$ por V, $s = x_k(b) > x_k(a) = x$. Pelo lema 2.15 e usando V, $s \equiv x \bmod u$, portanto c pode ser escolhido para satisfazer VI. Pelo lema 2.18, $t \geq k$ e pelo lema 2.14, $t \equiv k \bmod b - 1$, o que leva, usando V, a $t \equiv k \bmod 4y$. Assim sendo, d pode ser encontrado de forma a que VII seja verdadeira. Novamente pelo lema 2.18, $y \geq k$, portanto $VIII$ pode ser satisfeita fazendo $e = y - k + 1$. □

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

Prova: Basta juntar ao sistema $I - VIII$ a equação $a = z + 1$. Pelo Teorema, o sistema $I - VIII$ com esta nova equação tem solução se e só se $x = x_k(a) = g(z, k)$.

Assim sendo, uma definição diofantina de g pode ser obtida com o truque já referido de somar quadrados de polinómios (neste caso, nove polinómios). □

Lema 3.2. Se $a > y^k$, então $2ay - y^2 - 1 > y^k$.

Prova: Seja $g(y) = 2ay - y^2 - 1$. Como a é um inteiro maior que 1, $a \geq 2$, logo $g(1) = 2a - 2 \geq a$. Para $1 \leq y < a$, $g'(y) = 2a - 2y > 0$, portanto g é crescente nesse intervalo. Então $g(y) \geq a,\ y < a$. Então, para $y \leq y^k < a$, $y^k < a \leq 2ay - y^2 - 1$. □

Estamos agora em posição de provar o teorema principal desta secção:

Teorema 3.3 A função exponencial $h(n,k) = n^k$ é diofantina.

Para tal, adicionem-se ao sistema $I - VIII$ as seguintes equações:

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

(X) $\quad m + g = 2an - n^2 - 1$

(XI) $\quad w = n + h = k + l$

(XII) $\quad a^2 - (w^2 - 1)(w-1)^2 z^2 = 1$

O Teorema 3.3 decorre directamente de

Lema 3.4. $m = n^k$ se e só se as equações $I - XII$ têm solução nos restantes argumentos.

Prova: Em primeiro lugar, suponhamos que o sistema de equações $I - XII$ se verifica. Por XI, $w > 1$, logo $(w-1)z > 0$ e, por XII, $a > 1$ $(a^2 - 1 > 0)$. Então pode aplicar-se o Teorema 3.1 e tem-se $x = x_k(a),\ y = y_k(a)$.

Por IX e pelo lema 2.17, $m \equiv n^k \bmod 2an - n^2 - 1$.

A equação XI indica que $k, n < w$. A partir de XII (usando lema 2.4), para algum j, $a = x_j(w)$, $(w-1)z = y_j(w)$ e, portanto, pelo lema 2.14, $(w-1)z \equiv j \bmod w - 1, \bmod 4n$ ou seja,

$$j \equiv 0 \bmod w - 1$$

de modo que $j \geq w - 1$. Assim sendo, pelo lema 2.19,

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

logo por lema 3.2, $n^k < 2an - n^2 - 1$. Pela equação X, $m < 2an - n^2 - 1$ e, como m e n^k são congruentes módulo $2an - n^2 - 1$ e ambos menores que esse valor, terão de ser iguais, o que prova a implicação '$\Leftarrow$' do lema.

Por outro lado, suponhamos que $m = n^k$. Será necessário encontrar soluções para

os argumentos do sistema $I - XII$. Escolha-se qualquer número w tal que $w > n, k$. Faça-se $a = x_{w-1}(w)$ de modo a que $a > n^k$ (veja-se o argumento acima). Pelo lema 2.14, $y_{w-1}(w) \equiv 0 \bmod w - 1$. Assim, pode escrever-se $y_{w-1}(w) = z(w-1)$, satisfazendo XII. Para satisfazer XI, faça-se $h = w - n$, $l = w - k$. Ainda se tem a maior que n^k e, portanto, pelo lema 3.2, $m = n^k < 2ay - y^2 - 1$, satisfazendo X. Fazendo $x = x_k(a)$, $y = y_k(a)$, $I - VIII$ são satisfeitas pelo Teorema 3.1. Resta apenas a equação IX, mas para esse fim, o lema 2.17 permite definir f de modo a que $x - y(a-n) - m = \pm(f-1)(2an - n^2 - 1)$ e, portanto, IX é satisfeita. Para finalizar, o Teorema 3.1 permite satisfazer $I - VIII$. □

3.4. A linguagem de predicados diofantinos

3.4.1. Os conectivos lógicos "e" e "ou"

Depois de provar, na última secção, que a função exponencial é diofantina, outras funções diofantinas podem ser deduzidas a partir desta. É disto exemplo a função $h(u, v, w) = u^{v^w}$.

Emprestando o símbolo lógico "$\wedge$" para "e", é fácil de comprovar que h é diofantina a partir da equivalência $(y = u^{v^w}) \Leftrightarrow (\exists z)(y = u^z \wedge z = v^w)$:

usando o Teorema 3.3, existe um polinómio P tal que

$$\begin{aligned} (y = u^z) &\Leftrightarrow (\exists r_1, \ldots, r_n)(P(y, u, z, r_1, \ldots, r_n) = 0), \\ \text{e } (z = v^w) &\Leftrightarrow (\exists t_1, \ldots, t_n)(P(z, v, z, t_1, \ldots, t_n) = 0). \end{aligned}$$

Então,

$$y = u^{v^w} \Leftrightarrow (\exists z, r_1 \ldots, r_n, t_1, \ldots, t_n)(P^2(y, u, z, r_1, \ldots, r_n) + P^2(z, v, w, t_1, \ldots, t_n) = 0).$$

Note-se que este procedimento pode ser estendido a quaisquer expressões já tidas como conjuntos diofantinos, combinando com os conectivos lógicos "e" e "ou" ou "existe" e originando novos conjuntos diofantinos (os quais são também chamados de *predicados diofantinos*). O conectivo "ou", "$\vee$", também é permitido nesta linguagem pois

$$(\exists r_1, \ldots, r_n)(P_1 = 0) \vee (\exists t_1, \ldots, t_m)(P_2 = 0) \Leftrightarrow (\exists r_1, \ldots, r_n, t_1, \ldots, t_m)(P_1 P_2 = 0).$$

Passemos então ao resultado mais importante desta secção:

Teorema 4.1. As seguintes três funções são diofantinas:

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

Nota: a notação de $\lfloor r \rfloor$, onde r é real, será usada para representar o maior inteiro contido em r, isto é, $\lfloor r \rfloor$ é o único inteiro tal que $\lfloor r \rfloor \leq r < \lfloor r \rfloor + 1$.

Lema 4.1. Para $0 < k \leq n$, $2^n < u$

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

Prova: $\frac{(u+1)^n}{u^k}$ é igual a $\sum_{i=0}^{n} \binom{n}{i} u^{i-k}$. Separemos este somatório em duas partes, de 0 a $k-1$ e de k a n:

Então,

$$\sum_{i=0}^{n} \binom{n}{i} u^{i-k} = S + R$$

onde

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

S é obviamente inteiro, pois k é um inteiro menor ou igual a n e, portanto, u^{i-k} é múltiplo de u. Por outro lado, $\frac{u^i}{u^k} < \frac{1}{u}$, para $i = 0, 1, \ldots, k-1$, ou seja,

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

pois, por hipótese, $u > 2^n$. Então, $R < 1$.

Concluindo, $\frac{(u+1)^n}{u^k} = S + R$, com $R < 1$ e S inteiro, donde $S \leq \frac{(u+1)^n}{u^k} < S + 1$, ou seja,

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

□

Lema 4.3. A função $f(n,k) = \binom{n}{k}$ é diofantina.

Prova: Temos $S = \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k} \equiv_u \binom{n}{k}$, uma vez que no somatório $i > k$. Como $\binom{n}{k} \leq \sum_{i=0}^{n} \binom{n}{i} = 2^n < u$, $\binom{n}{k}$ é o único inteiro positivo, menor que u e congruente

com $\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor$ módulo u. Assim sendo, temos a seguinte equivalência:

$$f = \binom{n}{k} \Leftrightarrow (\exists u, v, w)(v = 2^n \ \wedge \ u > v \wedge w = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \wedge f \equiv w \bmod u \wedge f < u).$$

Pelo que foi referido no início desta secção acerca de predicados diofantinos, para ver que $\binom{n}{k}$ é diofantina, basta vermos que cada uma das expressões separadas pelo símbolo lógico da conjugação é diofantina. Faremos isso de seguida.

Graças ao Teorema 3.3, sabemos que $v = 2^n$ é diofantina: numa representação polinomial que testemunhe que a relação $v = m^n$ é diofantina faça-se $m = 2$. Obtem-se uma representação que testemunha que $v = 2^n$ é diofantina. A relação $u > v$ é obviamente diofantina, já que $u > v$ é equivalente a existir x tal que $u = v + x$. Assim sendo, restam as expressões $w = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor$, $f < u$ e $f \equiv w \bmod u$. Ora,

$$((f \equiv w \bmod u) \wedge (f < u)) \Leftrightarrow ((\exists y, z)(w = f + yu) \wedge (f + z = u))$$

é uma equivalência que vem comprovar que as duas últimas expressões são diofantinas.

Por último, temos que $w = \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor$ é equivalente à existência de inteiros r, s, t tais que $((u + 1 = r) \wedge (u^k = s) \wedge (r^n = t) \wedge (ws \leq t < (w + 1)s))$; isto porque $ws \leq t < (w+1)s$ é equivalente a $w \leq \frac{t}{s} < w + 1$, ou melhor, a $w \leq \frac{(u+1)^n}{u^k} < w + 1$.

□

Lema 4.4 Se $r > (2x)^{x+1}$, então

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

Prova: Tomemos $r > (2x)^{x+1}$. Sabemos que

$$\begin{aligned} \frac{r^x}{\binom{r}{x}} = \frac{r^x x!}{r(r-1)\cdots(r-x+1)} &= x! \frac{r}{r} \frac{r}{r-1} \cdots \frac{r}{r-x+1} \\ &= x! \frac{1}{(1-\frac{1}{r})\cdots(1-\frac{x-1}{r})} < x! \frac{1}{(1-\frac{x}{r})^x} \end{aligned}$$

ou seja, $x! < \frac{r^x}{\binom{r}{x}} < x! \frac{1}{(1-\frac{x}{r})^x}$. Precisamos mostrar que $\frac{r^x}{\binom{r}{x}} < x! + 1$.

Como $\frac{x}{r} < 1$, da expansão da série geométrica obtemos

$$\begin{aligned} \frac{1}{1-\frac{x}{r}} &= 1 + \frac{x}{r} + \left(\frac{x}{r}\right)^2 + \cdots \\ &= 1 + \frac{x}{r}(1 + \frac{x}{r} + \left(\frac{x}{r}\right)^2 + \cdots) \\ &\overset{(r>2x)}{<} 1 + \frac{x}{r}(1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \cdots) \\ &= 1 + \frac{2x}{r}. \end{aligned}$$

Portanto,

$$\begin{aligned}\frac{1}{(1-\frac{x}{r})^x} &< (1+\tfrac{2x}{r})^x \\ &= \sum_{i=0}^{x}\tbinom{x}{i}(\tfrac{2x}{r})^i \\ &= 1+\sum_{i=1}^{x}\tbinom{x}{i}(\tfrac{2x}{r})^i \\ &< 1+\tfrac{2x}{r}\sum_{i=1}^{x}\tbinom{x}{i} \quad < 1+\tfrac{2x}{r}2^x.\end{aligned}$$

Ora, como $\frac{r^x}{\binom{r}{x}}$ era menor que $x!\frac{1}{(1-\frac{x}{r})^x}$, temos agora que

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

Como, por hipótese, temos $(2x)^{x+1} < r$, resulta que $\frac{r^x}{\binom{r}{x}} < x! + 1$, e assim podemos concluir que

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

□

Lema 4.5. A função $g(n) = n!$ é uma função diofantina.

Prova: A seguinte equivalência provará que $n!$ é uma função diofantina por aquilo que vimos no lema anterior e pelo facto de a conjunção de predicados diofantinos ser diofantina:

$$\begin{aligned}(g = n!) \Leftrightarrow [(\exists r,x,y,z)(z = n+1) \wedge (r > (2n)^z) \wedge (r^n = x) \wedge (\tbinom{r}{n} = y) \\ \wedge (gy \leq x < (g+1)y)].\end{aligned}$$

□

Lema 4.6. Seja $bq \equiv a \bmod M$. Então para todo o inteiro positivo y,

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

Prova: Expandindo parte do segundo membro da congruência, $b^y y!\binom{q+y}{y}$, obtemos $b^y(q+y)(q+y-1)\cdots(q+1) = (bq+yb)(bq+(y-1)b)\cdots(bq+b)$, que é congruente, por hipótese, a $(a+yb)(a+(y-1)b)\cdots(a+b) \bmod M$. Como são y termos, temos então o pretendido: $\prod_{k=1}^{y}(a+bk) \equiv b^y y!\binom{q+y}{y} \bmod M$. □

Resta então provar o último resultado desta secção:

Lema 4.7. A função $h(a,b,y) = \prod_{k=1}^{y}(a+bk)$ é uma função diofantina.

Prova: No lema 4.6, escolhemos $M = b(a+by)^y+1$. Então, o máximo divisor comum entre M e b será 1 e M será maior que $\prod_{k=1}^{y}(a+bk)$. Desta forma, a congruência

$bq \equiv a \bmod M$ terá solução em q e podemos determinar $\prod_{k=1}^{y}(a+bk)$ como sendo o único inteiro (positivo) congruente com $b^y y!\binom{q+y}{y} \bmod M$ que é menor que M, isto é, podemos definir a seguinte equivalência

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

que vem comprovar que h é diofantina, usando as expressões usadas nos anteriores lemas para a função factorial e para o coeficiente binomial. □

O Teorema 4.1 fica então provado com o que demonstrámos nas provas dos lemas 4.3, 4.5 e 4.7.

3.4.2. Quantificadores limitados

Na secção anterior vimos como o uso dos conectivos lógicos "e" e "ou" e da existência é permitido no âmbito da linguagem dos predicados diofantinos. No entanto, existem outros operadores e conectivos lógicos, também usados no contexto do estudo da lógica matemática como a *negação* de uma fórmula, o quantificador *universal* ("$\forall$") e o conectivo de *implicação* ($\rightarrow$) que podem gerar expressões que definem conjuntos que não serão diofantinos.

Não obstante, podemos definir *quantificadores limitados*, tanto existenciais como universais, que podem ser anexados à linguagem de predicados diofantinos, estendendo-a, mas mantendo-a, ainda, como uma linguagem de predicados diofantinos. Definamos então o **quantificador existencial limitado**

$$((\exists x)_{\leq y} \ldots) \text{ como sendo } (\exists x)((x \leq y) \wedge \ldots)$$

e o **quantificador universal limitado**

$$((\forall x)_{\leq y} \ldots) \text{ como sendo } (\forall x)((x > y) \vee \ldots).$$

Assim sendo, o que foi dito previamente pode ser resumido neste Teorema:

Teorema 4.2 Se P for um polinómio, os conjuntos

$$R = \{(y, x_1, \ldots, x_n) | (\exists z)_{\leq y} (\exists y_1, \ldots, y_m)(P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0)\} \text{ e}$$

$$S = \{(y, x_1, \ldots, x_n) | (\forall z)_{\leq y} (\exists y_1, \ldots, y_m)(P(y, z, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0)\}$$

são diofantinos.

Que R é um conjunto diofantino decorre imediatamente da equivalência

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

O segundo conjunto precisa da ajuda de dois lemas.

Lema 4.8 A seguinte equivalência é verdadeira:

$$\begin{gathered}\big((\forall k)_{\leq y}(\exists y_1, \ldots, y_m)(P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0)\big) \\ \Updownarrow \\ \big((\exists u)(\forall k)_{\leq y}(\exists y_1, \ldots, y_m)_{\leq u}(P(y, k, x_1, \ldots, x_n, y_1, \ldots, y_m) = 0)\big)\end{gathered}$$

Prova: Que o lado direito da equivalência implica o esquerdo é trivialmente demonstrado: pois se em particular existem elementos $y_1, \ldots, y_m$ menores que u que verificam a equação, então também existem elementos que não tenham obrigatoriamente que verificar essa condição (embora o possam fazer). Todos os outros valores se mantêm de um membro para o outro.

Provemos então a segunda parte da equivalência, i.e. a implicação '$\Downarrow$':

Suponhamos que o primeiro membro da equivalência é válido para dados $y, x_1, \ldots, x_n$. Então, iterando k de 1 até y, existem números bem definidos $y_1^{(k)}, \ldots, y_m^{(k)}$ para os quais $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) = 0$ se verifica. Tomando u como sendo o maior de todos esses $y_i^{(k)}$, isto é,

$$u = \text{ máx } \{y_i^{(k)} | i = 1, \ldots, n, k = 1, \ldots, y\},$$

a implicação no sentido pretendido é também verdadeira. □

O próximo lema, embora pareça transformar uma expressão simples numa bastante mais complexa, tem o objectivo de libertar a primeira de quantificadores limitados. Com esse propósito:

Lema 4.9. Seja P um polinómio em $m + n + 2$ variáveis e $Q(y, u, x_1, \ldots, x_n)$ um polinómio com as seguintes 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 $y_1, \ldots, y_m \leq u$ implicam que

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

Então

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

$$\Updownarrow$$

$$(\exists c,t,a_1,\ldots,a_m)\big((1{+}ct=\prod_{k=1}^{y}(1{+}kt))\wedge(t=Q(y,u,x_1,\ldots,x_n)!)\wedge((1{+}ct)|\prod_{j=1}^{u}(a_1{-}j))$$

$$\wedge\cdots\wedge((1+ct)|\prod_{j=1}^{u}(a_m-j))\wedge(P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)\equiv 0 \bmod 1+ct)\big)$$

Prova: Vejamos que, nas condições do lema, o segundo membro da equivalência implica o primeiro membro: tomemos p_k, para $k=1,2,\ldots,y$, como sendo um factor primo de $1+kt$ e seja $y_i^{(k)}$ o resto da divisão inteira de a_i por p_k $(i=1,2,\ldots,m,k=1,2,\ldots,y)$. Provaremos que

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

b)$P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})=0$, o que conclui esta parte da demonstração.

Como $p_k|1+kt$, que, por sua vez, divide $1+ct$, e como, por outro lado, temos que $1+ct|\prod_{j=1}^{u}(a_i-j)$, podemos afirmar que $p_k|\prod_{j=1}^{u}(a_i-j)$. Dado que p_k é primo, p_k divide a_i-j, para algum $j=1,2,\ldots,u$. O que isto significa é que $a_i\equiv j\equiv y_i^{(k)} \bmod p_k$.

Ora, tendo em conta que $t=Q(y,u,x_1,\ldots,x_n)!$, podemos dizer que cada divisor de $1+kt$ será maior que $Q(y,u,x_1,\ldots,x_n)$(todos os números menores que Q dividem kt e, portanto, não podem dividir $1+kt$). Então, $p_k>Q(y,u,x_1,\ldots,x_n)$ e, pela propriedade 1, $p_k>u$. Como j itera nos naturais até u, obviamente que $j\leq u<p_k$ e, como $y_i^{(k)}$ é o *resto da divisão inteira* de a_i por p_k tem-se $y_i^{(k)}<p_k$. Portanto

$$y_i^{(k)}=j \text{ logo } 1\leq y_i^{(k)}\leq u.$$

Em relação à segunda parte a provar, a alínea b), comecemos por ver que $1+ct$ e $1+kt$ são obviamente congruentes módulo p_k (pois são divisíveis por este valor), donde

$$k+kct\equiv c+ckt \bmod pk, \text{ isto é, } k\equiv c \bmod p_k.$$

Como já vimos, na alínea anterior, que $a_i\equiv y_i^{(k)} \bmod p_k$, então

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

ou seja, $P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})$ é divisível por p_k. Mas, pela propriedade 3, sabemos que $|P(y,k,x_1,\ldots,x_n,y_1^{(k)},\ldots,y_m^{(k)})|$ é menor ou igual a Q que, por sua

vez, é menor que p_k. Então, destes dois últimos resultados, o polinómio P nestas variáveis é divisível por p_k e menor, em módulo, que p_k, o que limita o seu valor a 0, como desejávamos.

Provemos agora a segunda parte da implicação ($\Downarrow$):

Para cada $k = 1, 2 \ldots, y$, suponhamos que $P(y, k, x_1, \ldots, x_n, y_1^{(k)}, \ldots, y_m^{(k)}) = 0$, onde cada $y_i^{(k)} \leq u$. Façamos $t = Q(y, u, x_1, \ldots, x_n)!$ e, dado que $\prod_{k=1}^{y}(1 + kt) \equiv 1 \bmod t$, é possível achar c tal que $1 + ct = \prod_{k=1}^{y}(1 + kt)$. Temos já, então, c e t nas condições pretendidas.

Vejamos então que os números $1 + kt$ formam uma sequência admissível de módulos para que o Teorema Chinês dos Restos se possa aplicar. Tomemos k e l tais que $1 \leq k < l \leq y$ e provemos que $(1 + kt, 1 + lt) = 1$:

Seja d divisor de $1+kt$ e $1+lt$. Então $d|(l-k)$ e, portanto, d é menor que y que, por sua vez, é inferior a $Q(y, u, x_1, \ldots, x_n)$(pelas condições iniciais do lema). Então d é menor que t e, por isso mesmo, $d|t$ ($t = Q(y, u, x_1, \ldots, x_n)!$). Então, como $d|1 + kt$ e $d|t$, d divide 1 e, portanto, $d = 1$. Temos, então, uma sequência admissível de módulos e, pelo Teorema Chinês dos Restos, para cada $i = 1, \ldots, m$, existe a_i tal que

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

Como na implicação contrária, também aqui k e c serão equivalentes módulo $1 + kt$, portanto

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

$$= 0 \text{ (ver hipótese).}$$

Isto acontece para cada $k = 1, 2, \ldots, y$. Ora, como para cada k, $1 + kt$ divide $P(y, c, x_1, \ldots, x_n, a_1, \ldots, a_m)$ e os números $1 + kt$ são primos dois a dois, o produto também dividirá o polinómio. Assim sendo, $P(y, k, x_1, \ldots, x_n, a_1, \ldots, a_m) \equiv 0 \bmod 1 + ct$ também é satisfeito. Resta-nos provar que

$$1 + ct | \prod_{j=1}^{u}(a_i - j),\ i = 1, \ldots, m.$$

Primeiro, como $a_i \equiv y_i^{(k)} \bmod 1 + kt$, $1 + kt$ divide $a_i - y_i^{(k)}$. Ora, $y_i^{(k)}$ é um inteiro entre 1 e u donde obviamente que $1+kt$ divide o produto das diferenças $(a_i - j)$, com j a variar entre 1 e u, já que $y_i^{(k)}$ vai tomar um desses valores. Novamente porque

$1+kt$ são 2 a 2 primos entre si, como cada um destes números vai dividir o produto, também $1+ct|\prod_{j=1}^{u}(a_i-j)$, $i=1,\ldots,m$. □

Completemos então a prova do Teorema 4.2 usando os lemas 4.8 e 4.9. Falta-nos provar que o conjunto S desse teorema é diofantino.

Como queremos aplicar o lema 4.9, precisamos de um polinómio Q que satisfaça as 3 condições do enunciado deste lema. P será um polinómio qualquer, portanto P será da forma

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

com $t_r=cy^ak^bx_1^{q_1}x_2^{q_2}\ldots x_n^{q_n}y_1^{s_1}y_2^{s_2}\ldots y_m^{s_m}$ e c um inteiro positivo ou negativo.

Para Q cumprir as condições, façamos então $u_r=|c|y^{a+b}bx_1^{q_1}\ldots x_n^{q_n}u^{s_1+s_2+\cdots+s_m}$ e seja

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

Para valores não nulos, é óbvio que $Q(y,u,x_1,\ldots,x_n)>u$ e $Q(y,u,x_1,\ldots,x_n)>y$, portanto as propriedades 1 e 2 são satisfeitas. A aplicação da desigualdade triangular, implica para que $k\leq y$ e $y_1,\ldots,y_m\leq y$, também a terceira condição se verifica.

Assim, como foi visto no lema anterior,

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

é equivalente a

$$(\exists c,t,a_1,\ldots,a_m)\big((1+ct=\prod_{k=1}^{y}(1+kt))\wedge(t=Q(y,u,x_1,\ldots,x_n)!)\wedge(1+ct|\prod_{j=1}^{u}(a_1-j))$$

$$\wedge\cdots\wedge(1+ct|\prod_{j=1}^{u}(a_m-j))\wedge(P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_m)\equiv 0 \bmod 1+ct)\big)$$

que podemos escrever como

$$(\exists u,c,t,a_1,\ldots,a_m,e,f,g_1,\ldots,g_m,h_1,\ldots,h_m,l)\big((e=1+ct)\wedge(e=\prod_{k=1}^{y}(1+kt))$$

$$\wedge(f=Q(y,u,x_1,\ldots,x_n))\wedge(t=f!)\wedge(g_1=a_1-u-1)\wedge\cdots\wedge(g_m=a_m-u-1)$$

$$\wedge(h_1=\prod_{k=1}^{u}(g_1+k))\wedge\cdots\wedge(h_m=\prod_{k=1}^{u}(g_m+k))\wedge(e|h_1)\wedge\cdots\wedge(e|h_m)$$

$$\wedge(l=P(y,c,x_1,\ldots,x_n,a_1,\ldots,a_n))\wedge(e|l)\big)$$

Os termos $\prod_{j=1}^{u}(a_i-j)$ foram decompostos nos equivalentes pares $(g_i=a_i-u-1)\wedge(h_i=\prod_{k=1}^{u}(g_i+k))$ pois, no Teorema 4.1 foi a função $h(a,b,y)=\prod_{k=1}^{y}(a+bk)$ que vimos ser diofantina.

Conseguimos então reduzir a expressão que define os elementos do conjunto S do Teorema 5.1 a uma expressão que sabemos já ser diofantina, o que conclui a prova de que S é diofantino. □

3.5. Exemplos

Será então altura, com todas as ferramentas de que já dispomos, de darmos alguns exemplos do que são conjuntos diofantinos.

O conjunto S dos números compostos é um conjunto diofantino que pode ser representado por

$$(n \in S) \Leftrightarrow (\exists x, y)(n = (x+1)(y+1)).$$

Por outro lado, um número pertence ao conjunto P dos números primos se

$$(p > 1) \wedge (\forall x, y)_{\leq p}((xy < p) \vee (xy > p) \vee (x = 1) \vee (y = 1)).$$

Então, uma representação do conjunto diofantino dos números primos pode ser dada por

$$(p \in P) \Leftrightarrow (p > 1) \wedge (\forall x, y)_{\leq p} \exists u, v((xy + u - p)^2 (xy - v + p)^2 (x-1)^2 (y-1)^2).$$

Segundo a teoria atrás exposta esta expressão podia ser libertada da sua quantificação limitada e abranger $p > 1$ usando o lema 4.9, mas a expressão seria demasiado pesada.

Em relação ao conjunto das relações de modularidade, teremos um conjunto constituído por pares de inteiros, sempre relativos ao módulo em questão. Neste caso (x, y) pertencem ao conjunto S sse $x \equiv y \bmod c$. Este conjunto pode ser representado por

$$(x, y) \in S \Leftrightarrow (\exists z)((x-y)^2 = c^2(z-1)^2).$$

(Se admitíssemos quantificação sobre os inteiros (eventualmente negativos) podíamos escrever $(x, y) \in S \Leftrightarrow (\exists z)(x - y) - cz = 0)$.)

O conjunto dos ternos (x, y, z) tais que $x|y$ e $x < z$. Aqui

$$(x|y) \Leftrightarrow (\exists u)(y = xu) \text{ e } (x < z) \Leftrightarrow (\exists v)(z = x + v)^2.$$

Então,

$$((x, y, z) \in S) \Leftrightarrow (\exists u, v)((y - xu)^2 + (x + v - z)^2 = 0).$$

3.6. Funções recursivas

Até aqui fizemos um estudo aprofundado de funções e relações diofantinas. É altura de fazer a ligação do nosso problema de indecidibilidade às noções de método efectivo ou algorítmico que são o núcleo de problemas deste tipo, como mencionado na introdução. Surgidas no seguimento de desenvolvimentos da lógica moderna e do crescente interesse por máquinas calculadoras, Post e Turing propuseram, de forma independente, modelos computacionais idealizados de tais máquinas. Isto ocorria em 1936 e estas máquinas seriam equiparáveis a humanos na capacidade de cálculo, mas mais rápidas e menos falíveis, por serem processos mecânicos e, assim, se eliminarem os normais erros humanos. Ao mesmo tempo, nos desenvolvimentos da lógica, o programa de Hilbert, o logicismo de Russel e a aritmetização da metamatemática de Gödel levaram a tentativas de especificação do que seria calculável ou decidível, levando a que, cada um à sua maneira, definisse o que seria a classe de funções computáveis que actualmente se chamam recursivas.

A *tese de Turing-Church*, hoje completamente aceite, baseia-se no facto de todas as abordagens à questão da computabilidade se mostrarem equivalentes: máquinas de Turing ou funções recursivas captam essencialmente aquilo que é mecanizável em matemática.

Em relação às funções diofantinas, temos já uma linguagem extensa, a partir de vários métodos que usámos (quantificadores limitados, a função $S(i,u)...$), que nos permite obter um número bastante vasto de conjuntos diofantinos. Convergimos então os dois estudos neste capítulo: usaremos a classe das funções recursivas para testar os métodos usados no estudo das funções diofantinas.

3.6.1. A classe das funções recursivas

Há várias definições equivalentes desta classe. A que usaremos será a que se apoia em três funções base: a função constante, a função sucessor e a função projecção (respectivamente, $\mathbb{N} \ni x \mapsto c(x) = 1 \in \mathbb{N}$, $\mathbb{N} \ni x \mapsto s(x) = x + 1 \in \mathbb{N}$, $\mathbb{N}^n \ni (x_1, \ldots, x_n) \mapsto P_n^k(x_1, \ldots, x_n) = x_k \in \mathbb{N}$)

A estas funções chamaremos as funções iniciais.

Todas as outras funções recursivas são construídas a partir destas, iterando através das três operações

• **composição** em que, se $f : \mathbb{N}^m \to \mathbb{N}$ e $g_i : \mathbb{N} \to \mathbb{N}$, $i = 1, 2 \ldots, m$ forem recursivas, então $h : \mathbb{N}^n \to \mathbb{N}$ definida por

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

é recursiva;

• **recursão primitiva** em que, se $f : \mathbb{N}^n \to \mathbb{N}$ e $g : \mathbb{N}^{n+2} \to \mathbb{N}$ forem recursivas, então $h : \mathbb{N}^{n+1} \to \mathbb{N}$ definida por

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

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

é recursiva;

• **operador mínimo** em que para $f, g : \mathbb{N}^{n+1} \to \mathbb{N}$ recursivas, a função $h : \mathbb{N}^n \to \mathbb{N}$ definida por

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

é recursiva. h devolve o menor valor y para o qual $f(x_1, \ldots, x_n, y) = g(x_1, \ldots, x_n, y)$, assumindo que para cada $x_1, \ldots, x_n$, existe pelo menos um y para o qual a equação é satisfeita, ou seja, h está definida em toda a parte.

A esta definição adicionamos o facto de que a função $S(i, u)$ definida no Teorema 1.2 ser recursiva. Por definição, isto pode ser provado a partir das três funções iniciais e das três operações acima referidas.

3.6.2. Funções diofantinas vs. funções recursivas

Nesta secção comparamos funções diofantinas com funções recursivas e chegamos à extraordinária conclusão de que as funções diofantinas são precisamente as recursivas e vice-versa, isto é

Teorema 6.1. Uma função é diofantina se e só se é recursiva.

Primeiro, sabemos que um polinómio com coeficientes inteiros positivos é construído iterando sobre somas e multiplicações e, portanto, vejamos a recursividade destas operações: As equações

$$\begin{aligned} \text{sum}(x, 1) &= s(x) \\ \text{sum}(x, t+1) &= (s \circ P_2^3)(t, sum(t, x), x) \end{aligned}$$

comprovam a recursividade da soma, por recursividade primitiva.

Em relação à multiplicação, também pela recursão primitiva e com o auxílio da soma,

podemos usar as seguintes equações

$$\begin{aligned} \text{mult}(x,1) &= P_1^1(x) \\ \text{mult}(x,t+1) &= (\text{sum} \circ (P_3^3, P_2^3))(t, mult(t,x), x) \end{aligned}$$

como testemunha da sua recursividade.

Como sabemos, a função $c_1(x) = 1$ é recursiva (por definição). De facto, todas as funções constantes $c_k(x) = k$, $k \in \mathbb{N}$ são recursivas, como vemos por indução em k, atendendo a

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

Como todo o polinómio se escreve por composição destas três funções, todo o polinómio de coeficientes inteiros será recursivo.

Seja então f uma função diofantina e escreva-se

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

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

onde P e Q são polinómios com coeficientes inteiros positivos. Então, usando a função $S(i,u)$, podemos reescrever f como

$$f(x_1, \ldots, x_n) = S(1, \mu_u[P(x_1, \ldots, x_n, y, S(1,u), S(2,u), \ldots, S(m+1,u)) = \\ = Q(x_1, \ldots, x_n, y, S(1,u), S(2,u), \ldots, S(m+1,u))]).$$

Como P, Q e $S(i,u)$ são recursivas, usando a composição e o operador mínimo também f será recursiva.

Falta provar que o recíproco é também verdadeiro, isto é, que toda a função recursiva é diofantina.

Ora as funções iniciais são obviamente diofantinas, basta apenas provar que as funções diofantinas são uma classe fechada para a composição, para a recursão primitiva e para o operador mínimo.

Seja $h : \mathbb{N}^n \to \mathbb{N}$ definida por $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$, com $f : \mathbb{N}^m \to \mathbb{N}$ e $g_i : \mathbb{N}^n \to \mathbb{N}$ diofantinas. Então, h também é diofantina pois

$$y = h(x_1, \ldots, x_n) \Leftrightarrow (\exists t_1, \ldots, t_m)(t_1 = g_1(x_1, \ldots, x_n) \wedge \ldots \\ \wedge t_m = g_m(x_1, \ldots, x_n) \wedge y = f(t_1, \ldots, t_m)).$$

Portanto, assegurámos que, após composição, as funções continuam diofantinas.

De seguida veremos o que sucede com a recursão primitiva. Sejam então $f : \mathbb{N}^n \to \mathbb{N}$

e $g : \mathbb{N}^{n+2} \to \mathbb{N}$ diofantinas e h definida como

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

Se, novamente, usarmos a função $S(i, u)$ para "guardar" os números $h(x_1, \ldots, x_n, 1)$, $h(x_1, \ldots, x_n, 2)$,..., $h(x_1, \ldots, x_n, t)$, respectivamente em $S(1, u)$, $S(2, u)$,..., $S(t, u)$. Então $y = h(x_1, \ldots, x_n, t)$ é equivalente a

$$(\exists u)[(\exists v)\big((v = S(1, u)) \wedge (v = f(x_1, \ldots, x_n))\big)\wedge$$

$$(\forall s)_{\leq t}\big((s = t) \vee (\exists v)((v = S(s+1, u)) \wedge v = g(s, S(s, u), x_1, \ldots, x_n))\big) \wedge y = S(t, u)]$$

o que, devido a tudo o que vimos na secção 3.4 garante que a função h é ainda diofantina.

Em relação ao operador mínimo, como f e g são diofantinas e h é definida, *grosso modo*, como o menor valor para o qual as funções f e g se igualam, podemos reescrevê-la como sendo

$$\begin{aligned} y = h(x_1, \ldots, x_n) \Leftrightarrow \\ &\big((\exists z)((z = f(x_1, \ldots, x_n, y)) \wedge (z = g(x_1, \ldots, x_n, y)) \big) \\ &\wedge(\forall t)_{\leq y}((t = y) \vee (\exists u, v)((u = f(x_1, \ldots, x_n, y)) \\ &\wedge((v = g(x_1, \ldots, x_n, y)) \wedge ((u > v) \vee (v > u))))\big). \end{aligned}$$

Isto demonstra que h é também diofantina, concluindo a nossa demonstração sobre a equivalência das classes das funções recursivas e diofantinas. □

3.7. A indecidibilidade do décimo problema de Hilbert

Na secção anterior provámos que a classe das funções diofantinas e a classe das funções recursivas são equivalentes. Estamos agora preparados para provar a indecidibilidade do décimo problema de Hilbert. Comecemos por descrever uma enumeração de todos os conjuntos diofantinos de *números inteiros positivos*:

Como qualquer polinómio com coeficientes inteiros positivos pode ser construído a partir de 1 por sucessivas adições e muiltiplicações, fixamos um alfabeto de variáveis $x_0, x_1, x_2, \ldots$ e contruímos os restantes polinómios a partir das funções L e R (definidas na secção 3.1), enumerando como aqui descrito

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

Escreva-se $P_i = P_i(x_0, x_1, \ldots, x_n)$, onde n é suficientemente grande para que todas as variáveis que ocorrem no polinómio sejam incluídas. (É claro que, regra geral, o polinómio não irá depender de todas estas variáveis!)

Sejam agora os conjuntos diofantinos D_i, definidos desta forma

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

Nesta definição, $P_{L(n)}$ e $P_{R(n)}$ não envolvem necessariamente todas estas variáveis, mas obviamente não podem envolver quaisquer outras, pois, como vimos na primeira secção, $L(n),\ R(n) \leq n$.

Os primeiros polinómios gerados por esta enumeração são

$$\begin{aligned} P_1 &= 1 & P_5 &= x_1 \\ P_2 &= x_0 & P_6 &= P_2 + P_1 = x_0 + 1 \\ P_3 &= P_{L(1)} + P_{R(1)} = 1 + 1 = 2 & P_7 &= P_2 \cdot P_1 = x_0 \\ P_4 &= P_{L(1)} \cdot P_{R(1)} = 1 \cdot 1 = 1 & P_8 &= x_2 \end{aligned}$$

E os primeiros conjuntos diofantinos são

$$D_1 = \{x_0 | (\exists x_1)(P_{L(1)}(x_0, x_1) = P_{R(1)}(x_0, x_1)\ )\}$$

$$= \{x_0 | (\exists x_1)(P_1(x_0, x_1) = P_1(x_0, x_1)\ )\} = \{x_0 | (\exists x_1) 1 = 1\} = \mathbb{Z}$$

$$D_2 = \{x_0 | (\exists x_1, x_2)(P_{L(2)}(x_0, x_1, x_2) = P_{R(2)}(x_0, x_1, x_2)\ )\}$$

$$= \{x_0 | (\exists x_1, x_2)(x_0 = 1\ )\} = \{1\}$$

$$D_3 = D_2$$

$$D_4 = \{x_0 | (\exists x_1, x_2, x_3, x_4)(P_{L(4)}(x_0, x_1, x_2, x_3, x_4) = P_{R(4)}(x_0, x_1, x_2, x_3, x_4)\ )\}$$

$$= \{x_0 | (\exists x_1, x_2, x_3, x_4)(P_3 = P_1\ )\} = \{x_0 | 2 = 1\} = \emptyset$$

Da maneira que foram construídos os polinómios (a partir das funções L e R, que traduzem uma bijecção entre $\mathbb{N}^2$ e os naturais) e os conjuntos diofantinos, a sequência de conjuntos $D_1,\ D_2,\ D_3, \ldots$ vai conter todos os conjuntos diofantinos de naturais.

Teorema 7.1. Teorema da Universalidade:

O conjunto $\{(n, x) | x \in D_n\}$ é diofantino.

Prova: Usemos a função $S(i,u)$ uma vez mais para "guardar" números. Afirmamos que:

$$\begin{aligned} x \in D_n \Leftrightarrow (\exists u)\{S(1,u) = 1 \wedge S(2,u) = x \\ \wedge(\forall i)_{\leq n}(\ S(3i,u) = S(L(i),u) + S(R(i),u)\ ) \\ \wedge(\forall i)_{\leq n}(\ S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)\ ) \\ \wedge S(L(n),u) = S(R(n),u)\ \} \end{aligned}$$

Obviamente que o segundo membro da equivalência é diofantino, portanto só precisamos de verificar que a equivalência é, de facto, verdade.

Seja x pertencente a D_n para dados x e n. Então existem naturais $t_1, \ldots, t_n$ tais que $P_{L(n)}(x, t_1, \ldots, t_n) = P_{R(n)}(x, t_1, \ldots, t_n)$.

É uma observação trivial (mas talvez útil) que o natural $P_j(x, t_1, ..., t_n)$ pode ser construído indutivamente pelas fórmulas acima dadas, se substituirmos desde início as variáveis por naturais.

Dados então os naturais $x, t_1, ..., t_n$, podemos escolher u (pelo teorema 1.2) tal que

$$S(j,u) = P_j(x, t_1, t_2, \ldots, t_n), \text{ com j=1,2,. . . ,3n+2.}$$

Em particular, pela definição dos polinómios que demos, $S(1,u) = 1$, $S(2,u) = x$, $S(3i+1,u) = S(L(i),u) \cdot S(R(i),u)$ e $S(3i,u) = S(L(i),u) + S(R(i),u)$, com $i = 1, 2, \ldots, n+1$. Assim, a implicação neste sentido ($\Rightarrow$) fica provada. Suponhamos agora que o lado direito da equivalência se verifica. Faça-se

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

Então, $P_j(x, t_1, \ldots, t_n) = S(j,u),\ j = 1, \ldots, 3n+2$ é verdade. Como $S(L(n),u) = S(R(n),u)$ se verifica, terá de acontecer

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

isto é, $x \in D_n$. □

A partir do momento em que podemos listar todos os conjuntos diofantinos, é fácil construir um conjunto a partir destes que não seja Diofantino. Definamos

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

Teorema 7.2 O conjunto V não é diofantino.

Prova: A prova rege-se pelo método de diagonalização de Cantor. Se V fosse diofantino, para algum i, $V = D_i$. O que aconteceria ao elemento i? Por um lado, se $i \in V$, como $V = D_i$, então $i \in D_i$. Por outro lado, se $i \in V$, então i, pela definição

de V, não pode pertencer a D_i. Isto gera uma contradição, portanto V não pode ser diofantino. □

Chegamos então ao ponto alto deste capítulo. O que decorre da demonstração do próximo teorema vai ser de suprema importância para o nosso objectivo pois contradiz a existência de um algoritmo que resolva equações diofantinas.

Teorema 7.3 A função $g(n,x)$ definida por

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

não é recursiva.

Prova: Se g fosse recursiva, pelo Teorema 6.1 seria diofantina, isto é, existiria um polinómio P tal que

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

Mas, nesse caso, seria possível definir-se V da forma

$$V = \{x | (\exists y_1, \ldots, y_m)(P(x,x,1,y_1,\ldots,y_m) = 0 \ )$$

o que viria contradizer o que foi provado no Teorema 7.2, pois $P(x,x,1,y_1,\ldots,y_m)$ é evidentemente um polinómio. □

Teorema 7.4 O décimo problema de Hilbert é indecidível.

Prova: Usando o Teorema 7.1, poderíamos escrever

$$x \in D_n \Leftrightarrow (\exists y_1, \ldots, y_k)(P(n,x,y_1,\ldots,y_k) \ ),$$

onde P seria potencialmente um polinómio complicado, mas, ainda assim, possível de definir.

Suponhamos que existia um algoritmo para decidir se equações diofantinas tinham solução, isto é, um algoritmo que resolvesse o décimo problema de Hilbert. Então, para dados x e n, esse algoritmo podia testar se a equação $P(n,x,y_1,\ldots,y_k) = 0$ tinha solução, isto é, se x estaria ou não em D_n. Mas nesse caso teríamos um método mecânico que computaria a função g, algo que já provámos não ser possível, pois as funções recursivas são precisamente aquelas para as quais um algoritmo computável

existe! Isto iria contradizer o Teorema 7.3 e, assim, concluímos que **o décimo problema de Hilbert é indecidível**! □

Capítulo 4

Conclusão

Ao longo deste trabalho pudemos ver de forma razoavelmente clara o que se entende por um problema indecidível. Mais ainda, vimos dois exemplos de problemas indecidíveis, bastante diferentes no seu âmago. Eram não só diferentes em tipo, como a própria forma de demonstrar a sua indecidibilidade se provou ser distinta. De facto, enquanto que com o décimo problema de Hilbert foi necessário ir às profundezas das definições do tema e demonstrar explicitamente como não era possível exibir um algoritmo que resolvesse todas as instâncias do problema, no caso da mortalidade em semigrupos foi adoptada uma abordagem que é mais comum nestes problemas: reduzir a um problema já conhecido como indecidível e provar a indecidibilidade dessa forma. No entanto, ambas as abordagens são válidas e a existência de problemas indecidíveis continua a assegurar-nos de que o olhar humano continua a não ser substituível pelo computorizado: a nossa capacidade de ver para além do mecanizável supera ainda as máquinas.

Bibliografia

[1] Daniel E Cohen. *Computability and logic*. Ellis Horwood Limited, 1987.

[2] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

[3] Vesa Halava and Tero Harju. Mortality in matrix semigroups. *The American Mathematical Monthly*, 108(7):649–653, 2001.

[4] J Malitz. Introduction to mathematical logic. set theory. computation functions. model theory, 1974.

[5] Emil L Post. A variant of a recursively unsolvable problem. *Bulletin of the American Mathematical Society*, 52(4):264–268, 1946.