DOI: http://dx.doi.org/10.29069/forscience.2013v1n1.e26

EQUAÇÕES DIOFANTINAS LINEARES: FUNDAMENTAÇÃO MATEMÁTICA E UM ALGORITMO DE RESOLUÇÃO

Hugo Brener Oliveira Ferreira[1]
José Sérgio Domingues[2]

RESUMO

Diofanto foi um matemático Grego (aproximadamente 300 DC) que viveu em Alexandria e foi praticamente o único matemático de renome da Grécia Antiga que se dedicou à Teoria dos Números, sendo o pioneiro na determinação de soluções para equações polinomiais com coeficientes inteiros. Em sua homenagem recebem o nome de Equações Diofantinas Lineares a duas variáveis, as equações do tipo $ax + by = c$, em que $a, b, c \in \mathbb{Z}$. Neste artigo, apresentam-se alguns dos principais resultados necessários para se provar em que condições uma equação diofantina linear a duas variáveis admite soluções, além de uma possível aplicação da disciplina de programação de computadores na disciplina de Teoria dos Números, em um curso de licenciatura em matemática, onde se desenvolve um algoritmo na linguagem Pascal. Este permite encontrar em um intervalo pré-definido, todas as soluções para uma equação diofantina dada, caso estas existam.

Palavras-chave: Equações diofantinas. Teoria dos números. Algoritmo de resolução.

LINEAR DIOPHANTINE EQUATION: MATHEMATICS REASONING AND AN ALGORITHM OF RESOLUTION

ABSTRACT

Diofanto was a Greek mathematician (about 300 AD) who lived in Alexandria. He was practically the only renowned mathematician of ancient Greece who dedicated himself to the Theory of Numbers, being the pioneer in determining solutions to polynomial equations with entire coefficients. In his honor are called linear Diophantine equations in two variables, the equations of the type $ax + by = c$ where $a, b, c \in \mathbb{Z}$. In this article, it is presented some of the main results needed, to prove in which conditions that a linear Diophantine equation with two variables admits solutions. It is also stated a possible application of the computer programming subject in the Theory of Numbers discipline in mathematics, which develops an algorithm in Pascal language. It allows finding, on a certain pre-defined range, all solutions for a given Diophantine equation, if it exists.

Keywords: Diophantine equations. Number theory. Algorithm of resolution.

[1] Professor de Matemática e Física do Instituto Nossa Senhora Aparecida - Salinas MG, graduado em Licenciatura Plena em Matemática pela Universidade Estadual de Montes Claros (UNIMONTES). E-mail: brennerhugo@yahoo.com.br

[2] Doutorando em Engenharia Mecânica/Bioengenharia pela Universidade Federal de Minas Gerais (UFMG). Mestre em Modelagem Matemática e Computacional pelo Centro Federal de Educação Tecnológica de Minas Gerais (CEFET MG). Professor do curso de Matemática do IFMG – Campus Formiga.
E-mail: sergio.domingues@ifmg.edu.br

1 INTRODUÇÃO MATEMÁTICA

As equações diofantinas lineares são todas as equações de grau 1, da forma:

$$a_0x_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \quad (1)$$

sendo $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, das quais se procuram somente as soluções inteiras. Isso significa que se quer escrever c como combinação linear inteira de todos os a_i com $0 \leq i \leq n$. Sendo assim, determinar uma solução desse tipo de equação significa encontrar o conjunto de valores inteiros $\alpha_0, \alpha_1, \ldots, \alpha_n$ que, ao serem substituídos nos respectivos lugares de $x_0, x_1, \ldots, x_n$, verifiquem a equação (1).

Neste trabalho, dá-se ênfase às equações desse tipo, porém àquelas com duas variáveis, x e y, com coeficientes $a_0 = a$ e $a_1 = b$. Ou seja, consideram-se as equações do tipo:

$$ax + by = c. \quad (2)$$

Para melhor compreensão de como resolver essas equações, é necessário o conhecimento de alguns resultados da Teoria dos Números, sendo que os principais são apresentados nesta seção, e, na maior parte, são demonstrados. Contudo, as demonstrações omitidas podem ser facilmente encontradas nas referências indicadas ao final do trabalho.

Definição 1.1 Dados $a, b \in \mathbb{Z}$ com $a \neq 0$, diremos que a divide b e simbolizaremos $a|b$, quando $b = ak$, para algum $k \in \mathbb{Z}$, denominado quociente de b por a. Neste caso, dizemos que b é um múltiplo de a, e também que a é um divisor de b. Porém, se não existir $k \in \mathbb{Z}$ tal que $b = ak$, dizemos que a não divide b e simbolizamos por $a \nmid b$.

Exemplo 1.2 Dados os inteiros $a = 432$ e $b = 4$, pode-se afirmar que $4|432$ (lê-se: 4 divide 432), pois $432 = 4 \cdot 108$, ou seja, para esse caso, basta considerar $k = 108$. Sendo assim, 432 é um múltiplo de 4, ou, de forma equivalente, 4 é um divisor de 432. Porém, como não existe inteiro k tal que $12k = 355$, é possível dizer que 12 não divide 355, isto é, $12 \nmid 355$.

No caso onde $a \nmid b$, ou seja, onde a relação de divisibilidade não existir, ainda é possível efetuar a chamada *divisão euclidiana* de b por a, em que sempre é possível obter o quociente dessa divisão, considerando-se a existência de um resto *r*.

Teorema 1.3 (Divisão Euclidiana) Sejam $a, b \in \mathbb{N}$ com $0 < a < b$. Então, existem e são únicos os naturais r e q tais que $b = aq + r$ e $r < a$.

Definição 1.4 Sejam $a, b \in \mathbb{Z}$ e não simultaneamente nulos. Um inteiro d é denominado o máximo divisor comum entre a e b, e simbolizado por $d = mdc(a, b)$, se ele for o maior inteiro tal que $d|a$ e $d|b$.

Proposição 1.5 Se $d = mdc(a, b)$, então d divide qualquer combinação linear inteira de a e b, ou seja, $d|(ax + by)$ para quaisquer valores inteiros de x e y.

Demonstração: Observe que mostrar que $d|(ax + by)$ significa concluir que existe $k \in \mathbb{Z}$ tal que $ax + by = dk$.

Ora, como $d = mdc(a, b)$, tem-se que $d|a$ e que $d|b$, isto é, pode-se escrever que $a = dk_1$ e que $b = dk_2$ com $k_1, k_2 \in \mathbb{Z}$. Sendo assim, fica claro que:

$$ax + by = dk_1x + dk_2y = d(k_1x + k_2y).$$

Tomando-se $k = k_1x + k_2y$, é possível concluir que $ax + by = dk$, e a demonstração está finalizada.

□

Axioma 1.6 (Princípio da Boa Ordenação (PBO)) Todo subconjunto não vazio Ω de números inteiros positivos possui um menor elemento. Isto é, existe $w \in \Omega$ tal que $\forall\, x \in \Omega$ com $x \neq w$, tem-se que $w < x$.

Teorema 1.4 (Teorema de Bezout) Sejam $a, b \in \mathbb{Z}$, ambos não nulos, e $d = mdc(a, b)$. Então, existem dois inteiros m e n tais que $d = am + bn$.

Demonstração: Como $d > 0$, considerar-se-á o conjunto Ω de todos os inteiros positivos da forma $am + bn$ com $m, n \in \mathbb{Z}$. Ou seja,

$$\Omega = \{am + bn; m, n \in \mathbb{Z}\ e\ am + bn > 0\}.$$

É claro que $\Omega \neq \emptyset$, pois se $m = a$ e $n = b$ tem-se $am + bn = a^2 + b^2 > 0$, o que implica que $(a^2 + b^2) \in \Omega$.

Pela Proposição 1.5, temos que d divide todos os elementos de Ω, e, pelo Axioma 1.6, Ω possui um menor elemento w que, obviamente, pode ser escrito como $w = am_0 + bn_0$ com $m_0, n_0 \in \mathbb{Z}$.

Pelo Teorema 1.3, se a for dividido por w, obter-se-á $a = wq + r$ com $0 \leq r < w$. Logo, percebe-se que $r = a - wq = a - (am_0 + bn_0)q = a(1 - qm_0) + b(-qn_0) \in \Omega$, significando que $r \geq w$, o que é um absurdo, pois contraria a minimalidade de w. Sendo assim, tem-se que $r = 0 \Rightarrow w|a$.

Com raciocínio análogo ao que foi feito anteriormente, demonstra-se facilmente que $w|b$. Sendo assim, pela Definição 1.4, falta apenas demonstrar que w é o maior inteiro com essa propriedade, e isso pode ser feito por contradição, supondo que exista um inteiro $t > w$ tal que $t|a$ e $t|b$. Então, $a = tk_1$ e $b = tk_2$, com $k_1, k_2 \in \mathbb{Z}$. Além disso, pode-se escrever que $w = am_0 + bn_0 = tk_1m_0 + tk_2n_0 = t(k_1m_0 + k_2n_0) = tk \Rightarrow t|w$, o que contradiz o fato de $t > w$.

Portanto, w é o maior inteiro positivo tal que $w|a$ e $w|b$, ou seja, $am_0 + bn_0$ é o máximo divisor entre a e b, e o teorema está demonstrado.

□

As definições e os resultados apresentados e demonstrados até aqui servem de base para se demonstrar os teoremas que especificam as condições para que uma equação diofantina linear possua soluções inteiras. Na próxima seção esses resultados serão demonstrados e um deles servirá de técnica de resolução para as equações do tipo (2).

2 A TÉCNICA DE RESOLUÇÃO E UM EXEMPLO DE APLICAÇÃO

Nesta seção, faz-se a apresentação de um problema simples de aplicação das equações diofantinas lineares a duas variáveis e também são apresentados e demonstrados dois importantes teoremas para a determinação das soluções desse tipo de equações, caso existam. Além disso, os resultados demonstrados foram utilizados para apresentar uma sequência de passos para a resolução do problema proposto.

Considerando-se a seguinte situação:

Uma empresa distribui a seus funcionários vales-alimentação no valor total de R$ 250,00. Sabendo-se que estes vales são de R$ 5,00 e de R$ 7,00, como saber quantos vales de cada valor devem ser entregues a cada funcionário?

É fácil perceber que a resolução do problema dado está na solução da equação diofantina $5x + 7y = 250$, cujas variáveis x e y só podem assumir valores inteiros e positivos.

Em meio a problemas deste tipo, perguntas como as apresentadas a seguir podem surgir naturalmente:

i. Quais condições são necessárias para que se possa garantir a existência de soluções inteiras da equação?
ii. Quantas soluções a equação possui?
iii. Como podem ser calculadas as soluções, caso existam?

Para se resolver problemas como o descrito acima, é necessário utilizar os resultados adquiridos até aqui para tentar demonstrar outros que possam responder às três perguntas destacadas. Dessa forma, apresenta-se a seguir um teorema que permite saber se dada equação possui ou não solução, e outro que possibilita saber a forma geral de apresentação do conjunto de soluções quando o *mdc* entre os coeficientes da equação diofantina é igual a 1.

Teorema 2.1 A equação diofantina $ax + by = c$ possui soluções inteiras se, e somente se, $d = mdc(a, b)$ divide c.

Demonstração: Suponha que a equação admita uma solução (x_0, y_0). Então, vale a igualdade $ax_0 + by_0 = c$. Como $d = mdc(a, b)$, temos que $d|a$ e $d|b$, logo, pela Proposição 1.5 temos que $d|(ax_0 + by_0)$, isto é $d|c$.

Reciprocamente, suponha que $d|c$, ou seja, $c = dk$, para algum inteiro k. Por outro lado, pelo Teorema 1.4 sabe-se que existem inteiros m e n tais que $d = am + bn$.

Multiplicando ambos os lados da igualdade acima por k, obtém-se:

$$dk = a(mk) + b(nk) \Rightarrow c = a(mk) + b(nk).$$

Portanto, a equação diofantina linear $ax + by = c$ admite pelo menos a solução $(x_0, y_0) = (mk, nk)$. □

Corolário 2.2 Se $mdc(a, b) = 1$, a equação diofantina $ax + by = c$ possui solução.

Demonstração: Consequência direta do Teorema 2.1, bastando observar que, se $mdc(a, b) = 1$, sempre valerá que $d|c$.

□

Teorema 2.3 Seja o par ordenado (x_0, y_0) uma solução particular da equação diofantina linear $ax + by = c$, onde $mdc(a, b) = 1$. Então, as soluções desta equação são da forma $x = x_0 + tb$ e $y = y_0 - ta$, para t variando em $\mathbb{Z}$.

Demonstração: Se (x_0, y_0) é uma solução particular da equação diofantina, tem-se que $ax + by = ax_0 + by_0 = c$. Então, $ax - ax_0 = by_0 - by$, que implica em:

$$a(x - x_0) = b(y_0 - y). \tag{3}$$

Daí, segue-se que $a|b(y_0 - y)$ e $b|a(x - x_0)$. Além disso, como $mdc(a, b) = 1$ tem-se que:

$$y_0 - y = ta \tag{4}$$

e

$$x - x_0 = sb \tag{5}$$

para t e s em $\mathbb{Z}$.

Substituindo as equações (4) e (5) na equação (3), conclui-se que:

$$asb = bta \Rightarrow s = t.$$

Logo, a solução é dada por $x = x_0 + tb$ e $y = y_0 - ta$.

Reciprocamente, se $x = x_0 + tb$ e $y = y_0 - ta$, é possível substituir esses valores na equação $ax + by = c$, obtendo-se:

$$a(x_0 + by) + b(y_0 - at) = ax_0 + by_0 + bat - bat = ax_0 + by_0 = c.$$

□

Usando os Teoremas 2.1 e 2.3 pode-se resolver qualquer equação diofantina linear de duas variáveis. Vejamos agora como resolver o problema proposto no início dessa seção.

Tem-se que a resolução do problema está na solução da equação $5x + 7y = 250$. Além disso, sabe-se que 5 e 7 são primos e, portanto, $mdc(5,7) = 1$, o que permite concluir, pelo Corolário 2.2, que a equação possui solução. Sendo assim, deve-se encontrar um par (x_0, y_0) que satisfaça a igualdade. Observa-se que $5x + 7y = 250 \Rightarrow 5x = 250 - 7y$.

Dessa forma, é possível afirmar que $250 - 7y$ deve ser um múltiplo de 5. Além disso, como $5|250$, tem-se, obrigatoriamente, $5|7y$.

Logo, se $y = 5$, tem-se que $x = 43$, sendo o par $(43, 5)$ uma solução particular para o problema proposto. Pelo Teorema 2.3, sabe-se que o conjunto de soluções possíveis para esse problema é da forma:

$$\begin{cases} x = 43 + 7t \\ y = 5 - 5t \end{cases} com\ t \in \mathbb{Z}.$$

Contudo, é preciso lembrar que o problema aceita apenas soluções positivas, ou seja, x e y devem ser não negativos. Então, é necessário descobrir em qual intervalo a variável independente t deve variar.

Como se desejam valores não negativos para x e y, vale que $43 + 7t \geq 0$ e $5 - 5t \geq 0 \Rightarrow t \geq -6$ e $t \leq 1$.

Sendo assim, tem-se que os valores que a variável t pode assumir devem satisfazer:

$$\{t \in \mathbb{Z};\ -6 \leq t \leq 1\}.$$

Portanto, todas as soluções possíveis para o problema em questão são os pares ordenados:

$$(1,35), (8,30), (15,25), (22,20), (29,15), (36,10), (43,5), (50,0)$$

Ou seja, todas as possíveis formas de entrega dos vales-alimentação para os funcionários da empresa estão descritas acima. Por exemplo, a solução $(15, 25)$ indica que podem ser entregues 15 vales no valor de R$ 5,00 e 25 vales no valor de R$ 7,00.

Na próxima seção, será apresentado um algoritmo em Linguagem Pascal, que permite encontrar as soluções de qualquer equação diofantina linear a duas variáveis, de maneira prática e eficiente, com base nos conhecimentos vistos anteriormente.

3 DESENVOLVIMENTO DE UM ALGORITMO DE RESOLUÇÃO EM PASCAL

A Linguagem Pascal foi desenvolvida entre 1968 e 1970 por Nicklaus Wirth na Universidade Técnica de Zurique, Suíça. Em 1970, foi disponibilizado o primeiro compilador

para a linguagem, com o objetivo de desenvolver uma linguagem de programação para ensinar programação estruturada. Esta linguagem foi batizada com o nome de Pascal, em homenagem a Blaise Pascal, filósofo e matemático francês que viveu entre 1623 e 1662, responsável pela invenção de uma das primeiras máquinas lógicas que se tem notícia. O programa Pascal segue a estrutura dos algoritmos, onde os comandos são seguidos na sequência em que vão aparecendo.

Aplicando-se os conhecimentos adquiridos em Teoria dos Números, juntamente com os adquiridos em Programação de Computadores, foi possível desenvolver um algoritmo em Linguagem Pascal que resolve essas equações diofantinas de maneira prática e rápida, determinando quais são suas soluções em um dado intervalo. A necessidade de um intervalo se fez presente devido ao fato de essas equações poderem apresentar infinitas soluções.

O algoritmo funciona de maneira simples, e o usuário precisa apenas digitar os coeficientes da equação diofantina a ser resolvida e o intervalo em que deseja encontrar as soluções.

A estrutura do algoritmo na Linguagem Pascal foi construída de maneira que possibilitasse ao usuário, mesmo sem nenhum conhecimento de programação de computadores, resolver equações diofantinas do tipo $ax + by = c$.

A ideia partiu da necessidade de conferir se os cálculos efetuados manualmente estavam corretos e, principalmente, com o intuito de mostrar uma utilidade direta da programação de computadores na matemática, em especial para acadêmicos de licenciatura que estão tendo o primeiro contato com a programação.

Foi necessário declarar variáveis para os coeficientes da equação e também as variáveis de controle, onde, a partir destas, o programa determinasse as soluções da equação, caso existissem.

As variáveis de controle funcionaram como contadores que permitiram encontrar soluções em um determinado intervalo de valores inteiros. Primeiramente, imaginou-se ser possível apenas para valores positivos; porém, ao usar um intervalo já definido para se procurar as possíveis soluções ($|t| \leq \varepsilon$ ou seja, $-\varepsilon \leq t \leq \varepsilon$), foi possível encontrar tanto soluções positivas quanto negativas.

É importante ressaltar que o programa resolve equações diofantinas lineares sem considerar as restrições para os valores de t, com exceção dos valores caracterizados por $|t|$, pois estes variam de problema para problema. Sendo assim, para cada problema que se quiser determinar a solução, basta inserir no código as restrições desejadas.

```
PROGRAMA: eqdio {obtem as solucoes de equacoes diofantinas ax+by=c}

VARIAVEIS
      longint a,b,c {coeficientes da equação diofantina}
      longint m,t {variáveis de controle}
      longint x,y {coordenadas da solução da equação diofantina}

INICIO
      escreva ("Entre com o valor do coeficiente a: ")
      leia (a)
      escreva ("Entre com o valor do coeficiente b: ")
      leia (b)
      escreva ("Entre com o valor do coeficiente c: ")
      leia (c)
      escreva ("Entre com o módulo do intervalo das soluções: ")
      leia (t)

            PARA x=-t ate x=t faça
                  PARA y=-t ate y=t faça
                        SE a*x+b*y=c faça
                        escreva ("(x,y)")
                        m←m+1
                        FIM_SE
                  FIM_PARA
            FIM_PARA
      SE m=0 faça
      escreva ("A equação não possui solução nesse intervalo.")

FIM
```

Percebe-se facilmente que a complexidade do programa desenvolvido é $O(t^2)$, devido aos laços PARA aninhados que fazem $(2t + 1)$ iterações cada e onde todos os outros são $O(1)$. Isso permite garantir uma boa eficiência do algoritmo, desde que os valores da variável t não sejam demasiadamente grandes.

A validação do algoritmo implementado foi feita com a resolução de várias equações diofantinas e com diversos intervalos de resolução. Em particular, resolveu-se a equação $5x + 7y = 250$, que foi foco de estudo na seção 2, considerando-se as soluções no intervalo $|t| = 50$, ou seja, $-50 \leq t \leq 50$.

A resposta do programa na resolução do problema descrito anteriormente foi praticamente em tempo real, pois mesmo sendo $O(t^2)$, o intervalo é relativamente pequeno. Nela, foram encontradas três soluções com abscissas negativas e ordenadas positivas, além de

outras 8 soluções com ambas as coordenadas positivas. As soluções obtidas pelo programa foram:

$$(-20,50), (-13,45), (-6,40), (1,35), (8,30), (15,25)$$
$$(22,20), (29,15), (36,10), (43,5), (50,0)$$

Comparando os resultados obtidos na resolução analítica desse problema, na seção 2, com os obtidos pelo programa desenvolvido, percebe-se que, com exceção das soluções de abscissas negativas, as soluções são as mesmas. Sendo assim, como já mencionado, para cada equação diofantina a ser resolvida, basta adicionar ao programa as restrições desejadas para os valores de t, e as soluções computacionais serão iguais às soluções analíticas.

4 CONCLUSÕES

O programa desenvolvido trouxe praticidade e eficiência na resolução de equações diofantinas lineares do tipo $ax + by = c$, possibilitando aplicar o aprendizado obtido pela Teoria dos Números na disciplina de Programação de Computadores, e, portanto, pode auxiliar em uma aprendizagem mais sólida e também na visualização de um exemplo de inter-relação entre essas duas áreas do conhecimento. O programa Pascal utilizado favorece o trabalho, pois possui uma estrutura organizada e uma linguagem de fácil entendimento. Além disso, ficou demonstrado que, para valores não muito grandes para o intervalo de soluções, o algoritmo é eficiente, com complexidade $O(t^2)$.

REFERÊNCIAS

HEFEZ, A. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2005. (Textos Universitários).

HEFEZ, A. **Introdução à aritmética**: PIC-OBMEP. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2009.

MANZANO, J. A. N. G.; YAMATUMI, W. Y. **Estudo dirigido turbo pascal.** 4. ed. São Paulo: Érica, 2000.

SANTOS, J. P. O. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 1998. (Coleção Matemática Universitária).

Recebido em: 10/08/2013

Aprovado em: 06/10/2013