UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
CURSO DE LICENCIATURA EM MATEMÁTICA

EQUAÇÕES DIOFANTINAS LINEARES E ALGUMAS APLICAÇÕES

NEWTON CÉSAR DA SILVA MONTEIRO

CAMPINA GRANDE
2018

NEWTON CÉSAR DA SILVA MONTEIRO

EQUAÇÕES DIOFANTINAS LINEARES E ALGUMAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento as exigências para obtenção do título de Licenciado em Matemática.

Orientadora: Profa. Dra. Maria Isabelle Silva Dias Yanes

CAMPINA GRANDE

2018

M757e Monteiro, Newton Cesar da Silva.
Equações diofantinas lineares e algumas aplicações [manuscrito] / Newton Cesar da Silva Monteiro. - 2018.
48 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2018.

"Orientação : Profa. Dra. Maria Isabelle Silva Dias Yanes , Departamento de Matemática - CCT."

1. Aritmética. 2. Teoria dos números. 3. Equação polinomial. 4. Ensino de matemática. I. Título

21. ed. CDD 513.2

NEWTON CÉSAR DA SILVA MONTEIRO

EQUAÇÕES DIOFANTINAS LINEARES E ALGUMAS APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento as exigências para obtenção do título de Licenciado em Matemática.

Aprovado em: 09/08/2018.

BANCA EXAMINADORA

Maria Isabelle Silva Dias Yanes

Profa. Dra. Maria Isabelle Silva Dias Yanes (Orientadora)

Universidade Estadual da Paraíba (UEPB)

Luciana R Freitas

Profa. Dra. Luciana Roze de Freitas

Universidade Estadual da Paraíba (UEPB)

Kátia Suzana Medeiros Graciano

Profa. Ma. Kátia Suzana Medeiros Graciano

Universidade Estadual da Paraíba (UEPB)

Dedicatória

À minha querida família,
DEDICO.

Agradecimentos

Agradeço primeiramente a Deus pela minha vida, caso contrário eu não estaria aqui realizando tal conquista. Agradeço aos meus familiares, em especial à minha mãe Maria Neusa que sempre fez de tudo para que eu pudesse chegar até aqui, ao meu pai Carlos Augusto que também teve sua parcela de contribuição, à minha irmã Fernanda Kalina pelo auxílio durante a realização deste e principalmente pela inspiração diária na vida acadêmica, não podendo esquecer da minha namorada Maria Victória pelo apoio e incentivo nos dias de maior dificuldade.

Agradeço a todos os meus amigos e colegas que estiveram presentes durante minha graduação, por todos os momentos descontraídos que serviram para minimizar a pressão e a responsabilidade em alguns momentos do curso. Para não correr o risco de esquecer alguém optei por não mencionar vossos nomes. Todavia o apreço é o mesmo por todos, além do mais, quem esteve comigo saberá da minha gratidão para com eles.

Agradeço a toda equipe do departamento de matemática da UEPB, a todos os professores em que tive o prazer de ser aluno, pois foram muito importantes para a minha formação, sou grato por todos os ensinamentos.

Resumo

O presente trabalho tem como objetivo realizar um estudo sobre equações diofantinas lineares em duas e três variáveis. Utilizaremos alguns dos principais conceitos da teoria elementar dos números, como divisibilidade, divisão euclidiana e máximo divisor comum. Ademais, vamos explorar suas aplicações em situações-problema que envolvem números inteiros, evidenciando a importância do nosso tema.

Palavras-chave: Aritmética. Máximo Divisor Comum. Teoria dos Números.

Abstract

The present work aims to conduct a study on linear diophantine equations in two and three variables. We will use some of the main concepts of the elementary theory of numbers, such as divisibility, Euclidean division and common maximum divisor. In addition, let's explore their applications in problem situations involving integers, highlighting the importance of our theme.

Keywords: Arithmetic. Greatest Common Denominator. Theory of Numbers.

Sumário

Introdução

Diofanto é considerado o maior algebrista grego, bastante conhecido por seu livro *Arithmetica*, um trabalho sobre a teoria algébrica dos números que consta em 13 livros, dos quais sete desapareceram. A parte que restou do trabalho é dedicada à resolução de 130 problemas. O primeiro livro destina-se a equações determinadas em uma incógnita e os demais a equações indeterminadas de segundo grau em duas ou três incógnitas.

Diofanto realizou seu trabalho na grande Alexandria, a segunda cidade mais populosa do Egito. Durante o período de 250 a.C a 350 d.C, Alexandria era o centro da aprendizagem matemática, estava na sua "idade de prata". Foi considerada assim pois viria após uma época de grande desenvolvimento no campo da matemática, em torno de 300 a.C, tempo de Euclides além de outros matemáticos e filósofos gregos, que ficou conhecida como "idade de ouro".

Diofanto é o pioneiro na solução das equações justamente chamadas de diofantinas. Esse tipo de equação, ao ser aplicada pelos matemáticos modernos à análise dos números inteiros, produziu um grande desenvolvimento da teoria dos números. Em particular, Fermat foi levado ao seu *grande* ou *último* teorema quando procurou generalizar um problema que tinha lido na *Arithmetica* de Diofanto: dividir um quadrado dado em dois outros quadrados. O, então, Último Teorema de Fermat afirma que não há três inteiros positivos a, b e c que satisfazem a equação $a^n + b^n = c^n$ para qualquer valor inteiro de n maior do que 2. Em 1994 o britânico Andrew Wiles, com colaboração de Richard Taylor, finalmente publica a demonstração definitiva do teorema. Andrew provou que a equação não possui soluções inteiras para $n \geq 3$. A partir de então o teorema passou a ser chamado de Teorema de Fermat-Wiles.

De acordo com [2], quase tudo que conhecemos sobre a vida pessoal de Diofanto está contido no seguinte sumário de um epitáfio que aparece na Antologia Grega:

"Caminhante! Aqui jaz o matemático Diofanto, que passou um sexto de sua vida como criança, um doze avos como adolescente e mais um sétimo na condição de solteiro. Cinco anos depois de se casar nasceu-lhe um filho que morreu 4 anos antes de seu pai, com metade da idade (final) de seu pai".

De acordo com esse enigma, podemos calcular o seu tempo de vida. Então, sendo D a idade de Diofanto, temos:

[...] passou um sexto de sua vida como criança. $\Rightarrow \dfrac{D}{6}$

[...] um doze avos como adolescente. $\Rightarrow \dfrac{D}{12}$

[...] um sétimo na condição de solteiro. $\Rightarrow \dfrac{D}{7}$

Cinco anos depois de se casar nasceu-lhe um filho. $\Rightarrow 5$

[...] morreu 4 anos antes de seu pai. $\Rightarrow 4$

[...] com metade da idade (final) de seu pai. $\Rightarrow \dfrac{D}{2}$

Assim, a idade D de diofanto é obtida com a seguinte soma:

$$D = \frac{D}{6} + \frac{D}{12} + \frac{D}{7} + 5 + 4 + \frac{D}{2} = \left(\frac{25}{28}\right) D + 9$$
$$D = \frac{252}{3} = 84$$

Daí podemos concluir que Diofanto viveu 84 anos.

Acerca das Equações Diofantinas, faremos um estudo mais aprofundado nas Equações Diofantinas Lineares, vamos enunciar sua definição, mostraremos como determinar uma solução particular e a solução geral quando lidarmos com duas variáveis e também com três variáveis a posteriori, onde faremos uso dos principais conceitos da Teoria dos Números no decorrer deste trabalho.

Divideremos este trabalho em três capítulos, onde serão organizados da seguinte maneira:

No Capítulo 1, abordaremos alguns dos principais tópicos da Teoria dos Números, começando por uma introdução sobre o conjunto dos números inteiros a partir de uma fundamentação axiomática, em seguida falaremos sobre divisibilidade nos inteiros, divisão euclidiana, máximo divisor comum, inclusive para mais de dois números, e números primos. Todos os tópicos que serão abordados são de suma importância para que haja um maior entendimento do que será apresentado posteriormente.

No Capítulo 2, vamos mostrar a definição de uma equação diofantina e, de fato, voltar nossas atenções para as equações diofantinas lineares, onde mostraremos a resolução das equações com duas e com três variáveis.

No Capítulo 3, iremos mostrar algumas aplicações das equações diofantinas lineares em situações-problema do cotidiano, por meio de problemas encontrados em livros didáticos, banco de questões da OBMEP e também do PROFMAT.

Capítulo 1

Números Inteiros

Nesta seção iremos abordar alguns conceitos que são de fundamental importância para a compreensão do conteúdo que será apresentado no Capítulo 2. Todas as definições, teoremas e corolários vem das referências [3], [4] e [5].

1.1 Uma Fundamentação Axiomática

Consideremos, inicialmente, o conjunto dos números inteiros, denotado por $\mathbb{Z}$

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3 \ldots\}$$

Estão definidas duas operações no conjunto dos números inteiros, adição e multiplicação, as quais denotaremos, respectivamente, por "+" e "·".

O conjunto $\mathbb{Z}$, munido destas duas operações, possui as seguintes propriedades:

- **Propriedade associativa:** Para todo $a, b, c \in \mathbb{Z}$, temos

$$a + (b + c) = (a + b) + c$$

- **Existência do neutro para adição:** Existe um único elemento, denominado *neutro aditivo* ou *zero*, tal que

$$a + 0 = a, \text{para todo } a \in \mathbb{Z}$$

- **Existência do inverso aditivo (Simétrico):** Para cada inteiro a existe um único elemento que chamaremos de inverso de a e indicaremos por $-a$, tal que

$$a + (-a) = 0, \text{para todo } a \in \mathbb{Z}$$

- **Propriedade comutativa da adição:** Para todo $a, b \in \mathbb{Z}$ tem-se

$$a + b = b + a$$

- **Propriedade associativa da multiplicação:** Para todo $a, b, c \in \mathbb{Z}$, temos

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- **Existência do neutro para multiplicação:** Existe um único elemento, diferente de zero, que indicaremos por 1, tal que

$$1 \cdot a = a, \text{para todo } a \in \mathbb{Z}$$

- **Propriedade cancelativa:** Para todo $a, b, c \in \mathbb{Z}$ com $a \neq 0$, tem-se que

$$\text{se } a \cdot b = a \cdot c, \text{então}, b = c$$

- **Propriedade comutativa da multiplicação:** Para todo $a, b, c \in \mathbb{Z}$ com $a \neq 0$, tem-se que

$$a \cdot b = b \cdot a$$

- **Propriedade distributiva:** Para todo $a, b, c \in \mathbb{Z}$, tem-se que

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Mostraremos, agora, propriedades que resultam das que foram vistas até o momento.

Proposição 1.1. *Para todo $a, b, c \in \mathbb{Z}$, temos que*

(1) $a \cdot 0 = 0$

(2) *Se $a \cdot b = 0$, então, $a = 0$ ou $b = 0$*

(3) *Se $a + b = a + c$, então, $b = c$.*

Demonstração: (1) Temos que

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0,$$

ou seja, $a \cdot 0 + a \cdot 0 = a \cdot 0$. Como $a \cdot 0 \in \mathbb{Z}$, então existe $-(a \cdot 0) \in \mathbb{Z}$ tal que $-(a \cdot 0) + (a \cdot 0) = 0$. Logo, adicionando $-(a \cdot 0)$ a ambos os membros da igualdade $a \cdot 0 + a \cdot 0 = a \cdot 0$, e usando a propriedade associativa da adição, obtemos

$$(-(a \cdot 0) + a \cdot 0) + a \cdot 0 = -(a \cdot 0) + a \cdot 0,$$

isto é, $0 + a \cdot 0 = 0$, portanto $a \cdot 0 = 0$.

(2) Temos, por hipótese, que $a \cdot b = 0$ e pelo item (1) que $a \cdot 0 = 0$, assim, $a \cdot b = a \cdot 0$. Se $a = 0$, a demonstração está concluída. Se $a \neq 0$, usando a propriedade do cancelamento, segue que $b = 0$.

(3) Adicionando $-a$ a ambos os membros de $a + b = a + c$, obtemos

$$-a + (a + b) = -a + (a + c) \Rightarrow (-a + a) + b = (-a + a) + c.$$

Assim, $0 + b = 0 + c$, ou seja, $b = c$.

■

Proposição 1.2. *Dados inteiros a e b, temos que:*

(1) $-(-a) = a$.

(2) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

(3) $(-a) \cdot (-b) = a \cdot b$.

Demonstração: (1) Dados $a, b \in \mathbb{Z}$

$$a + b = 0 \Rightarrow \; a + b + (-b) = 0 + (-b) \Rightarrow \; a = -b,$$

Desse modo, como $a + (-a) = 0$, segue que $a = -(-a)$.

(2) Temos,

$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0,$$

ou seja, $(-a) \cdot b = -(a \cdot b)$. Do mesmo modo,

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0,$$

logo, $a \cdot (-b) = -(a \cdot b)$. Portanto,

$$(-a) \cdot b = -(a \cdot b) = a \cdot (-b).$$

(3) Usando o item (2), temos,

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)).$$

Usando, agora, o item (1), temos que $-(-a) = a$, para todo $a \in \mathbb{Z}$. Consequentemente, $(-a) \cdot (-b) = a \cdot b$. ■

Ainda sobre o conjunto dos números inteiros, temos a definição da relação de ordem "menor ou igual", denotada por "$\leq$", que satisfaz as seguintes propriedades:

- **Reflexiva:** para todo inteiro a, tem-se que $a \leq a$.
- **Antissimétrica:** dados inteiros a e b, se $a \leq b$ e $b \leq a$, então $a = b$.
- **Transitiva:** dados inteiros a, b e c, se $a \leq b$ e $b \leq c$, então $a \leq c$.

1.2 Divisibilidade em $\mathbb{Z}$

Definição 1.1. *Dados dois números inteiros a e b, diremos que b divide a, em símbolos $b \mid a$, se existir um inteiro c tal que*

$$a = bc.$$

Diremos ainda que a é um múltiplo de b.

Quando ocorrer de b não dividir a, indicaremos por $b \nmid a$

Exemplo 1.1. Temos que 5 divide 35, pois existe um inteiro $c = 7$ tal que $35 = 5 \cdot 7$, logo $5 \mid 35$. Por outro lado, temos que 4 não divide 18, pois não existe um inteiro c tal que $18 = 4 \cdot c$, logo $4 \nmid 18$.

Lema 1.1. *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então existe $c \in \mathbb{Z}$ tal que $a = b \cdot c$. Logo,

$$|a| = |b \cdot c| = |b| \cdot |c|.$$

Como $c \neq 0$, segue que $1 \leq |c|$. Assim, multiplicando ambos os membros desta desigualdade por $|b|$, obtemos $|b| \leq |b| \cdot |c| = |a| \Rightarrow |b| \leq |a|$. ■

Proposição 1.3. *Em $\mathbb{Z}$ valem as seguintes propriedades:*

(1) *Os únicos divisores de 1 são 1 e -1.*

(2) *Se $a \mid b$ e $b \mid a$, então $a = \pm b$.*

Demonstração: (1) Se b é um divisor de 1, pelo Lema 1.1, $|b| \leq |1| = 1$, desse modo, $0 < |b| \leq 1$, logo $|b| = 1$, isto é, $b = \pm 1$.

(2) Se $a \mid b$ e $b \mid a$ existem $\lambda_1, \lambda_2 \in \mathbb{Z}$ tais que, $a = \lambda_1 b$ e $b = \lambda_2 a$. Assim,

$$a = (\lambda_1 \lambda_2)a,$$

logo, $\lambda_1 \lambda_2 = 1$, donde segue que $\lambda_1 = \pm 1$, portanto, $a = \pm b$. ■

Teorema 1.1. *Propriedades da divisibilidade:*

(1) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

(2) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

(3) *Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, $\forall\, m, n \in \mathbb{Z}$.*

Demonstração: (1) Temos, por hipótese, que $b = a\lambda_1$ e $c = b\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Substituindo o valor de b em $c = b\lambda_2$, obtemos $c = a(\lambda_1 \lambda_2)$, ou seja, temos que $a \mid c$.

(2) Sendo $b = a\lambda_1$ e $d = c\lambda_2$, temos $bd = (ac)(\lambda_1 \lambda_2)$, ou seja, $ac \mid bd$.

(3) Temos, por hipótese, que $b = a\lambda_1$ e $c = a\lambda_2$. Sejam $m, n \in \mathbb{Z}$, $mb = am\lambda_1$ e $nc = an\lambda_2$,

temos que $mb + nc = a(m\lambda_1 + n\lambda_2)$. Assim, $a \mid (mb + nc)$. ■

1.3 Divisão Euclidiana

Teorema 1.2 (Algoritmo da Divisão). *Sejam $a, b \in \mathbb{Z}$, com $b > 0$. Então, existem únicos $q, r \in \mathbb{Z}$, tais que*

$$a = bq + r, \text{ com } 0 \leq r < b.$$

Demonstração: Considere o conjunto

$$L = \{a - bq : q \in \mathbb{Z} \text{ e } a - bq \geq 0\}.$$

Note que, sendo $b \geq 1$, temos $|a| \cdot b \geq |a|$. Logo,

$$a - (-|a|) \cdot b = a + |a| \cdot b \geq a + |a| \geq 0.$$

Como $x = a - (-|a|) \cdot b$ é da forma $a - bq$, com $q = -|a|$, segue que $x \in L$. O que mostra que L é não vazio.

(Existência) Sendo L limitado inferiormente, pelo Princípio da Boa Ordem, L possui menor elemento, digamos $r = \min L$. Como $r \in L$, temos $r \geq 0$ e $r = a - bq$, com $q \in \mathbb{Z}$.

Podemos afirmar que $r < b$. De fato, suponha que $r \geq b$, assim $r - b \geq 0$ e

$$r - b = a - bq - b = a - b(q + 1).$$

Assim, $r - b \in L$ e $r - b < r$, o que contraria o fato de r ser o menor elemento de L. Portanto,

$$a = bq + r, \text{ com } q \in \mathbb{Z} \text{ e } 0 \leq r < b \tag{1.1}$$

Provando a existência dos inteiros q e r.

(Unicidade) Consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < b. \tag{1.2}$$

De (1.1) e (1.2), segue que $bq + r = bq_1 + r_1$. Assim,

$$r - r_1 = b(q_1 - q),$$

ou seja, $b \mid r - r_1$. Como $|r - r_1| < b$, temos que $r - r_1 = 0$. Portanto, $r = r_1$ e $q = q_1$, pois $b \neq 0$. Portanto, são únicos os inteiros q e r. ■

1.4 Máximo Divisor Comum

Definição 1.2. *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{N}$ é o máximo divisor comum de a e b quando as seguintes condições são satisfeitas:*

(1) $d \mid a$ e $d \mid b$.

(2) Se $c \mid a$ e $c \mid b$, então $c \mid d$.

Indicaremos o máximo divisor comum de a e b por

$$d = mdc(a, b).$$

Para um número inteiro a, indicaremos seu conjunto de divisores positivos por D_a, e para $a \neq 0$, denotaremos seu conjunto de múltiplos positivos por M_a, ou seja,

$$D_a = \{n \in \mathbb{N} : n \mid a\} \quad \text{e} \quad M_a = \{n \in \mathbb{N} : a \mid n\}$$

É claro que $D_a = D_{-a}$ e $M_a = M_{-a}$. Diante disto, é fácil ver que

$$mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b),$$

portanto é suficiente considerar a e b positivos.

A seguir mostraremos um teorema muito importante para a teoria elementar dos números, bastante utilizado na resolução de problemas envolvendo inteiros. Trata-se de uma famosa identidade que leva o nome do matemático francês Étienne Bézout (1730-1783). Tal identidade relaciona números a e b com seu mdc.

Teorema 1.3 (**Teorema de Bézout**). *Dados inteiros a e b, quaisquer, se $d = mdc(a, b)$, então existem inteiros n e m tais que*

$$d = an + bm.$$

Demonstração: Consideremos o conjunto

$$W = \{ax + by : x, y \in \mathbb{Z} \text{ e } ax + by > 0\}.$$

Notemos que W é não vazio. De fato, para $x = y = 1$,

$$a \cdot 1 + b \cdot 1 = a + b > 0 \Rightarrow a + b \in W.$$

Assim, pelo Princípio da Boa Ordem, W possui menor elemento, digamos $\lambda = \min W$. Vamos mostrar que $\lambda = mdc(a, b)$. Como $\lambda \in W$, existem $n, m \in \mathbb{Z}$ tais que

$$\lambda = an + bm. \tag{1.3}$$

Usando o algoritmo da divisão com os elementos a e λ, temos

$$a = \lambda q + r, \quad \text{com} \quad 0 \leq r < \lambda. \tag{1.4}$$

Substituindo o valor de λ em (1.3) na igualdade de (1.4), segue que

$$r = a - \lambda q = a - (an + bm)q = a - aqn - bqm.$$

Daí,

$$r = a(1 - qn) + b(-qm).$$

Logo, temos que $r = au + bv$, com $u = 1 - qn$ e $v = -qm$. Consequentemente, $r = 0$, caso contrário, $r > 0$ e, assim, $r \in W$, o que contraria o fato de λ ser o menor elemento de W, visto que $r < \lambda$. Portanto, $a = \lambda q$, ou seja, $\lambda \mid a$ Analogamente, prova-se que $\lambda \mid b$. Sendo $d = mdc(a, b)$, então $a + d\lambda_1$ e $b = d\lambda_2$. Logo, por (1.3),

$$\lambda = (d\lambda_1)n + (d\lambda_2)m = d(\lambda_1 n + \lambda_2 m),$$

ou seja, $d \mid \lambda$, e como $\lambda \mid d$, pois $d = mdc(a, b)$, segue que $d = \lambda$. Portanto, $d = an+bm$. ■

1.4.1 Algoritmo de Euclides

Teorema 1.4 (Algoritmo de Euclides). *Se $a = bq + r$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Note que se $D_a \cap D_b = D_b \cap D_r$ seus máximos divisores serão iguais. Então é suficiente mostrar essa igualdade. Se $d \in D_a \cap D_b$, então $d \mid a$ e $d \mid b$. Sabemos que $r = a - bq$, então segue que $d \mid r$, logo $d \in D_b \cap D_r$. Analogamente, se $d \in D_b \cap D_r$, então $d \mid b$ e $d \mid r$, assim $d \mid bq + r = a$, ou seja, $d \in D_a \cap D_b$. Logo, $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc(a, b) = mdc(b, r)$. ■

Exemplo 1.2. Calcular $d = mdc(2040, 496)$.

Solução. De acordo com o Algoritmo de Euclides, com $a = 2040$ e $b = 496$, temos,

$$2040 = 496 \cdot 4 + 56 \Rightarrow mdc(2040, 496) = mdc(496, 56),$$

$$496 = 56 \cdot 8 + 48 \Rightarrow mdc(496, 56) = mdc(56, 48),$$

$$56 = 48 \cdot 1 + 8 \Rightarrow mdc(56, 48) = mdc(48, 8),$$

$$48 = 8 \cdot 6 + 0 \Rightarrow mdc(48, 8) = mdc(8, 0) = 8,$$

Portanto $d = mdc(2040, 496) = 8$.

Exemplo 1.3. Como $50 = 4 \cdot 7 + 22$, então $mdc(50, 4) = mdc(4, 22) = 2$ e $mdc(50, 7) = mdc(7, 22) = 1$.

Exemplo 1.4. Como $84 = 4 \cdot 12 + 36$, então $mdc(84, 4) = mdc(4, 36) = 4$ e $mdc(84, 12) = mdc(12, 36) = 12$.

1.4.2 Máximo Divisor Comum de Mais de Dois Inteiros

Em conformidade com [5], sejam a, b e c inteiros positivos. Podemos ver que $D_a \cap D_b \cap D_c$ é um conjunto finito não vazio, logo, possui maior elemento, que é o máximo divisor comum de a, b e c, indicado por $mdc(a, b, c)$. Agora, entre estes inteiros vamos escolher dois deles, sejam a e b, com $d_1 = mdc(a, b)$. Qualquer número k que seja divisor comum de a, b e c também deve dividir d_1. Assim, sendo k um divisor comum de d_1 e c, temos que k divide $d_2 = mdc(d_1, c)$. Daí, se d_2 divide d_1 e c implica que o próprio d_2 é um divisor comum de a, b e c. Assim, d_2 não apenas os divide, mas qualquer divisor comum desses três números divide d_2. Consequentemente, temos que d_2 é o máximo divisor comum de a, b e c.

Teorema 1.5. *Sejam a,b e c inteiros não todos nulos. Se $d_1 = mdc(a, b)$, então o máximo divisor comum entre a,b e c, $d_2 = mdc(a, b, c)$, é dado por*

$$d_2 = mdc(d_1, c).$$

Exemplo 1.5. Determinar $d_2 = mdc(232, 120, 518)$.

Solução. De acordo com o Algoritmo de Euclides, com $a = 232$ e $b = 120$, temos,

$$232 = 120 \cdot 1 + 112 \Rightarrow mdc(232, 120) = mdc(120, 112),$$

$$120 = 112 \cdot 1 + 8 \Rightarrow mdc(120, 112) = mdc(112, 8),$$

$$112 = 8 \cdot 14 + 0 \Rightarrow mdc(112, 8) = mdc(8, 0) = 8,$$

Assim $d_1 = mdc(232, 120) = 8$. Agora, de maneira análoga, vamos determinar $d_2 = mdc(d_1, c)$. Temos que $d_1 = 8$ e $c = 518$, então, pelo Algoritmo de Euclides,

$$518 = 8 \cdot 512 + 6 \Rightarrow mdc(518, 8) = mdc(8, 6),$$

$$8 = 6 \cdot 1 + 2 \Rightarrow mdc(8, 6) = mdc(6, 2),$$

$$6 = 2 \cdot 3 + 0 \Rightarrow mdc(6, 2) = mdc(2, 0) = 2,$$

Portanto $d_2 = mdc(232, 120, 518) = 2$.

Definição 1.3. *Dois inteiros a e b são ditos* ***primos entre si*** *ou* ***relativamente primos*** *quando $mdc(a, b) = 1$.*

Exemplo 1.6. Os inteiros 2 e 17 são primos entre si. De fato, utilizando o método visto anteriormente para determinar o $mdc(2, 17)$, temos,

$$17 = 2 \cdot 8 + 1 \Rightarrow mdc(17, 2) = mdc(2, 1),$$

$$2 = 1 \cdot 2 + 0 \Rightarrow mdc(2, 1) = mdc(1, 0) = 1,$$

Portanto $d = mdc(2, 17) = 1$. Logo, pela definição anterior, 2 e 17 são primos entre si.

Proposição 1.4. *Os inteiros a e b são primos entre si, e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$*

Demonstração: Se a e b são primos entre si, pela Definição (1.3), temos que $mdc(a, b) = 1$ e de acordo com o Teorema de Bézout, existem inteiros n e m tais que $an + bm = 1$. Reciprocamente, se existem inteiros n e m tais que $an + bm = 1$, com $mdc(a, b) = d$, pela Definição (1.2), temos que $d \mid a$ e $d \mid b$. Portanto, $d \mid (an + bm)$ e $d \mid 1$, por conseguinte $d = mdc(a, b) = 1$, ou seja, a e b são primos entre si. ■

Proposição 1.5. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração: Por hipótese, $bc = ak$, com $k \in \mathbb{Z}$. Além disso, pela Proposição (1.4), existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Logo, multiplicando ambos os lados da igualdade por c, obtemos

$$cax + cby = cax + aky = c \Rightarrow a(cx + ky) = c.$$

Portanto, $a \mid c$. ■

Corolário 1.1. *Se $a, b \in \mathbb{Z}$ e $mdc(a, b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$*

Demonstração: Nota-se inicialmente que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, haja vista que d é um divisor comum de a e b. Como $mdc(a, b) = d$ então existem inteiros n e m tais que $an + bm = d$. Dividindo ambos os membros da igualdade por d, obtemos

$$\left(\frac{a}{d}\right) n + \left(\frac{b}{d}\right) m = 1$$

Logo, pela Definição (1.3), os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, ou seja, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ■

Até aqui apresentamos os principais conceitos da Teoria dos Números, portanto, podemos dar início ao próximo capítulo acerca das equações diofantinas.

Capítulo 2

Equações Diofantinas

Neste capítulo vamos apresentar a definição de uma equação diofantina linear, enunciar e demonstrar os teoremas que são necessários para a resolução destas, com duas e com três variáveis.

2.1 Equação Diofantina Linear com Duas Variáveis

Uma equação da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

é chamada equação diofantina linear, em que $a_1, \ldots, a_n$ são inteiros dados, chamados coeficientes, b que também é um inteiro dado, é chamado termo constante e $x_1, \ldots, x_n$ são as variáveis.

Nesta seção abordaremos o estudo das equações diofantinas lineares com duas variáveis, que são equações da forma

$$ax + by = c.$$

Uma solução inteira desta equação é constituída por um par de inteiros x_0 e y_0 tais que

$$ax_0 + by_0 = c.$$

Acerca de uma equação diofantina surgem dois questionamentos iniciais:

a) Existe solução para a equação $ax + by = c$?

b) Caso exista, quantas são e como determiná-las?

Podemos responder tais questionamentos com os teoremas que vêm a seguir.

Teorema 2.1. *A equação diofantina $ax + by = c$ tem solução inteira se, e somente se, $d \mid c$, onde $d = mdc(a, b)$.*

Demonstração: Suponha que a equação admita uma solução x_0, y_0. Então vale a igualdade $ax_0 + by_0 = c$. Como $mdc(a, b)$ divide a e divide b, segue que ele divide $ax_0 + by_0$, logo divide c. Agora, suponha que d divida c, ou seja, $c = k \cdot d$, onde $d = mdc(a, b)$, para algum inteiro k. Pelo Teorema de Bachet-Bézout, sabemos que existem inteiros n e m tais que

$$d = a \cdot n + b \cdot m.$$

Multiplicando ambos os membros da igualdade por k, obtemos

$$c = k \cdot d = a \cdot (k \cdot n) + b \cdot (k \cdot m).$$

Logo, a equação diofantina $ax + by = c$ admite pelo menos a solução

$$x_0 = (k \cdot n) \text{ e } y_0 = (k \cdot m).$$

■

Nota: De acordo com a Geometria Analítica a equação $ax + by = c$ representa uma reta no plano. Quando constatamos que certa equação $ax + by = c$ não possui soluções inteiras, estamos afirmando que não existem pontos (x, y) do plano com coordenadas inteiras que satisfaçam a equação. Por exemplo, a equação $6x + 4y = 5$ não possui solução inteira. De fato, temos que o $mdc(6, 4) = 2$ não divide 5. Mostrando que a reta de equação $6x + 4y = 5$ não contém pontos (x, y) com $x, y \in \mathbb{Z}$.

Teorema 2.2. *Se x_0 e y_0 é uma solução particular da equação $ax + by = c$ e $d = mdc(a, b)$, então sua solução geral é dada por*

$$x = x_0 + \frac{b}{d}t \quad e \quad y = y_0 - \frac{a}{d}t, \ t \in \mathbb{Z}$$

Demonstração: Se x, y é uma solução qualquer da equação, temos que

$$ax + by = ax_0 + by_0 = c$$

donde

$$a(x - x_0) = b(y_0 - y) \tag{2.1}$$

Como $mdc(a, b) = d$, existem inteiros M_1 e M_2 tais que $a = dM_1$ e $b = dM_2$. Substituindo os valores em (2.1) e cancelando d na igualdade, obtemos

$$M_1(x - x_0) = M_2(y_0 - y) \tag{2.2}$$

Logo, temos que $M_1 \mid M_2(y_0 - y)$ e $M_2 \mid M_1(x - x_0)$. Como $mdc(M_1, M_2) = 1$, segue que $M_1 \mid (y_0 - y)$ e $M_2 \mid (x - x_0)$. Assim,

$$y_0 - y = tM_1 \text{ e } x - x_0 = sM_2, \tag{2.3}$$

para alguns inteiros t e s. Substituindo esses valores em (2.2), obtemos

$$M_1 s M_2 = M_2 t M_1,$$

o que implica que $s = t$. Logo, de (2.3), temos que a solução é dada por $x = x_0 + M_2 t$ e $y = y_0 - M_1 t$. Mas, temos que $M_1 = \dfrac{a}{d}$ e $M_2 = \dfrac{b}{d}$, ou seja, $x = x_0 + \dfrac{b}{d}t$ e $y = y_0 - \dfrac{a}{d}t$.

Reciprocamente, se $x = x_0 + \dfrac{b}{d}t$ e $y = y_0 - \dfrac{a}{d}t$, substituindo esses valores na equação $ax + by = c$, obtemos

$$a\left[x_0 + \frac{b}{d}t\right] + b\left[y_0 - \frac{a}{d}t\right] = ax_0 + by_0 + \left(\frac{ab}{d} - \frac{ba}{d}\right)t = ax_0 + by_0 = c.$$

■

Corolário 2.1. *Toda equação diofantina linear da forma $ax + by = c$, onde $mdc(a, b) = d$ e $d \mid c$, é equivalente a uma equação do tipo $Ax + By = C$ em que $mdc(A, B) = 1$. Para tal, basta considerar $A = \dfrac{a}{d}$, $B = \dfrac{b}{d}$ e $C = \dfrac{c}{d}$.*

Para determinar uma solução particular x_0 e y_0 de uma equação diofantina $ax + by = c$ e, assim, determinar todas as suas soluções usamos o Algoritmo de Euclides da seguinte maneira: Sejam $a, b \in \mathbb{Z}$ e $mdc(a, b) = d$. Vamos determinar inteiros n e m tais que

$$an + bm = d. \tag{2.4}$$

Fazendo $c = dt$ e multiplicando a igualdade (2.4) por t, obtemos

$$a(nt) + b(mt) = dt = c,$$

isto é, $x_0 = nt$ e $y_0 = mt$ é uma solução particular de $ax + by = c$.

Exemplo 2.1. Determinar as soluções da equação diofantina $58x + 74y = 42$

Solução. Determinando o $mdc(58, 74)$ pelo Algoritmo de Euclides, temos:

$$\begin{aligned}
74 &= 58 \cdot 1 + 16 \Rightarrow 16 = 74 - 58 \cdot 1\\
58 &= 16 \cdot 3 + 10 \Rightarrow 10 = 58 - 16 \cdot 3\\
16 &= 10 \cdot 1 + 6 \Rightarrow 6 = 16 - 10 \cdot 1\\
10 &= 6 \cdot 1 + 4 \Rightarrow 4 = 10 - 6 \cdot 1\\
6 &= 4 \cdot 1 + 2 \Rightarrow 2 = 6 - 4 \cdot 1\\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

Portanto o $mdc(58, 74) = 2$ e a equação dada possui solução inteira, pois $mdc(58, 74) = 2 \mid 42$. De fato, para determinar as soluções vamos escrever 2 como combinação linear de 58 e 74, isolando os restos e fazendo as substituições necessárias, obtemos

$$\begin{aligned}
2 &= 6 - 4 = 6 - (10 - 6) = 2 \cdot 6 - 10 = 2 \cdot (16 - 10) - 10\\
&= 2 \cdot 16 - 3 \cdot 10 = 2 \cdot (74 - 58) - 3 \cdot (58 - 16 \cdot 3)\\
&= 2 \cdot 74 - 2 \cdot 58 - 3 \cdot 58 + 9 \cdot 16 = 2 \cdot 74 - 5 \cdot 58 + 9 \cdot (74 - 58)\\
&= 2 \cdot 74 - 5 \cdot 58 + 9 \cdot 74 - 9 \cdot 58 = 58 \cdot (-14) + 74 \cdot 11
\end{aligned}$$

Daí,

$$58 \cdot (-14) + 74 \cdot 11 = 2$$

Multiplicando ambos os membros da equação por 21, obtemos

$$58 \cdot (-294) + 74 \cdot 231 = 42$$

Logo, $x_0 = -294$ e $y_0 = 231$ é uma solução particular da equação. Para determinar todas as soluções utilizaremos o Teorema (2.2), desse modo a solução geral é dada por

$$x = -294 + 74t \ \text{ e } \ y = 231 - 58t \ \text{ com } t \in \mathbb{Z}$$

Exemplo 2.2. Determine a solução geral da equação diofantina $15x + 21y = 7$.
Solução. Determinando o $mdc(15, 21)$ pelo Algoritmo de Euclides, temos:

$$21 = 15 \cdot 1 + 6 \Rightarrow 6 = 21 - 15 \cdot 1$$

$$15 = 6 \cdot 2 + 3 \Rightarrow 3 = 15 - 6 \cdot 2$$

$$6 = 3 \cdot 2 + 0$$

Portanto o $mdc(15, 21) = 3$, desse modo a equação dada não possui solução inteira, pois $mdc(15, 21) = 3 \nmid 7$.

2.2 Equação Diofantina Linear com Três Variáveis

Nesta seção, tomando como referência [1] e [5], mostraremos como determinar a solução de equações diofantinas lineares com três variáveis, que será feita de maneira análoga à seção anterior, onde tínhamos duas variáveis. Então, do mesmo modo, uma solução inteira de uma equação da forma

$$a_1x + a_2y + a_3z = b$$

é um terno de inteiros (x_0, y_0, z_0) tais que

$$a_1x_0 + a_2y_0 + a_3z_0 = b.$$

Exemplo 2.3. O terno $(8, 3, 2)$ é uma solução da equação $3x + 7y + 2z = 49$, pois $3 \cdot (8) + 7 \cdot (3) + 2 \cdot (2) = 49$.

A seguir veremos um teorema, análogo ao Teorema (2.1), que nos garante quando é que uma equação diofantina de três variáveis admite solução.

Teorema 2.3. *A equação diofantina*

$$a_1x + a_2y + a_3z = b$$

tem solução se, e somente se, $d \mid b$, onde $d = mdc(a_1, a_2, a_3)$.

Demonstração: Vamos supor que (x_0, y_0, z_0) seja uma solução da equação, ou seja,

$$a_1x_0 + a_2y_0 + a_3z_0 = b, \tag{2.5}$$

e $d = mdc(a_1, a_2, a_3)$. Como d divide a_1, a_2 e a_3, então de (2.5), segue que $d \mid b$.

Reciprocamente, suponhamos que $d \mid b$, com $b = dt$. Se $d_1 = mdc(a_1, a_2)$, então pelo Teorema de Bézout, sabemos que existem inteiros k_1 e k_2 tais que

$$d_1 = a_1k_1 + a_2k_2.$$

Agora, sendo $d = mdc(d_1, a_3)$, temos que

$$d = d_1k_0 + a_3z_0, \tag{2.6}$$

onde k_0 e z_0 são inteiros. Substituindo o valor de d_1 em (2.6), obtemos

$$d = k_0(a_1k_1 + a_2k_2) + a_3z_0 = a_1(k_0k_1) + a_2(k_0k_2) + a_3z_0.$$

Fazendo $x_0 = k_0k_1$ e $y_0 = k_0k_2$, temos

$$d = a_1x_0 + a_2y_0 + a_3z_0. \tag{2.7}$$

Multiplicando ambos os membros de (2.7) por t, obtemos,

$$b = dt = a_1(x_0t) + a_2(y_0t) + a_3(z_0t),$$

logo (x_0t, y_0t, z_0t) é uma solução de $a_1x + a_2y + a_3z = b$, como queríamos.

Agora, vejamos como obter todas as soluções de uma equação diofantina de três variáveis. Alguns passos que serão mostrados a seguir são análogos ao caso com duas variáveis.

(1) Consideremos, inicialmente, uma equação diofantina da forma

$$a_1x + a_2y = t, \quad a_2y + a_3z = t \;\; ou \;\; a_1x + a_3z = t.$$

(2) A partir de uma solução da equação anterior, obtemos uma equação com duas variáveis a partir de substituições. Ao resolver essa equação obtida, podemos determinar a solução geral da equação original.

Então, consideremos a equação

$$a_1x + a_2y + a_3z = b, \tag{2.8}$$

com $d \mid b$, em que $d = mdc(a_1, a_2, a_3)$. Agora, seguindo o primeiro passo descrito anteriormente, consideremos

$$a_1x + a_2y = t,$$

isto é,

$$t + a_3z = b,$$

obtemos uma equação onde t e z são as variáveis. Temos que $mdc(1, a_3) = 1$, então a equação possui solução inteira. Ademais, segundo o Teorema (2.2), a solução geral é dada por

$$t = t_0 + a_3k \ \text{ e } \ z = z_0 - k, \ \text{com } k \in \mathbb{Z},$$

sendo (t_0, z_0) solução particular. Logo,

$$a_1x + a_2y = t_0 + a_3k. \tag{2.9}$$

Esta equação possui uma solução x_0 e y_0. Assim, sua solução geral é

$$x = x_0 + \frac{a_2}{d_1}\lambda \ \text{ e } \ y = y_0 - \frac{a_1}{d_1}\lambda, \ \text{ com } \ \lambda \in \mathbb{Z}.$$

Portanto, a solução geral da equação (2.8) é dada por

$$x = x_0 + \frac{a_2}{d_1}\lambda, \ \ y = y_0 - \frac{a_1}{d_1}\lambda \ \text{ e } \ z = z_0 - k,$$

para $\lambda, k \in \mathbb{Z}$. ■

Exemplo 2.4. Resolver a equação diofantina

$$15x + 12y + 30z = 24. \tag{2.10}$$

Solução. Para esta equação, tem-se $a_1 = 15, a_2 = 12, a_3 = 30$ e $b = 24$. Onde $mdc(15, 12, 30) = 3$ e $3 \mid 24$, logo a equação possui solução. Então, seja $t = 15x + 12y$, donde

$$t + 30z = 24. \tag{2.11}$$

Temos que $mdc(1, 30) = 1$ e $1 \mid 24$, logo uma solução desta equação pode ser obtida de maneira direta. Fazendo $z = 1$, obtemos $t = 24 - 30 = -6$. Assim, $t_0 = -6$ e $z = 1$ é solução particular de (2.11) e sua solução geral é dada por

$$t = -6 + 30k \ \text{ e } \ z = 1 - k \ \text{ com } \ k \in \mathbb{Z}$$

Agora, temos

$$15x + 12y = t = -6 + 30k. \tag{2.12}$$

Para que essa equação possua solução é necessário que o $mdc(15, 12) = 3$ divida $-6 + 30k$. Com efeito, pelo Algoritmo de Euclides, vem

$$3 = 15 \cdot 1 - 12 \cdot 1$$

Agora, multiplicando ambos os membros da igualdade acima por $\dfrac{-6 + 30k}{3}$, obtemos

$$3 \cdot \left(\frac{-6 + 30k}{3}\right) = 15 \cdot \left(\frac{-6 + 30k}{3}\right) - 12 \cdot \left(\frac{-6 + 30k}{3}\right)$$
$$-6 + 30k = 15 \cdot (-2 + 10k) + 12 \cdot (2 - 10k)$$

Assim, a solução geral de (2.12) é

$$x = -2 + 10k + \frac{12}{3}\lambda \ \text{ e } \ y = 2 - 10k - \frac{15}{3}\lambda,$$

ou ainda,

$$x = -2 + 10k + 4\lambda \ \text{ e } \ y = 2 - 10k - 5\lambda.$$

Portanto, a solução geral da equação (2.10) é

$$x = -2 + 10k + 4\lambda, \ \ y = 2 - 10k - 5\lambda \ \text{ e } \ z = 1 - k, \ \ \text{com } \ k, \lambda \in \mathbb{Z}.$$

Exemplo 2.5. Determinar uma solução particular da equação diofantina

$$100x + 72y + 90z = 6. \tag{2.13}$$

Solução. Seguindo os passos vistos anteriormente, temos que $a_1 = 100, a_2 = 72, a_3 = 90$ e $b = 6$. Onde $mdc(100, 72, 90) = 2$ e $2 \mid 6$, logo a equação possui solução. Então, seja $d_1 = mdc(100, 72) = 4$, assim

$$\begin{aligned} 4 &= (16 - 12) = 16 - (28 - 16) = 2 \cdot 16 - 28 \\ &= 2 \cdot (72 - 28 \cdot 2) - 28 = 2 \cdot 72 - 5 \cdot 28 \\ &= 2 \cdot 72 - 5 \cdot (100 - 72) = 100 \cdot (-5) + 72 \cdot 7 \end{aligned}$$

Agora, sendo $d = mdc(4, 90) = 2$, temos que

$$2 = 4 \cdot (-22) + 90 \cdot 1 \;\text{ e }\; 4 = 100 \cdot (-5) + 72 \cdot 7$$

Fazendo as devidas substituições,

$$\begin{aligned} 2 &= [100 \cdot (-5) + 72 \cdot 7] \cdot (-22) + 90 \cdot 1 \\ &= 100 \cdot 110 + 72 \cdot (-154) + 90 \cdot 1 \end{aligned}$$

Multiplicando ambos os membros da igualdade por 3, obtemos

$$\begin{aligned} 6 = 2 \cdot 3 &= 100 \cdot (110 \cdot 3) + 72 \cdot (-154 \cdot 3) + 90 \cdot (1 \cdot 3) \\ &= 100 \cdot 330 + 72 \cdot (-462) + 90 \cdot 3 \end{aligned}$$

logo, o terno $(330, -462, 3)$ é uma solução particular de (2.13).

Exemplo 2.6. Determinar a solução geral da equação dada no exemplo anterior.

Solução. Seja $t = 100x + 72y$, donde

$$t + 90z = 6, \tag{2.14}$$

que também possui solução, pois $mdc(1, 90) = 1 \mid 6$. Logo,

$$1 = 1 \cdot (-89) + 90 \cdot 1$$

$$6 = 1 \cdot (-534) + 90 \cdot 6$$

assim, sendo $t_0 = -534$ e $z_0 = 6$ uma solução particular de (2.14), sua solução geral é dada por

$$t = -534 + 90k \ \text{ e } \ z = 6 - k, \ \text{ com } \ k \in \mathbb{Z}$$

ademais, temos

$$100x + 72y = t = -534 + 90k. \tag{2.15}$$

Para que essa equação possua solução, o $mdc(100, 72) = 4$ deve dividir $-534 + 90k$. Com efeito, pelo Algoritmo de Euclides, segue

$$4 = 100 \cdot (-5) + 72 \cdot 7$$

Agora, multiplicando ambos os membros da igualdade acima por $\dfrac{-534 + 90k}{4}$, obtemos

$$4 \cdot \left(\frac{-534 + 90k}{4}\right) = 100 \cdot (-5) \cdot \left(\frac{-534 + 90k}{4}\right) + 72 \cdot 7 \cdot \left(\frac{-534 + 90k}{4}\right)$$
$$-534 + 90k = 100 \cdot \left(\frac{2670 - 450k}{4}\right) + 72 \cdot \left(\frac{-3738 + 630k}{4}\right)$$

Assim, a solução geral de (2.15) é

$$x = \left(\frac{2670 - 450k}{4}\right) + \frac{72}{4}\lambda \ \text{ e } \ y = \left(\frac{-3738 + 630k}{4}\right) + \frac{100}{4}\lambda$$

ou seja,

$$x = \left(\frac{2670 - 450k}{4}\right) + 18\lambda \ \text{ e } \ y = \left(\frac{-3738 + 630k}{4}\right) + 25\lambda.$$

Por fim, temos que a solução geral da equação diofantina linear de três variáveis (2.13) é

$$x = \left(\frac{2670 - 450k}{4}\right) + 18\lambda, \ \ y = \left(\frac{-3738 + 630k}{4}\right) + 25\lambda \ \text{ e } \ z = 1 - k, \ \text{ com } \ k, \lambda \in \mathbb{Z}.$$

Capítulo 3

Aplicações

Este capítulo destinar-se-á a resolução de problemas por meio de equações diofantinas lineares. Alguns problemas selecionados encontram-se em livros didáticos, banco de questões da OBMEP e outros são do PROFMAT.

Problema 1

O valor da entrada de um cinema é R$ 8,00 e da “meia” entrada é de R$ 5,00. Qual é o menor número de pessoas que podem assistir a uma sessão de maneira que a bilheteria seja de R$ 500,00?

Solução. Tomando $a = 8, b = 5$ e $c = 500$. Podemos representar o problema com a equação diofantina

$$8x + 5y = 500. \tag{3.1}$$

Como o $mdc(8, 5) = 1$ e $1 \mid 500$, a equação possui solução. Então, pelo Algoritmo de Euclides, vamos escrever 1 como combinação linear de 8 e 5. Logo,

$$8 = 5 \cdot 1 + 3 \Rightarrow 3 = 8 - 5 \cdot 1$$

$$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 3 \cdot 1$$

$$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 2 \cdot 1$$

$$2 = 1 \cdot 2 + 0$$

ou seja,

$$1 = 3 - (5 - 3) = 2 \cdot 3 - 5$$

$$= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5$$

$$= 8 \cdot 2 + 5 \cdot (-3)$$

Multiplicando a igualdade acima por 500, obtemos

$$8 \cdot (2 \cdot 500) + 5 \cdot (-3 \cdot 500) = 1 \cdot 500$$

isto é,

$$8 \cdot 1000 + 5 \cdot (-1500) = 500$$

Desse modo, $x_0 = 1000$ e $y_0 = -1500$ é uma solução particular de (3.1) e sua solução geral é

$$x = 1000 + 5t \;\text{ e }\; y = -1500 - 8t, \;\text{ com }\; t \in \mathbb{Z}.$$

Agora, devemos encontrar soluções inteiras e positivas já que o problema trata de um número de pessoas. Assim, deve-se ter

$$x > 0 \Rightarrow 1000 + 5t > 0 \Rightarrow 5t > -1000 \Rightarrow t > -200$$

e

$$y > 0 \Rightarrow 1500 + 8t < 0 \Rightarrow 8t < -1500 \Rightarrow t < -187,5$$

ou seja,

$$-200 < t < -187,5$$

Para encontrar o menor número de pesoas devemos escolher o maior valor inteiro que t pode assumir. Então, para $t = -188$, obtemos

$$x = 1000 + 5 \cdot (-188) = 60 \;\text{ e }\; y = -1500 - 8 \cdot (-188) = 4$$

Portanto, o menor número de pessoas para que a bilheteria seja de R\$500,00 será 64, onde 60 pessoas irão pagar R\$8,00 e 4 pessoas irão pagar R\$5,00.

Problema 2

Dois irmãos, João e José, pescaram em uma manhã x e y peixes, respectivamente. Sabendo que $3x + 4y = 61$, determine as possíveis quantidades de peixes que eles conseguiram juntos?

Solução. Fazendo

$$x = \frac{61 - 4y}{3} \tag{3.2}$$

obtemos,

$$\begin{aligned} x &= \frac{61}{3} - \frac{4y}{3} = \frac{60}{3} + \frac{1}{3} - \frac{3y}{3} - \frac{y}{3} \\ &= 20 - y + \frac{(1-y)}{3} \end{aligned}$$

Como x e y devem ser inteiros, $\dfrac{(1-y)}{3}$ também deve sê-lo. Então, para um inteiro t, segue

$$\frac{(1-y)}{3} = t \Rightarrow 1 - y = 3t \Rightarrow y = 1 - 3t$$

Agora, substituindo o valor de y em (3.2), obtemos

$$\begin{aligned} x &= \frac{61 - 4(1-3t)}{3} = \frac{61 - 4 + 12t}{3} = \frac{57 + 12t}{3} \\ &= \frac{57}{3} + \frac{12t}{3} = 19 + 4t \Rightarrow x = 19 + 4t \end{aligned}$$

Além do fato que x e y devem ser inteiros, eles também devem ser positivos, já que se trata da quantidade de peixes que cada um dos dois amigos conseguiu pescar. Assim,

$$x = 19 + 4t > 0 \Rightarrow 4t > -19 \Rightarrow t > \frac{-19}{4} \Rightarrow t > -4,75 \Rightarrow t \geq -4$$

e

$$y = 1 - 3t > 0 \Rightarrow 3t < 1 \Rightarrow t < \frac{1}{3} \Rightarrow t \leq 0$$

ou seja,

$$-4 \leq t \leq 0$$

Portanto, fazendo o t correr dentro desse intervalo, obtemos os seguintes resultados

$$\text{para } t = -4, \quad x = 19 + 4 \cdot (-4) = 3 \;\text{ e }\; y = 1 - 3 \cdot (-4) = 13$$
$$\text{para } t = -3, \quad x = 19 + 4 \cdot (-3) = 7 \;\text{ e }\; y = 1 - 3 \cdot (-3) = 10$$
$$\text{para } t = -2, \quad x = 19 + 4 \cdot (-2) = 11 \;\text{ e }\; y = 1 - 3 \cdot (-2) = 7$$
$$\text{para } t = -1, \quad x = 19 + 4 \cdot (-1) = 15 \;\text{ e }\; y = 1 - 3 \cdot (-1) = 4$$
$$\text{para } t = 0, \quad x = 19 + 4 \cdot (0) = 19 \;\text{ e }\; y = 1 - 3 \cdot (0) = 1$$

Desse modo, as possíveis quantidades de peixes que eles conseguiram juntos são $16, 17, 18, 19$ e 20.

Problema 3

Encontrar todos os números naturais N menores do que 10000 tais que:

- O resto da divisão de N por 37 é 9;
- O resto da divisão de N por 52 é 15.

Solução. Dividindo o natural N por 37, obtemos um quociente x e resto 9, isto é

$$N = 37x + 9 \tag{3.3}$$

Agora, dividindo o mesmo N por 52, obtemos um quociente y e resto 15, ou seja

$$N = 52y + 15 \tag{3.4}$$

Agora, de (3.3) e (3.4), obtemos a seguinte equação diofantina

$$37x + 9 = 52y + 15 \Rightarrow 37x - 52y = 6$$

Como o $mdc(37, 52) = 1$, já que 37 é primo e não divide 52, e $1 \mid 6$, a equação possui solução inteira. Então, pelo Algoritmo de Euclides, vamos escrever 1 como combinação linear de 37 e 52. Logo,

$$52 = 37 \cdot 1 + 15 \Rightarrow 15 = 52 - 37 \cdot 1$$

$$\begin{aligned}
37 &= 15 \cdot 2 + 7 \Rightarrow 7 = 37 - 15 \cdot 2 \\
15 &= 7 \cdot 2 + 1 \Rightarrow 1 = 15 - 7 \cdot 2 \\
7 &= 1 \cdot 7 + 0
\end{aligned}$$

Agora, isolando os restos e fazendo as substituições necessárias, obtemos

$$\begin{aligned}
1 &= 15 - 7 \cdot 2 = 15 - (37 - 15 \cdot 2) = \\
&= 15 \cdot 5 - 37 \cdot 2 = (52 - 37) \cdot 5 - 37 \cdot 2 = \\
&= 52 \cdot 5 + 37 \cdot (-7) = 37 \cdot (-7) - 52 \cdot (-5)
\end{aligned}$$

Daí,

$$37 \cdot (-7) - 52 \cdot (-5) = 1$$

Multiplicando ambos os membros da equação por 6, obtemos,

$$37 \cdot (-42) - 52 \cdot (-30) = 6$$

Logo $x_0 = -42$ e $y_0 = -30$ é uma solução particular da equação. Para determinar todas as soluções utilizaremos o Teorema (2.2), assim a solução geral é dada por

$$x = -42 - 52t \;\text{ e }\; y = -30 - 37t, \;\text{ com }\; t \in \mathbb{Z}.$$

Para encontrar soluções naturais da equação, basta que sejam satisfeitas as seguintes condições

$$x \geq 0 \Rightarrow -42 - 52t \geq 0 \Rightarrow 52t \leq -42 \Rightarrow t \leq -\frac{42}{52} \approx -0,808$$

e

$$y \geq 0 \Rightarrow -30 - 37t \geq 0 \Rightarrow 37t \leq -30 \Rightarrow t \leq -\frac{30}{37} \approx -0,811$$

Desse modo, para N ser natural devemos ter $t \leq -1, \; t \in \mathbb{Z}$. Porém a quantidade de soluções naturais para a equação $37x - 52y = 6$ é infinita e a questão inicial pede que N seja menor que 10000. Desse modo, os números N procurados são dados por

$$N = 52y + 15 = 52 \cdot (-30 - 37t) + 15 = -1560 - 1924t + 15 = -1545 - 1924t.$$

Para $N < 10000$, teremos

$$-1545 - 1924t < 10000 \Rightarrow 1924t > -11545 \Rightarrow t > -\frac{11545}{1924} \approx -6,0005$$

Logo, para $t \geq -6$ a equação $N = -1545 - 1924t$ resulta em um número $N < 10.000$. Assim, para que tenhamos o número N natural e menor que 10000 devemos ter

$$-1 \geq t \geq -6$$

ou seja,

$$t \in \{-6, -5, -4, -3, -2, -1\}.$$

Logo,

$$\begin{aligned}
&\text{para } t = -6, \quad N = -1545 - 1924 \cdot (-6) \Rightarrow N = 9999 \\
&\text{para } t = -5, \quad N = -1545 - 1924 \cdot (-5) \Rightarrow N = 8075 \\
&\text{para } t = -4, \quad N = -1545 - 1924 \cdot (-4) \Rightarrow N = 6151 \\
&\text{para } t = -3, \quad N = -1545 - 1924 \cdot (-3) \Rightarrow N = 4227 \\
&\text{para } t = -2, \quad N = -1545 - 1924 \cdot (-2) \Rightarrow N = 2303 \\
&\text{para } t = -1, \quad N = -1545 - 1924 \cdot (-1) \Rightarrow N = 379
\end{aligned}$$

Portanto, os possíveis valores naturais para N são: $379, 2303, 4227, 6151, 8075$ e 9999.

Problema 4

João pediu a Pedro que multiplicasse o dia de seu aniversário por 12 e o mês do aniversário por 31 e somasse os resultados. Pedro obteve 368. Qual é o produto do dia do aniversário de Pedro pelo mês de seu nascimento?

Solução. Como x representa o dia do aniversário de Pedro, temos que

$$1 \leq x \leq 31$$

e y representa o mês do seu aniversário, logo

$$1 \leq y \leq 12$$

A equação diofantina que representa o problema é a seguinte

$$12x + 31y = 368.$$

Agora, note que $mdc(12, 368) = 4$, porém 31 e 4 são primos entre si, desse modo, só resta uma opção para y: ser múltiplo de 4. Logo, de acordo com a restrição inicial de y, os possíveis valores que y pode assumir são $4, 8$ e 12. Substituindo tais valores na equação, obtemos,

$$\begin{aligned}
&\text{para } y = 4, \quad 12x + 31 \cdot 4 = 368 \Rightarrow 12x = 244 \Rightarrow x = \frac{61}{3} \notin \mathbb{Z} \\
&\text{para } y = 8, \quad 12x + 31 \cdot 8 = 368 \Rightarrow 12x = 120 \Rightarrow x = 10 \in \mathbb{Z} \\
&\text{para } y = 12, \quad 12x + 31 \cdot 12 = 368 \Rightarrow 12x = 4 \Rightarrow x = \frac{1}{3} \notin \mathbb{Z}
\end{aligned}$$

Portanto, somente $y = 8$ resultou em um valor inteiro para x. Logo o aniversário de Pedro é no dia 10 de agosto e o produto pedido é 80.

Problema 5

Numa criação de coelhos e galinhas, contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?

Solução. Sabemos que galinhas e coelhos possuem 2 e 4 pés, respectivamente. Então, seja x o número de galinhas e y o número de coelhos. Desse modo, como tem-se 400 pés ao todo, podemos representar com equação

$$2x + 4y = 400 \Rightarrow x + 2y = 200. \tag{3.5}$$

Como $mdc(1, 2) = 1$ e $1 \mid 200$ a equação possui solução. Assim, escrevendo 1 como combinação linear de 1 e 2, temos

$$1 = 2 \cdot 1 + 1 \cdot (-1)$$

Multiplicando a igualdade acima por 200, obtemos

$$200 \cdot 1 = 2 \cdot (1 \cdot 200) + 1 \cdot (-1 \cdot 200)$$

isto é

$$200 = 2 \cdot 200 + 1 \cdot (-200)$$

Assim, temos que $x_0 = -200$ e $y_0 = 200$ é uma solução particular de (3.5), logo sua solução geral é

$$x = -200 + 2t \;\text{ e }\; y = 200 - t, \quad \text{com } \; t \in \mathbb{Z}$$

Devemos ter x e y inteiros positivos, então

$$x \geq 0 \Rightarrow -200 + 2t \geq 0 \Rightarrow 2t \geq 200 \Rightarrow t \geq 100$$

e

$$y \geq 0 \Rightarrow 200 - t \geq 0 \Rightarrow t \leq 200$$

Desse modo,

$$100 \leq t \leq 200$$

Agora, fazendo $y - x$, obtemos

$$y - x = 200 - t - (-200 + 2t) = 400 - 3t$$

Buscamos a menor diferença entre y e x, então

$$400 - 3t > 0 \Rightarrow 400 > 3t \Rightarrow t < \frac{400}{3} \Rightarrow t < 133,\overline{3} \Rightarrow t = 133$$

Assim, para $t = 133$, temos

$$x = -200 + 2 \cdot 133 \Rightarrow x = -200 + 266 \Rightarrow x = 66$$

e

$$y = 200 - 133 \Rightarrow y = 67$$

Portanto, o número de coelhos é 67 e o número de galinhas é 66.

Problema 6

Mostre que nenhum número pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

Solução. De acordo com o Algoritmo da Divisão, dividindo um inteiro k por 12, obtemos um quociente x e resto 5, isto é

$$k = 12x + 5 \tag{3.6}$$

De maneira análoga, dividindo o mesmo k por 15, obtemos um quociente y e resto 4, ou seja

$$k = 15y + 4 \tag{3.7}$$

Agora, de (3.6) e (3.7), obtemos a seguinte equação diofantina

$$12x + 5 = 15y + 4 \Rightarrow 15y - 12x = 1$$

Note que o $mdc(15, 12) = 3$ e $3 \nmid 1$, portanto a equação não possui solução inteira. Provando que nenhum número satisfaz tais condições.

Problema 7

Camila possui R$ 500,00 depositados num banco. Duas operações bancárias são permitidas, retirar R$ 300,00 e depositar R$ 198,00. Essas operações podem ser repetidas quantas vezes Camila desejar, mas somente o dinheiro inicialmente depositado pode ser usado. Qual o maior valor que Camila pode retirar do banco?

Solução. De acordo com o enunciado, podemos representar o problema com a seguinte equação diofantina

$$198x - 300y = 500$$

onde x e y representam a quantidade das operações que Camila pode realizar.

Agora, como o $mdc(198, 300) = 6$ e $6 \nmid 500$, sabemos que ela não pode retirar todo o dinheiro depositado. O maior valor que ela pode retirar tem que ser um múltiplo de 6. Logo, o valor mais próximo da quantia depositada no banco, e fácil de ver, é 498. Portanto, o maior valor que Camila pode retirar é $R\$498,00$.

Problema 8

Um grupo de pessoas gastou 690 dólares num hotel. Sabendo que apenas alguns dos homens estavam acompanhados pelas esposas e que cada homem gastou 18 dólares e cada mulher gastou 15 dólares, determinar quantas mulheres e quantos homens estavam no hotel.

Solução. Sendo x e y a quantidade de homens e mulheres, respectivamente. Podemos representar o problema com a equação diofantina

$$18x + 15y = 690 \tag{3.8}$$

Fazendo,

$$y = \frac{690 - 18x}{15} \tag{3.9}$$

obtemos,

$$\begin{aligned} y &= \frac{690}{15} - \frac{18x}{15} = 46 - \frac{15x}{15} - \frac{3x}{15} \\ &= 46 - x - \frac{x}{5} \end{aligned}$$

Como x e y devem ser inteiros, $\frac{x}{5}$ também deve sê-lo. Então, para um inteiro t, segue

$$\frac{x}{5} = t \Rightarrow x = 5t$$

Agora, substituindo o valor de x em (3.9), obtemos

$$y = \frac{690 - 18x}{15} = \frac{690 - 18 \cdot 5t}{15} = 46 - 6t$$

Além de x e y serem inteiros, eles também devem ser positivos. Assim,

$$x = 5t > 0 \Rightarrow t > 0$$

e

$$y = 46 - 6t > 0 \Rightarrow 6t < 46 \Rightarrow t < \frac{46}{6} \Rightarrow t < 7,6$$

ou seja,

$$0 < t < 7,6$$

Portanto, atribuindo os possíveis valores de t, obtemos

$$\text{para } t = 1, \quad x = 5 \cdot 1 = 5 \text{ e } y = 46 - 6 \cdot 1 = 40$$

$$\text{para } t = 2, \quad x = 5 \cdot 2 = 10 \text{ e } y = 46 - 6 \cdot 2 = 34$$

$$\text{para } t = 3, \quad x = 5 \cdot 3 = 15 \ \text{ e } \ y = 46 - 6 \cdot 3 = 28$$

$$\text{para } t = 4, \quad x = 5 \cdot 4 = 20 \ \text{ e } \ y = 46 - 6 \cdot 4 = 22$$

$$\text{para } t = 5, \quad x = 5 \cdot 5 = 25 \ \text{ e } \ y = 46 - 6 \cdot 5 = 16$$

$$\text{para } t = 6, \quad x = 5 \cdot 6 = 30 \ \text{ e } \ y = 46 - 6 \cdot 6 = 10$$

$$\text{para } t = 7, \quad x = 5 \cdot 7 = 35 \ \text{ e } \ y = 46 - 6 \cdot 7 = 4$$

Portanto, apenas $t = 5, 6$ e 7 resulta valores de x e y que satisfazem a hipótese de que há mais homens que mulheres no hotel, tendo em vista que apenas alguns dos homens estavam com suas esposas.

Problema 9

Um fazendeiro comprou cem animais por um custo total de R$4.000, 00. Os preços desses animais foram os seguintes: bezerros, R$120, 00 cada um; cordeiros, R$50, 00 cada um; e porcos, R$25, 00 cada um. Se o fazendeiro obteve ao menos um animal de cada espécie, qual a quantidade comprada de cada uma delas?

Solução. Sejam x, y e z as quantidades de bezerros, cordeiros e porcos comprados, respectivamente. A equação diofantina que representa o problema é

$$120x + 50y + 25z = 4000 \tag{3.10}$$

Onde $a_1 = 120, a_2 = 50, a_3 = 25, b = 4000$ e o $mdc(120, 50, 25) = 5$ e $5 \mid 4000$, logo a equação possui solução. Então, seja $t = 120x + 25z$, donde

$$t + 50y = 4000 \tag{3.11}$$

Note que o $mdc(1, 50) = 1$ e $1 \mid 4000$, logo a equação possui solução e podemos obter uma solução de maneira direta. Fazendo $y = 1$, obtemos $t = 4000 - 50 = 3950$. Assim, $t_0 = 3950$ e $y_0 = 1$ é solução particular de (3.11) e sua solução geral é dada por

$$t = 3950 + 50k \ \text{ e } \ y = 1 - k, \quad \text{com} \ \ k \in \mathbb{Z}.$$

Agora, temos

$$120x + 25z = t = 3950 + 50k \tag{3.12}$$

Para que essa equação possua solução é necessário que o $mdc(120, 25) = 5$ divida $3950+50k$. Assim, pelo Altoritmo de Euclides, segue

$$\begin{aligned}
120 &= 25 \cdot 4 + 20 \Rightarrow 20 = 120 - 25 \cdot 4 \\
25 &= 20 \cdot 1 + 5 \Rightarrow 5 = 25 - 20 \\
20 &= 5 \cdot 4 + 0
\end{aligned}$$

fazendo as devidas substituições, obtemos

$$5 = 25 - (120 - 25 \cdot 4) = 25 - 120 + 25 \cdot 4 = 120 \cdot (-1) + 25 \cdot 5$$

ou seja,

$$5 = 120 \cdot (-1) + 25 \cdot 5$$

Agora, multiplicando ambos os membros da igualdade acima por $\dfrac{3950 + 50k}{5}$, obtemos

$$\begin{aligned}
5 \cdot \left(\frac{3950 + 50k}{5}\right) &= 120 \cdot \left[(-1) \cdot \left(\frac{3950 + 50k}{5}\right)\right] + 25 \cdot \left[5 \cdot \left(\frac{3950 + 50k}{5}\right)\right] \\
3950 + 50k &= 120 \cdot \left(\frac{-3950 - 50k}{5}\right) + 25 \cdot (3950 + 50k)
\end{aligned}$$

Logo, a solução geral de (3.12) é

$$x = \left(\frac{3950 + 50k}{5}\right) + \frac{25}{5}\lambda \ \text{ e } \ z = 3950 + 50k - \frac{120}{5}\lambda$$

isto é,

$$x = -790 - 10k + 5\lambda \ \text{ e } \ z = 3950 + 50k - 24\lambda$$

Assim, a solução geral de (3.10) é

$$x = -790 - 10k + 5\lambda, \ \ y = 1 - k \ \text{ e } \ z = 3950 + 50k - 24\lambda, \ \ \text{com} \ \ k, \lambda \in \mathbb{Z}.$$

Agora, perceba que

$$\begin{aligned}
x + y + z &= -790 - 10k - 5\lambda + 1 - k + 3950 + 50k = 24\lambda \\
&= 39k - 19\lambda + 3161
\end{aligned}$$

Mas, por hipótese temos que *"um fazendeiro comprou cem animais"*, logo $x + y + z = 100$, desse modo

$$39k - 19\lambda + 3161 = 100 \Rightarrow 39k - 19\lambda = -3061 \tag{3.13}$$

Obtemos uma equação diofantina nas variáveis k e λ. Onde o $mdc(39, 19) = 1$ e $1 \mid -3061$, desse modo a equação possui solução. Escrevendo 1 como combinação linear de 39 e 19, obtemos

$$39 = 19 \cdot 2 + 1 \Rightarrow 1 = 39 \cdot 1 - 19 \cdot 2$$

Multiplicando toda a igualdade acima por -3061, segue

$$-3061 = 39 \cdot (-3016) - 19 \cdot (6122)$$

logo, $k_0 = -3061$ e $\lambda_0 = -6122$ é solução particular de (3.13) e sua solução geral é

$$k = -3061 - 19t \;\text{ e }\; \lambda = -6122 - 39t, \;\; \text{com} \;\; t \in \mathbb{Z}.$$

Agora, ao substituir estas expressões na solução geral de (3.10), podemos expressar x, y e z com o parâmetro t apenas. Então, temos

$$\begin{aligned}
x &= -790 - 10 \cdot (-3061 - 19t) + 5 \cdot (-6122 - 39t) \\
&= -790 + 30610 + 190t - 30610 - 195t \\
&= -790 - 5t, \\
y &= 1 - (-3061 - 19t) \\
&= 1 + 3061 + 19t \\
&= 3062 + 19t, \\
z &= 3950 + 50 \cdot (-3061 - 19t) - 24 \cdot (-6122 - 39t) \\
&= 3950 - 153050 - 950t + 146928 + 936t \\
&= -2172 - 14t,
\end{aligned}$$

ou seja,

$$x = -5t - 790, \;\; y = 19t + 3062 \;\text{ e }\; z = -14t - 2172$$

É claro que x, y e z devem ser maiores ou iguais a 1. Desse modo, vamos determinar quais são os valores de t que são condizentes. Então,

$$x \geq 1 \Rightarrow -5t - 790 \geq 1 \Rightarrow 5t \leq -791 \Rightarrow t \leq \frac{-791}{5} \Rightarrow t \leq -159,$$
$$y \geq 1 \Rightarrow 19t + 3062 \geq 1 \Rightarrow 19t \geq -3061 \Rightarrow t \geq \frac{-3061}{19} \Rightarrow t \geq -161,$$
$$z \geq 1 \Rightarrow -14t - 2172 \geq 1 \Rightarrow 14 \leq -2173 \Rightarrow t \leq \frac{-2173}{14} \Rightarrow t \leq -156$$

Portanto,

$$-161 \leq t \leq -156$$

Logo, atribuindo os valores de t, obtemos

para $t = -161$,

$$x = -5 \cdot (-161) - 790 = 805 - 790 = 15,$$
$$y = 19 \cdot (-161) + 3062 = -3059 + 3062 = 3,$$
$$z = -14 \cdot (-161) - 2172 = 2254 - 2172 = 82,$$

para $t = -160$,

$$x = -5 \cdot (-160) - 790 = 800 - 790 = 10,$$
$$y = 19 \cdot (-160) + 3062 = -3040 + 3062 = 22,$$
$$z = -14 \cdot (-160) - 2172 = 2240 - 2172 = 68,$$

para $t = -159$,

$$x = -5 \cdot (-159) - 790 = 795 - 790 = 5,$$
$$y = 19 \cdot (-159) + 3062 = -3021 + 3062 = 41,$$
$$z = -14 \cdot (-159) - 2172 = 2226 - 2172 = 54,$$

para $t = -158$,

$$x = -5 \cdot (-158) - 790 = 790 - 790 = 0,$$
$$y = 19 \cdot (-158) + 3062 = -3002 + 3062 = 60,$$
$$z = -14 \cdot (-158) - 2172 = 2212 - 2172 = 40,$$

para $t = -157$,

$$x = -5 \cdot (-157) - 790 = 785 - 790 = -5,$$

$$y = 19 \cdot (-157) + 3062 = -2983 + 3062 = 79,$$

$$z = -14 \cdot (-157) - 2172 = 2198 - 2172 = 26,$$

para $t = -156$,

$$x = -5 \cdot (-156) - 790 = 785 - 790 = -10,$$

$$y = 19 \cdot (-156) + 3062 = -2964 + 3062 = 98,$$

$$z = -14 \cdot (-156) - 2172 = 2184 - 2172 = 12.$$

Portanto, como devemos ter x, y e y maiores ou iguais a 1, apenas os valores de $t = -161, -160$ e -159 satisfazem as condições do problema, logo, as possibilidades de compra são:

5 bezerros, 41 cordeiros, 54 porcos,

10 bezerros, 22 cordeiros, 68 porcos,

15 bezerros, 3 cordeiros, 82 porcos.

Considerações Finais

Neste trabalho, realizamos um estudo acerca das equações diofantinas lineares, tanto em duas, quanto em três variáveis. Acreditamos que nosso objetivo foi alcançado, pois o intuito deste é servir como fonte de estudo para estudantes do ensino básico e, também, de auxílio para estudantes do ensino superior a nível de graduação, pois vimos alguns detalhes adicionais, quanto às equações diofantinas, além do que é visto durante um primeiro curso de Teoria dos Números.

Buscamos apresentar alguns dos resultados mais importantes da teoria dos números que servem como base para o entendimento e a resolução das equações diofantinas lineares, para que não houvesse eventuais perdas no entendimento o que culminaria numa má compreensão do tema.

Futuramente, pretendemos expandir a resolução destas equações, agora para n variáveis, por meio da generalização do caso apresentado aqui para três variáveis.

Referências Bibliográficas

[1] ANDREESCU, T., ANDRICA, D., CUCUREZEANU, I. *An Introduction to Diophantine Equations: A Problem-Based Approach*. Springer Science & Business Media, 2010

[2] EVES, H. *Introdução à história da matemática*. Campinas: Editora da Unicamp, 2004.

[3] HEFEZ, A. *Elementos de Aritmética*. Rio de Janeiro: SBM, 2011.

[4] MILIES, C. P., COELHO, S. P. *Números: Uma introdução à Matemática*. São Paulo: Editora da Universidade de São Paulo, 2003.

[5] VIEIRA, V. L. *Um Curso Básico em Teoria dos Números*. Campina Grande/São Paulo: Editora da Universidade Estadual da Paraíba (Coedição: Editora Livraria da Física), 2015.