

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

LICENCIATURA EM MATEMÁTICA À DISTÂNCIA

Cyntia Magalhães Lima

EQUAÇÕES DIOFANTINAS: métodos de resolução e aplicações

Uberlândia - MG

2021

Cyntia Magalhães Lima

EQUAÇÕES DIOFANTINAS: métodos de resolução e aplicações

Trabalho de conclusão de curso
apresentado a Faculdade de
Matemática, UFU, como requisito
parcial para obtenção do título de
Licenciado em Matemática, sob a
orientação do Prof. Dr. Juliano
Gonçalves Oler.

Uberlândia - MG

2021

Cyntia Magalhães Lima

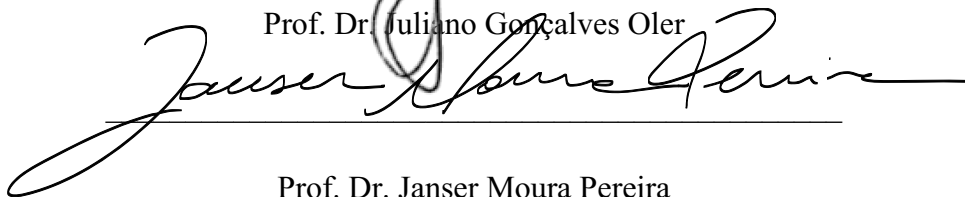
EQUAÇÕES DIOFANTINAS: métodos de resolução e aplicações

Trabalho de conclusão de curso
apresentado a Faculdade de
Matemática, UFU, como requisito
parcial para obtenção do título de
Licenciado em Matemática, sob a
orientação do Prof. Dr. Juliano
Gonçalves Oler.

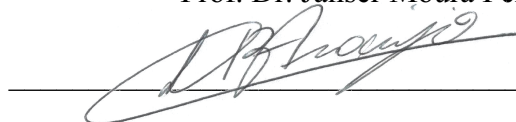
BANCA EXAMINADORA



Prof. Dr. Juliano Gonçalves Oler



Prof. Dr. Janser Moura Pereira



Prof. Dr. Lúcio Borges de Araújo

RESUMO

Equações diofantinas são equações polinomiais, com qualquer número de incógnitas, com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções também entre os inteiros. Neste trabalho trata-se das equações diofantinas lineares de n variáveis, objetivando explorar diferentes métodos de resolução, incluindo o conhecido método através da utilização do algoritmo de Euclides, e também o método das sucessivas extrações de inteiros. Além disso, mostra-se aplicações destas equações na resolução de alguns problemas relacionados com os números inteiros, ressaltando a importância do ensino de equações diofantinas no ensino regular, principalmente para alunos do ensino médio, tendo em vista que tal conteúdo matemático está constantemente presente em provas de vestibulares de todo o país, concursos públicos e também nas provas da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP).

Palavras chave: Algoritmo de Euclides; Máximo divisor comum; Resolução de problemas; Módulo; Inteiros.

SUMÁRIO

INTRODUÇÃO	06
CAPÍTULO 1: CONCEITOS E FERRAMENTAS PRELIMINARES	08
1.1 - Números inteiros	08
1.2 - Máximo divisor comum	11
1.3 - Números primos	13
1.4 - Algoritmo de Euclides	15
CAPÍTULO 2: EQUAÇÕES DIOFANTINAS: MÉTODO CLÁSSICO DE RESOLUÇÃO	19
2.1 - Equações diofantinas lineares com duas variáveis	19
2.2 - Equações diofantinas lineares com três variáveis	23
2.3 - Equações diofantinas lineares com n variáveis	25
CAPÍTULO 3: EQUAÇÕES DIOFANTINAS: RESOLUÇÃO ATRAVÉS DO PROCESSO DAS SUCESSIVAS EXTRAÇÕES DE INTEIROS	30
3.1 - Condição de existência de soluções inteiras da equação $ax + by = c$	30
3.2 - Cálculo das soluções inteiras da equação $ax + by = c$	33
3.3 - Condições de existência de soluções inteiras de m equações com $m + 2$ incógnitas	36
CAPÍTULO 4: EXPLORANDO O ENSINO DE EQUAÇÕES DIOFANTINAS LINEARES NO ENSINO MÉDIO	42
4.1 - Descrição da primeira atividade	43
4.2 - Descrição da segunda atividade	47
4.3 - Descrição da terceira atividade	49
CONSIDERAÇÕES FINAIS	53
REFERÊNCIAS	54

INTRODUÇÃO

Diofante de Alexandria viveu provavelmente no século III d.C. Dele se conhecem duas obras: *Sobre números poligonais* (da qual sobreviveram apenas fragmentos) e *Arithmetica*. Desta última restam seis livros em grego e quatro em árabe, a qual é a mais importante e original. Trata-se de uma coletânea de problemas, na maioria indeterminados, para cuja solução Diofante usa sempre métodos algébricos, com o que se distingue substancialmente da matemática grega clássica (DOMINGUES, 2017).

Segundo Domingues (2017, pg. 145) devido à *Arithmetica*, de Diofante, hoje recebem o nome de equações diofantinas todas as equações polinomiais (com qualquer número de incógnitas), com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções também entre os inteiros. Isso embora Diofante só tenha estudado algumas dessas equações e se limitado a encontrar uma solução apenas no conjunto dos números racionais positivos.

Segundo Boyer (2003, pg. 130) pouco se sabe sobre a vida de Diofante de Alexandria, além de uma tradição referida numa coleção de problemas datando do quinto ou sexto século, chamada Antologia Grega, citada abaixo,

Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem: Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança tardia: depois de chegar à medida da metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida.

Se este enigma é historicamente exato, Diofante viveu oitenta e quatro anos. Considerando os anos vividos por Diofante como D , tem-se:

$$\frac{D}{6} + \frac{D}{12} + \frac{D}{7} + 5 + \frac{D}{2} + 4 = D$$

o que aplicando o máximo divisor comum (mdc) resulta em $D = 84$.

Uma interessante aplicação do conceito de máximo divisor comum (mdc) e do algoritmo da divisão pode ser observada na resolução das equações diofantinas lineares. Embora o aluno do ensino fundamental tenha em seu conteúdo programático a definição e aplicação do máximo divisor comum, muitos alunos terminam o ensino básico sem conhecer soluções de equações diofantinas lineares básicas. Dessa forma propõe-se este trabalho para

explorar o conceito e métodos de resolução para equações diofantinas de n variáveis, além de algumas aplicações dessas equações em problemas relacionados com o cotidiano.

No capítulo 1 serão apresentadas ferramentas básicas usadas para a resolução das equações diofantinas lineares, mais especificamente enunciado e a demonstração de divisão nos inteiros, máximo divisor comum, números primos e algoritmo de Euclides.

No capítulo 2 será mostrado como pode-se encontrar soluções de equações diofantinas lineares com n variáveis, utilizando o método “tradicional”, no qual a equação diofantina somente admite solução se, e somente se, $d = \text{mdc}(a,b)$ divide c .

No capítulo 3 será apresentado o método de resolução para equações diofantinas lineares com n variáveis, no qual isola-se a variável que tem o menor coeficiente em módulo, efetua-se algumas divisões e introduz-se uma equação auxiliar construída com coeficientes formados pelos restos das divisões.

No capítulo 4 serão aplicados os conhecimentos e técnicas, apresentadas nos capítulos anteriores, na interpretação e resolução de problemas que envolvem números inteiros, sendo feita também a comparação das estratégias de resolução utilizando os métodos apresentados. Serão apresentadas situações-problemas nas quais a utilização de equações diofantinas lineares é meio de resolução, sendo tais questões formuladas para aplicação com alunos do ensino médio.

1 CONCEITOS E FERRAMENTAS PRELIMINARES

1.1 Números inteiros

Os algarismos que usamos hoje em dia surgiram na Índia, por volta do século VII, e sua difusão pelo mundo se deve aos árabes. Por este motivo, tais algarismos são chamados de “indo-arábicos”. A forma de se grafar tais símbolos foi se alterando ao longo dos anos e a forma atual mal se assemelha à original. O que de fato importa é que foi na Índia, quando o ocidente estava imerso na estagnação e na ignorância da primeira fase do período medieval, que as raízes de nosso sistema de numeração posicional começaram a brotar. Inclusive o zero, que mesmo entre os gregos do período alexandrino era usado apenas para indicar “ausência”, com os hindus alcançou o *status* pleno de número (DOMINGUES, 2017).

Segundo Domingues (2017, pg. 113) os números negativos surgiram inicialmente na China, há mais de dois milênios. Já por essa época, os chineses conheciam as regras de sinais para a adição e subtração. Mas não há registros, na Matemática chinesa, do uso da regra de sinais da multiplicação antes do século XIII. Mais tarde, ou por algum contato com a cultura chinesa ou independentemente, os hindus introduziram os números negativos em sua Matemática. O objetivo inicial era indicar débitos. O primeiro registro do uso de números negativos na Índia, de que se tem notícia, aparece na obra do matemático e astrônomo hindu Brahmagupta, que já conhecia inclusive as regras de sinais para as quatro operações com números negativos.

Ao introduzirem os números negativos, os hindus não tinham nenhuma preocupação de ordem teórica. Na verdade, os progressos matemáticos verificados na Índia por essa época ocorreram por razões práticas e sem preocupações com rigor e formalismo.

Segundo Domingues (2017, pg. 114) num enfoque informal, os novos números, correspondentes às diferenças $a - b$ ($a < b$), são interpretados intuitivamente (como débitos, por exemplo) e agregados a $\mathbb{N}$. Do resultado dessa união, surge o conjunto dos números inteiros. Como é lícito admitir que se deva ter $0 - 1 = 1 - 2 = 2 - 3 = \dots$, pode-se indicar cada uma dessas diferenças por -1 . De modo análogo, surgem $-2, -3, -4, \dots$. Se por questão de uniformidade passarmos a escrever $1 = +1, 2 = +2, \dots$, o conjunto dos números inteiros, que será indicado por $\mathbb{Z}$, será dado por:

$$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, +1, +2, +3, \dots \}.$$

Definição 1. (veja [1]) Dados a e b números inteiros, diremos que a divide b e denotaremos por $a|b$, quando existir um $k \in \mathbb{Z}$, tal que $b = ka$. A negação dessa sentença é denotada por $a \nmid b$.

Conclui-se da definição que se a é um divisor de b , então consequentemente, b é divisível por a , ou ainda, que b é múltiplo de a . Será a um divisor de b , se $a|b$ e $a > 0$.

Exemplo 1. $5|20$, pois existe um inteiro $k = 4$, tal que $20 = 5.4$.

Exemplo 2. $5 \nmid 28$, pois não existe um inteiro k que satisfaça $28 = 5.k$.

Proposição 1. (veja [1]) Sejam a , b e c números inteiros. Se $a|b$ e $b|c$, então $a|c$.

Demonstração. Considere números a , b e c inteiros tais que $a|b$ e $b|c$. Assim existem $k_1, k_2 \in \mathbb{Z}$ tais que $b = ak_1$ e $c = bk_2$. Logo, $c = (ak_1)k_2 = a(k_1k_2)$. Como $k_1, k_2 \in \mathbb{Z}$, tem-se que $k_1.k_2 \in \mathbb{Z}$. Portanto, $a|c$.

Exemplo 3. Como $3|27$ e $27|19683$, então $3|19683$. De fato,

$$27 = 3.3.3 \text{ e } 27.27.27 = 19683 \Rightarrow 3.3.3.27.27 = 19683.$$

Logo $3|19683$.

Proposição 2. (veja [1]) Sejam a , b e c números inteiros, tais que $a|b$ e $a|c$. Então $a|(mb + nc)$, para quaisquer $m, n \in \mathbb{Z}$.

Demonstração. São números a , b e c inteiros tais que $a|b$ e $a|c$, então existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = ak_2$. Multiplicando ambas as equações respectivamente por m e n obtém-se:

$$mb = mak_1 \tag{1.1}$$

e

$$nc = nak_2 \tag{1.2}$$

Combinando as equações (1.1) e (1.2), tem-se que:

$$mb + nc = mak_1 + nak_2 = a(mk_1 + nk_2).$$

Como m, k_1, n e $k_2 \in \mathbb{Z}$ tem-se que $mk_1 + nk_2 \in \mathbb{Z}$. Portanto, $a|(mb + nc)$.

Exemplo 4. Como $5|20$ e $5|15$, então $5|(5 \cdot 20 + (-6) \cdot 15)$. Note que, $5 \cdot 20 + (-6) \cdot 15 = 10$.

Teorema 1. (veja [1]) (Algoritmo da divisão em $\mathbb{Z}$ ou Algoritmo de Euclides) Dados a e b números inteiros, sendo b um número inteiro positivo, existe um único par de números inteiros q e r que satisfazem $a = q \cdot b + r$, com $0 \leq r < b$.

Demonstração. Considere b , um número inteiro positivo e não nulo. Se $a \in \mathbb{Z}$, então ou a é múltiplo de b ou a está situado entre dois múltiplos consecutivos de b , isto é, $qb \leq a < (q+1)b$.

Adicionando $-qb$ em todos os termos da desigualdade obtém-se:

$$qb - qb \leq a - qb < qb + b - qb, 0 \leq a - qb < b \quad (1.3)$$

Assim, fazendo $r = a - qb$, pode-se escrever também $a = qb + r$, em que $0 \leq r < b$. Supondo que existam inteiros q_1, q_2, r_1, r_2 , onde $q_1 \neq q_2$ e $r_1 \neq r_2$ e que satisfaçam às igualdades:

$$a = q_1b + r_1, \text{ com } 0 \leq r_1 < b \quad (1.4)$$

e

$$a = q_2b + r_2, \text{ com } 0 \leq r_2 < b \quad (1.5)$$

Suponha, sem perda de generalidade que $r_2 > r_1$ se $b > r_1$ e $b > r_2$, fazendo $b > r_2 - r_1$ e comparando (1.4) e (1.5) tem-se que: $a = bq_1 + r_1 = bq_2 + r_2$. Isolando $r_2 - r_1$, obtém-se: $b(q_2 - q_1) = r_2 - r_1$. Chamando de $t = (q_2 - q_1)$, segue que $r_2 - r_1 = tb$, com $t \in \mathbb{Z}$. Assim, tem-se que $b|(r_2 - r_1)$.

Portanto, $b \leq (r_2 - r_1)$, só se $r_2 > r_1$ o que é um absurdo, pois contradiz o fato de $b > r_2 - r_1$. Logo, $r_2 = r_1$.

Conclui-se que $(q_2 - q_1)b = 0$. Sendo $b \neq 0$, tem-se que $(q_2 - q_1) = 0 \Rightarrow q_2 = q_1$. Na equação $a = q \cdot b + r$, com $0 \leq r < b$, os inteiros, q e r são chamados, respectivamente, de quociente e resto da divisão de a por b . Vale lembrar que b somente é divisor de a se $r = 0$. Neste caso, tem-se que $a = bq$ e o quociente de q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$ ou $a|b$.

Exemplo 5. Numa divisão de 396 por $b > 0$, o quociente é 13 e o resto é r . Determine os possíveis valores para b e r .

Solução. Sabe-se que na divisão de a por b tem-se que $a = q \cdot b + r, 0 \leq r < b$. Então pode-se escrever:

$$396 - 13b + r, \text{ com } 0 \leq r < b. \quad (1.6)$$

Assim,

$$r = 396 - 13b, \text{ com } 0 \leq r < b. \quad (1.7)$$

Da inequação (1.7) obtém-se:

$$0 \leq 396 - 13b < b. \quad (1.8)$$

Desmembrando a inequação (1.8) tem-se:

$$0 \leq 396 - 13b \text{ e } 396 - 13b < b, \quad (1.9)$$

De (1.9) tem-se:

$$13b \leq 396 \text{ e } 14b > 396.$$

Logo, isolando b conclui-se que: $28,29 < b \leq 30,46$.

Além disso, procura-se apenas valores inteiros para b e r , os possíveis valores são:

$$b = 29 \text{ e } r = 19 \text{ ou } b = 30 \text{ e } r = 6.$$

1.2 Máximo divisor comum

Definição 2. (veja [\[5\]](#)) Chama-se divisor comum de dois inteiros a e b , todo inteiro $d \neq 0$, tal que $d|a$ e $d|b$.

Desta definição segue que para a, b, m e n inteiros com $d|a$ e $d|b$, então $d|(am + bn)$.

Exemplo 6. Os números 1, 3, 5, e 15 são divisores comuns de 30 e 45.

Definição 3. (veja [\[5\]](#)) Sejam a e b inteiros não simultaneamente nulos. Chama-se máximo divisor comum de a e b o inteiro $d > 0$ que satisfaz as condições:

- (i) d é um divisor comum de a e de b , e
- (ii) d é divisível por todo divisor comum de a e b , e
- (iii) se c é um divisor comum de a e b , então $c|d$.

Portanto, se d é um mdc de a e b , e c é um divisor comum desses números, então $c \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que se d e d' são dois mdc de um mesmo par de números, então $d \leq d'$ e $d' \leq d$, e, conseqüentemente, $d = d'$. Ou seja, o mdc de dois números, quando existe, é único.

O mdc de a e b , quando existe é denotado por (a, b) , e como o mdc de a e b não depende da ordem em que a e b são tomados, tem-se que $(a, b) = (b, a)$. Se d é máximo divisor comum entre a e b , então d também é máximo divisor comum entre a e $-b$, $-a$ e b , e ainda, entre $-a$ e $-b$.

Esta definição de mdc para inteiros a e b vale também para uma quantidade finita de inteiros $a_1, a_2, a_3, \dots, a_n$, como por exemplo o mdc entre três números

$$mdc(a_1, a_2, a_3) = mdc(mdc(a_1, a_2), a_3) = mdc(a_1, mdc(a_2, a_3)).$$

Definição 4. (veja [1]) Dados a e b dois inteiros não nulos. Diz-se que a e b são primos entre si se, e somente se, $mdc(a, b) = 1$.

Exemplo 7. Os inteiros 3 e 7, 9 e 11 são primos entre si. Tem-se que $mdc(3, 7) = 1$ e $mdc(9, 11) = 1$. Logo, 3 e 7, 9 e 11, são primos entre si.

Teorema 2. (veja [1]) Dados $a, b \in \mathbb{Z}$, ambos não nulos, e seja $t = mdc(a, b)$. Então, existem $x_1, y_1 \in \mathbb{Z}$ tais que: $ax_1 + by_1 = t$, ou seja, t é uma combinação linear de a e b .

Demonstração. Seja o conjunto:

$$S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Consideremos primeiro a não nulo. Fazendo-se $y = 0$ e $x = 1$, se $a > 0$, $x = -1$, se $a < 0$, tem-se que $ax + by = a(\pm 1) + b \cdot 0 = |a| > 0$ o que nos mostra que S não é vazio. Agora se $a = 0$, então $ax + by = 0 \cdot x + b(\pm 1) = |b|$. O que mostra que S é também não vazio.

Usando o princípio da indução, existe um $t \in S$ minimal. Se $t \in S$ temos $t > 0$ e existem $x_1, y_1 \in \mathbb{Z}$ tais que:

$$t = ax_1 + by_1 \quad (1.10)$$

Assim pode-se afirmar que t é o $\text{mdc}(a, b)$. Escrevendo a divisão de a por t com resto: $\exists q, r \in \mathbb{Z}$ tais que:

$$a = qt + r \text{ e } 0 \leq r < t.$$

Logo, $r = a - q \cdot t$, substituindo (1.10), tem-se $r = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1)$. Se fosse $r > 0$ poder-se-ia concluir que $r \in S$, o que é um absurdo, pois $r < t$ e t é o elemento minimal de S . Logo $r = 0$ e $a = qt$ o que significa que t divide a . Analogamente, pode-se mostrar que $t|b$. Portanto, t é o divisor comum de a e b . Conclui-se que $t = \text{mdc}(a, b)$.

Portanto, as combinações lineares de a e b , são exatamente os múltiplos do $\text{mdc}(a, b)$. Chamemos $L = \{ax + by/x, y \in \mathbb{Z}\}$ e $S = \{tz/z \in \mathbb{Z}\}$. Pelo teorema 2, sabe-se que existem $x_1, y_1 \in \mathbb{Z}$ tais que $t = ax_1 + by_1$. Para todos $z \in \mathbb{Z}$, segue:

$$tz = (ax_1z) + (by_1z) \in L.$$

Logo $S \subseteq L$. Como $t|(ax + by)$ para qualquer $ax + by \in L$, tem-se que $L \subseteq S$. Então $L = S$, ou seja:

$$\{ax + by/x, y \in \mathbb{Z}\} = \{tz/z \in \mathbb{Z}\}.$$

1.3 Números primos

Proposição 3. Sejam $a, b \in \mathbb{Z}$, não nulos. Então $\text{mdc}(a, b) = 1$ se, e somente se, existirem $x_1, y_1 \in \mathbb{Z}$ tais que: $ax_1 + by_1 = 1$.

Demonstração. Se $\text{mdc}(a, b) = 1$, então existem $x_1, y_1 \in \mathbb{Z}$ com $ax_1 + by_1 = 1$ pelo Teorema 2. Seja $ax + by = 1$, com $x, y \in \mathbb{Z}$. Se $t|a$ e $t|b$, pode-se concluir que $t|1$. Portanto, $t = 1$, ou seja, $\text{mdc}(a, b) = 1$.

Desta caracterização dos números primos entre si, surgem algumas consequências:

Proposição 4. Dados $a, b \in \mathbb{Z}$, não nulos, e $t = \text{mdc}(a, b)$. Então,

$$\text{mdc}\left(\frac{a}{t}, \frac{b}{t}\right) = 1, \text{ sendo } \frac{a}{t}, \frac{b}{t} \in \mathbb{Z}.$$

Demonstração. Se $ax + by = t$ para certos $x, y \in \mathbb{Z}$, dividindo-se todos os membros da equação por t , obtém-se:

$$\frac{ax}{t} + \frac{by}{t} = \frac{t}{t} \Rightarrow \frac{a}{t}x + \frac{b}{t}y = 1.$$

Pela proposição 3, conclui-se a afirmação.

Proposição 5. (veja [1]) Sejam $a, b, c \in \mathbb{Z}$, tais que $a|c$ e $b|c$. Se $\text{mdc}(a, b) = 1$ então $ab|c$.

Demonstração. Suponha que $a|b$ e $b|c$ então existem r e s inteiros, tais que:

$$ar = c = bs. \quad (1.11)$$

Além disso, com o $\text{mdc}(a, b) = 1$ existem x e y tais que:

$$ax + by = 1. \quad (1.12)$$

Multiplicando a equação (1.12) por c obtém-se:

$$c = cax + cby. \quad (1.13)$$

Substituindo os valores da equação (1.11) no lado direito da equação (1.13) tem-se que:

$$c = (bs)ax + (ar)by.$$

Ou seja, $c = ab(sx + ry)$, com $sx + ry \in \mathbb{Z}$.

Portanto, $ab|c$.

Proposição 6. (veja [1]) (Lema de Euclides) Dados $a, b, c \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = 1$ e $a|bc$. Então $a|c$.

Demonstração. Suponha que $a|bc$. Então existe $r \in \mathbb{Z}$, tal que:

$$ar = bc. \quad (1.14)$$

Além disso, como $\text{mdc}(a, b) = 1$, existem x e y inteiros, tais que:

$$ax + by = 1. \quad (1.15)$$

Multiplicando a equação (1.15) por c , obtém-se:

$$c = cax + cby. \quad (1.16)$$

Substituindo o valor da equação (1.14) na equação (1.16), tem-se que:

$$c = cax + ary \Rightarrow c = a(cx + ry) \text{ com } cx + ry \in \mathbb{Z}.$$

Portanto, $a|c$.

1.4 Algoritmo de Euclides

Segundo (HEFEZ, 2014) mesmo quando um número natural a não divide o número natural b , Euclides, nos seus Elementos, utiliza, sem enuncia-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a , com resto. Este resultado, não só é importante instrumento na obra de Euclides, como também é um resultado central da teoria.

Será apresentado um efetivo método para calcular o *mdc*, máximo divisor comum, entre dois números. O método é chamado de Algoritmo de Euclides, que constitui a aplicação de sucessivas divisões. Esse algoritmo é uma importante ferramenta da Teoria dos Números.

Sejam a e b , não nulos, com $a > 0$. Aplicando a divisão Euclidiana de b por a , tem-se:

$$b = aq_1 + r_1, 0 \leq r_1 < a.$$

Procedendo a divisão euclidiana de a por r_1 , tem-se:

$$a = r_1q_2 + r_2, 0 \leq r_2 < r_1.$$

Em seguida, faz a divisão euclidiana sucessivamente:

$$r_1 = r_2q_3 + r_3, 0 \leq r_3 < r_2$$

$\vdots$

$$r_n = r_{(n+1)}q_{(n+2)} + r_{(n+2)}, 0 \leq r_{(n+2)} < r_{(n+1)}.$$

Essa sucessão (r_n) é estritamente decrescente de inteiros positivos ou nulos, após p etapas, $r_p = 0$, tem se:

$$r_{(p-3)} = r_{(p-2)}q_{(p-1)} + r_{(p-1)}, 0 \leq r_{(p-1)} < r_{(p-2)}$$

$$r_{(p-2)} = r_{(p-1)}q_p + 0, 0 \leq r_p < r_{(p-1)}$$

$$r_{(p-1)} = r_p \cdot q_{(p+1)}.$$

Esse é o procedimento de cálculo do *mdc*, chamado de Algoritmo de Euclides: o último resto, não nulo, encontrado no algoritmo de Euclides, é o máximo divisor comum de a e b , pois só pode efetuar a divisão euclidiana enquanto $r_n \neq 0$ e nesse caso, tem-se que $r_1 > r_2 > \dots > r_n > 0$.

Pelo princípio da Boa Ordenação, é impossível ter uma sequência infinita: $r_1 > r_2 > \dots > r_n > \dots > 0$.

Logo, a um certo ponto tem-se $r_n = 0$.

Seja n , o maior índice para o qual $r_n \neq 0$, portanto $r_{(n+1)} = 0$. Prova-se o seguinte:

$$\text{mdc}(a, b) = r_n.$$

Então:

$$\text{mdc}(a, b) = \text{mdc}(a, b - aq_1) = \text{mdc}(a, r_1)$$

$$\text{mdc}(a, r_1) = \text{mdc}(r_1, a - r_1q_2) = \text{mdc}(r_1, r_2)$$

$$\text{mdc}(r_1, r_2) = \text{mdc}(r_1 - r_2q_3, r_2) = \text{mdc}(r_3, r_2) = \text{mdc}(r_2, r_3)$$

$\vdots$

$$\text{mdc}(r_{(n-1)}) = \text{mdc}(r_{(n-1)} - r_nq_{(n+1)}, r_n) = \text{mdc}(r_{(n+1)}, r_n) = \text{mdc}(0, r_n) = r_n.$$

Assim, segue o resultado. Na prática, assim sintetiza-se:

Efetuando-se a divisão $b = aq_1 + r_1$ e colocando os números envolvidos no diagrama abaixo:

	q_1	
b	a	
r_1		

Transportando o r_1 e efetuando a divisão: $a = r_1q_2 + r_2$, conforme diagrama abaixo:

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Novamente, transportando r_2 e prosseguindo, enquanto for possível (até que para algum $n \geq 2, r_n | r_{(n-1)}$, ou seja, $r_{(n+1)} = 0$), tem-se:

	q_1	q_2	q_3	$\dots$	$q_{(n-1)}$	q_n	$q_{(n+1)}$
b	a	r_1	r_2	$\dots$	$r_{(n-2)}$	$r_{(n-1)}$	$r_n = mdc(a, b)$
r_1	r_2	r_3	r_4	$\dots$	r_n	0	

Portanto, $r_n = mdc(a, b)$.

Segundo exemplo de (HEFEZ, 2014), procede-se o cálculo do mdc de 372 e 162, utilizando o Algoritmo de Euclides:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Observa-se que o Algoritmo de Euclides nos fornece a seguinte informação:

$$6 = 18 - 1.12$$

$$12 = 48 - 2.18$$

$$18 = 162 - 3.48$$

$$48 = 372 - 2.162$$

Dessa forma, segue que:

$$6 = 18 - 1.12 = 18 - 1.(48 - 2.18) = 3.18 - 48 = 3.(162 - 3.48) - 48 =$$

$$3.162 - 10.48 = 3.162 - 10.(372 - 2.162) = 23.162 - 10.372.$$

Tem-se, então, que:

$$(372, 162) = 6 = 23 \cdot 162 + (-10) \cdot 372.$$

Consegue-se então, através do uso do Algoritmo de Euclides de trás para frente, escrever $6 = (372, 162)$ como múltiplo de 162 mais um múltiplo de 372.

Em geral, seguindo o procedimento detalhado no exemplo acima, vê-se que o Algoritmo de Euclides também fornece um meio de escrever o *mdc* de dois números como soma de múltiplos dos números em questão. E sempre que o Algoritmo de Euclides for utilizado para expressar (a, b) na forma $ma + nb$, com $m, n \in \mathbb{Z}$, o denominaremos de Algoritmo de Euclides Estendido.

2 EQUAÇÕES DIOFANTINAS LINEARES

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

$$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n = c,$$

sendo $a_0, a_1, \dots, a_n \in \mathbb{Z}$, das quais se procuram somente as soluções inteiras. Isso significa que se quer escrever c como combinação linear inteira de todos os a_t com $0 \leq t \leq n$. Sendo assim, determinar uma solução desse tipo de equação significa encontrar o conjunto de valores inteiros $a_0, a_1, \dots, a_n$ que, ao serem substituídos nos respectivos lugares de $x_0, x_1, \dots, x_n$ verifiquem a equação descrita acima (FERREIRA, DOMINGUES, 2013).

2.1 Equações diofantinas lineares com duas variáveis

Inicia-se estudando as Equações Diofantinas Lineares com duas variáveis, da forma:

$$ax + by = c, \tag{2.1}$$

em que $a, b \in \mathbb{Z}$ e suponha a e b não simultaneamente nulos. Uma solução para a equação acima é um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ para o qual a igualdade

$$ax_0 + by_0 = c$$

é verdadeira.

A seguir, mostram-se as condições em que (2.1) admite soluções.

Proposição 7. Uma equação diofantina $ax + by = c$, em que $a, b, c \in \mathbb{Z}$, com a e b não nulos, admite solução se, e somente se, $d|c$, em que $d = \text{mdc}(a, b)$.

Demonstração. Se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é solução da equação (2.1), então vale a igualdade

$$ax_0 + by_0 = c.$$

Se $d = \text{mdc}(a, b)$ então $d|a$ e $d|b$, logo $d|(ax_0 + by_0)$ ou seja, $d|c$. Reciprocamente, se $d|c$ então $c = sd$ para algum $s \in \mathbb{Z}$. Como $d = \text{mdc}(a, b)$ então segue do Teorema 2 que existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Mas por hipótese, que $d|c$ ou seja, $c = sd$, para algum $s \in \mathbb{Z}$. Assim, $c = ds = (ax_0 + by_0)s = ax_0s + by_0s$ o que mostra que (x_0s, y_0s) é uma solução da equação dada.

Se (x_0, y_0) é uma solução particular da equação $ax + by = c$ e (x', y') uma solução qualquer desta equação, então tem-se que:

$$ax' + by' = c = ax_0 + by_0 \quad (2.2)$$

pode-se concluir que,

$$a(x' - x_0) = b(y' - y_0). \quad (2.3)$$

Suponha que $d = \text{mdc}(a, b)$, então existem inteiros t e u tais que $a = dt$ e $b = du$, com $\text{mdc}(t, u) = 1$. Assim, substituindo em (2.3) tem-se:

$$t(x' - x_0) = u(y' - y_0). \quad (2.4)$$

Da equação (2.4), tem-se que $t|u(y' - y_0)$. Como $\text{mdc}(t, u) = s$ segue que $(y' - y_0) = ts$, para algum $s \in \mathbb{Z}$, em que:

$$y' = y_0 + ts. \quad (2.5)$$

Portanto, obtém-se $y' = y_0 + \left(\frac{a}{d}\right)s$.

Substituindo o valor de y' dado pela equação (2.5) na equação (2.4), segue que:

$$t(x' - x_0) = u(y' - y_0) = sut$$

ou seja,

$$x' = x_0 + us = x_0 + \left(\frac{b}{d}\right)s.$$

Então, estes cálculos, nos permite enunciar a próxima proposição.

Proposição 8. (veja [\[1\]](#)) Seja (x_0, y_0) uma solução particular da equação diofantina $ax + by = c$ em que $a \neq 0$ e $b \neq 0$. Então qualquer solução dessa equação é dada pelo par de inteiros:

$$S = \left\{ \left(x_0 + \left(\frac{b}{d}\right)u, y_0 - \left(\frac{a}{d}\right)u \right) \mid u \in \mathbb{Z} \right\}$$

em que $d = \text{mdc}(a, b)$.

Corolário 1. Se $d = \text{mdc}(a, b) = 1$ e $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é uma solução particular da equação diofantina linear $ax + by = c$ então todas as soluções dessa equação são dadas por

$$S = \{(x_0 + bu, y_0 - au) | u \in \mathbb{Z}\}.$$

Exemplo 8. Dada a equação

$$54x + 21y = 906,$$

encontre sua solução geral.

Solução. Encontrando o $mdc(54,21)$, usando o algoritmo de Euclides para o cálculo de mdc , tem-se a Tabela 1:

	2	1	1	3
54	21	12	9	3
12	9	3	0	

Tabela 1: $mdc(54,21)$

A Tabela 1 acima foi construída da seguinte maneira, o que servirá para as demais construções com as devidas adequações:

- Constrói-se uma tabela (diagrama) com três linhas e cinco colunas. Na primeira linha serão dispostos os quocientes, na segunda linha dividendos e divisores e na terceira, os restos;
- Inicialmente divide-se 54 por 21 e obtém-se 2 de quociente e 12 de resto;
- Daí transporta-se o resto 12 para a linha do meio e efetua-se a divisão de 21 por 12, obtendo 1 de quociente e 9 de resto;
- Transporta-se 9 para a linha do meio e efetua-se a divisão de 12 por 9, obtendo 1 de quociente e 3 de resto;
- Transporta-se o 3 para a linha do meio e efetua-se a divisão de 9 por 3, obtendo 3 de quociente e 0 de resto, finalizando a divisão.

Portanto, o $mdc(54,21)$ é 3. Como $3|906$, a equação tem solução. Dividindo-se tudo por 3, obtém-se uma equação simplificada: $18x + 7y = 302$, com $mdc(18,7) = 1$. Se (x_0, y_0) for solução da equação $18x + 7y = 1$, então o par $(302x_0, 302y_0)$ é solução de $18x + 7y = 302$.

Usando o algoritmo de Euclides para o cálculo de mdc , tem-se a Tabela 2 a seguir:

	2	1	1	3
18	7	4	3	1
4	3	1	0	

Tabela 2: $\text{mdc}(18,7)$.

Logo,

$$4 = 18 - 7 \cdot 2,$$

$$3 = 7 - 4 \cdot 1$$

$$1 = 4 - 3 \cdot 1$$

Dessa forma,

$$1 = 4 - 3 \cdot 1 = 4 - (7 - 4 \cdot 1) = 4 \cdot 2 - 7 = (18 - 7 \cdot 2) \cdot 2 - 7 = 18 \cdot 2 + 7 \cdot (-5).$$

Portanto, $(x_0, y_0) = (2, -5)$. Assim, $(302x_0, 302y_0) = (604, -1510)$ é uma solução particular da equação. Consequentemente, sua solução geral é expressa da seguinte forma:

$$x = 604 + 7u, y = -1510 - 18u, \text{ com } u \in \mathbb{Z}.$$

Exemplo 9. Dada a equação $5x - 2y = 2$, encontre sua solução geral.

Solução. Primeiro encontra-se o $\text{mdc}(5,2)$. Tem-se então que $\text{mdc}(5,2) = 1$. Note que se (x_0, y_0) é solução de $5x - 2y = 1$, então o par $(2x_0, 2y_0)$ é solução de $5x - 2y = 2$.

Usando o algoritmo de Euclides para o cálculo do mdc , obtém-se a Tabela 3 a seguir:

	2	2
5	2	1
1	0	

Tabela 3: $\text{mdc}(5,2)$.

Assim, tem-se que:

$$1 = 5 \cdot 1 - 2 \cdot 2.$$

Portanto, $(x_0, y_0) = (1, 2)$. Assim, $(2x_0, 2y_0) = (2, 4)$ é uma solução particular da equação. Consequentemente, sua solução geral é:

$$\{x = 2 - 2t, y = 4 - 5t\}, \text{ com } t \in \mathbb{Z}.$$

2.2 Equações diofantinas lineares com três variáveis

Considerando a equação $a_1x + a_2y + a_3z = b$, em que os a_n ($n = 1, 2, 3$) não são nulos. A mesma argumentação utilizada na prova da proposição 7 pode ser aplicada neste caso, então a equação tem solução se, e somente se, $d = \text{mdc}(a_1, a_2, a_3)$ divide b .

É possível calcular o mdc de uma quantidade finita de números, então, primeiro analisa-se $\text{mdc}(a_1, a_2) = d_1$ e, a partir deste, $\text{mdc}(d_1, a_3) = d$ (ALVES, 2017).

Seja $d_1 = \text{mdc}(a_1, a_2)$ então existem $k_1, k_2 \in \mathbb{Z}$, para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d = \text{mdc}(d_1, a_3)$, então existem $k, z_0 \in \mathbb{Z}$ de maneira que $d = d_1k + a_3z_0$.

Logo,

$$d = (a_1k_1 + a_2k_2)k + a_3z_0 = a_1(k_1k) + a_2(k_2k) + a_3z_0 \quad (2.6)$$

Fazendo $k_1k = x_0$ e $k_2k = y_0$, substituindo em (2.6) obtém-se:

$$a_1x_0 + a_2y_0 + a_3z_0 = d. \quad (2.7)$$

Portanto, se $a_1x + a_2y = b$, admite solução e como $b = dq$, para algum $q \in \mathbb{Z}$, multiplicando (2.7) por q , tem-se:

$$a_1(x_0q) + a_2(y_0q) + a_3(z_0q) = dq = b,$$

o que mostra que (x_0q, y_0q, z_0q) é uma solução particular da equação dada.

Exemplo 10. Encontre uma das soluções particulares da equação $120x + 84y + 144z = 60$.

Solução. Verifica-se a existência de solução, a partir do cálculo do $\text{mdc}(120, 84, 144)$. Como $\text{mdc}(120, 84, 144) = 12$ e $12|60$, então a equação possui solução.

Dividindo toda a equação por 12, tem-se sua forma equivalente $10x + 7y + 12z = 5$ cujo $\text{mdc}(10, 7, 12) = 1$ e $1|5$. Assim, calcularemos o $\text{mdc}(10, 7)$ usando o algoritmo de Euclides tem-se a Tabela 4 a seguir:

	1	2	3
10	7	3	1
3	1	0	

Tabela 4: $\text{mdc}(10, 7)$.

$$10 = 7 \cdot 1 + 3 \Rightarrow 3 = 10 + 7 \cdot (-1)$$

$$7 = 3 \cdot 2 + 1 \Rightarrow 1 = 7 + 3 \cdot (-2)$$

$$3 = 1 \cdot 3 + 0.$$

Dessa forma,

$$1 = 7 + 3 \cdot (-2) = 7 + (10 - 7) \cdot (-2) = 7 \cdot 3 + 10 \cdot (-2). \quad (2.8)$$

Agora prossegue-se ao cálculo do $\text{mdc}(12, 1)$ usando o algoritmo de Euclides conforme Tabela 5:

	12	1
12	1	1
1	0	

Tabela 5: $\text{mdc}(12, 1)$.

$$12 = 1 \cdot 11 + 1 \Rightarrow 1 = 1 \cdot (-11) + 12.$$

Como $1 = 10 \cdot (-2) + 7 \cdot 3$, segue que

$$1 = (10 \cdot (-2) + 7 \cdot 3) \cdot (-11) + 12$$

$$1 = 10 \cdot 22 + 7 \cdot (-33) + 12.$$

Portanto, tem-se a solução particular da equação diofantina:

$$5 = 10 \cdot (110) + 7 \cdot (-165) + 12 \cdot 5.$$

Logo, a terna $(110, -165, 5)$ é a solução procurada.

Exemplo 11. Encontre todas as soluções inteiras da equação $120x + 84y + 144z = 60$.

Solução. Verificado a existência de solução da equação no exemplo anterior, passemos a encontrar a solução geral.

Tomando $k = 10x + 7y$, então teremos $k + 12z = 5$, que também possui solução, pois $\text{mdc}(12, 1) = 1$ e $1|5$. Podemos escrever $\text{mdc}(1, 12) = 1$ como combinação linear de 1 e 12:

$$1 = 1 \cdot (-11 + 12).$$

Multiplicando ambos os lados por 5 teremos:

$$5 = 1.(-55) + 12.5.$$

Assim, $(-55, 5)$ é uma solução particular de $k + 12z = 5$ e segue da proposição 8 que a solução geral é dada por:

$$S_1 = \{(-55 + 12u_1, 5 - u_1), \text{ com } u_1 \in \mathbb{Z}\}.$$

Verifica-se agora, que $10x + 7y = k = -55 + 12u_1$. É importante observar que $\text{mdc}(10, 7) = 1$ e $1|(-55 + 12u_1)$, isto é, u pode assumir qualquer valor inteiro pois:

$$1| - 55 \text{ e}$$

$$1|12.$$

No exemplo 9, obteve-se (2.8): $1 = 10.(-2) + 7.3$, então multiplicando ambos os lados por $(-55 + 12u_1)$, tem-se:

$$(-55 + 12u_1).1 = 10.(-2).(-55 + 12u_1) + 7.7.(-55 + 12u_1), \text{ ou seja,}$$

$$(-55 + 12u_1) = 10.(110 - 24u_1) + 7.(-165 + 36u_1).$$

Portanto, tem-se que a solução geral procurada é:

$$S_2 = \{(110 - 24u_1 + 7u_2, -165 + 36u_1 - 10u_2) \text{ com } u_1 \text{ e } u_2 \in \mathbb{Z}\}.$$

Que resulta na solução geral da equação $10x + 7y + 12z = 5$ é da forma:

$$S_2 = \{(110 - 24u_1 + 7u_2, -165 + 36u_1 - 10u_2, 5 - u_1) \text{ com } u_1 \text{ e } u_2 \in \mathbb{Z}\}.$$

2.3 Equações diofantinas lineares com n variáveis

Considera-se agora a equação $a_1x_1 + a_2x_2 + a_3x_3 + \dots + a_{n-1}x_{n-1} + a_nx_n = b$, em que cada a_t , com $t = 1, 2, 3, \dots, n$, sejam inteiros não nulos simultaneamente.

Segundo Campos (2013) a mesma argumentação usada para provar a Proposição 7 garante que essa equação admite soluções, se $d = \text{mdc}(a_1, a_2, a_3, \dots, a_n)$ divide b .

Se $d_1 = \text{mdc}(a_1, a_2)$, então existem k_1 e $k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. Agora como $d_2 = \text{mdc}(d_1, a_3)$, então existem k_3 e $k_4 \in \mathbb{Z}$ de maneira que $d_2 = d_1k_3 + a_3k_4$.

Procedendo de forma análoga, $n - 1$ vezes, chegaremos em $d = \text{mdc}(d_{n-1}, a_n)$, então

$$a_1(x_1q) + a_2(x_2q) + a_3(x_3q) + \cdots + a_{n-1}(x_{(n-1)}q) + a_n(x_nq) = dq = b$$

para algum $q \in \mathbb{Z}$, o que mostra que

$$(x_1q, x_2q, x_3q, \dots, x_{(n-1)}q, x_nq)$$

é uma de suas soluções particulares.

Para encontrar a solução geral de uma equação diofantina linear de n variáveis, $a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + a_nx_n = b$, em que cada a_t , com $t = 1, 2, 3, \dots, n$, sejam inteiros não nulos simultaneamente, devemos utilizar o processo de reduzi-la a uma equação diofantina linear de duas variáveis. Para isso, faz-se uma substituição de $n - 1$ variáveis, por uma outra variável qualquer, diferente das já existentes. Feito isso, basta encontrar a solução geral desta nova equação gerada (CAMPOS, 2013).

Aplicando esse processo repetidas vezes, encontram-se todos os valores de x_t , com $t = 1, 2, 3, \dots, n$, assim como desenvolvido para encontrar a solução geral das equações diofantinas lineares de três variáveis.

Então, a solução geral de uma equação diofantina linear de n variáveis, se apresenta da seguinte forma:

$$S = \left\{ \left(x_1 + \frac{a_2}{d_{n-1}}s_{n-1}, x_2 - \frac{a_1}{d_{n-1}}s_{n-1}, x_3 - s_{n-2}, \dots, x_n - s_1 \right) \mid s_t \in \mathbb{Z}, \text{ com } t = 1, 2, 3, \dots, n - 1 \right\}$$

Exemplo 12. Encontre a solução geral de $32x - 60y - 24z + 42w + 14u = 12$.

Solução. Como o $\text{mdc}(32, 60, 24, 42, 14) = 2$ e $2 \mid 12$, então a equação possui solução.

Dividindo a equação dada por 2 obtém-se a equação equivalente, $16x - 30y - 12z + 21w + 7u = 6$.

Seja $p = 16x - 30y - 12z + 21w$, daí, $p + 7u = 6$ (1), também possui solução, pois $\text{mdc}(1, 7) = 1$ e $1 \mid 6$.

Então,

$$1 = 1.(6) + 7.1$$

$$6 = 1.(-36) + 7.6.$$

Logo, $(-36, 6)$ é uma solução particular de (1), que nos leva a solução geral

$$S_1 = \{(-36 + 7t_1, 6 - t_1) | t_1 \in \mathbb{Z}\}.$$

Para continuarmos nossa busca pela solução geral, tem-se

$$16x - 30y - 12z + 21w = p = -36 + 7t_1$$

que possui solução, qualquer que seja o valor para t_1 , pois $\text{mdc}(16, 30, 12, 21) = 1$.

Considerando $p' = 16x - 30y - 12z$ obtém-se $p' + 21w = -36 + 7t_1$ (2) e como o $\text{mdc}(1, 21) = 1$, qualquer que seja o valor de t_1 tem-se o $\text{mdc}(1, 21)$ dividindo $-36 + 7t_1$.

Então, pode-se fazer

$$1 = 1 \cdot (-20) + 21 \cdot 1$$

$$-36 + 7t_1 = 1 \cdot (-20) \cdot (-36 + 7t_1) + 21 \cdot 1 \cdot (-36 + 7t_1)$$

$$-36 + 7t_1 = 1 \cdot (720 - 140t_1) + 21 \cdot (-36 + 7t_1)$$

que possui $(720 - 140t_1, -36 + 7t_1)$ como uma solução particular e

$$S_2 = \{(720 - 140t_1 + 21t_2, -36 + 7t_1 - t_2) | t_1 \text{ e } t_2 \in \mathbb{Z}\}$$

como solução geral de (2).

Seja agora,

$$16x - 30y - 12z = p' = 720 - 140t_1 + 21t_2$$

que possui solução atribuindo um valor para t_2 , de forma que $720 - 140t_1 + 21t_2$ seja divisível por $2 = \text{mdc}(16, 30, 12)$.

Tomando $p'' = 16x - 30y$, obtém-se $p'' - 12z = 720 - 140t_1 + 21t_2$ (3). Assim como anteriormente, qualquer que seja o valor de t_2 tem-se o $\text{mdc}(1, 12)$ dividindo $720 - 140t_1 + 21t_2$, obtém-se

$$1 = 1 \cdot 13 - 12 \cdot 1$$

$$720 - 140t_1 + 21t_2 = 1 \cdot 13 \cdot (720 - 140t_1 + 21t_2) - 12 \cdot 1 \cdot (720 - 140t_1 + 21t_2)$$

$$720 - 140t_1 + 21t_2 = 1 \cdot (9360 - 1820t_1 + 273t_2) - 12 \cdot (720 - 140t_1 + 21t_2)$$

que possui como uma solução particular

$$(9360 - 1820t_1 + 273t_2, 720 - 140t_1 + 21t_2) \text{ e}$$

$$S_3 = \{(9360 - 1820t_1 + 273t_2 - 12t_3, 720 - 140t_1 + 21t_2 - t_3) \mid t_1, t_2 \text{ e } t_3 \in \mathbb{Z}\}$$

como solução geral de (3).

Finalmente, seja

$$16x - 30y = p'' = 9360 - 1820t_1 + 273t_2 - 12t_3 \quad (4)$$

e como $\text{mdc}(16, 30) = 2$ deve-se escolher um valor conveniente para t_3 que faça com que 2 divida $9360 - 1820t_1 + 273t_2 - 12t_3$.

Utilizando o algoritmo de Euclides para o mdc , tem-se

	1	1	7
30	16	14	2
14	2	0	

Tabela 6: $\text{mdc}(16, 30)$.

Então,

$$14 = 30 - 16.1$$

$$2 = 16 - 14.1.$$

Assim,

$$2 = 16 - 14.1 = 2 = 16 - (30 - 16.1) = 16.2 - 30.1.$$

Com isso, tem-se

$$2 = 16.2 - 30.1$$

$$2 \cdot \left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} \right) = 16.2 \cdot \left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} \right) - 30.1 \cdot \left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} \right)$$

$$9360 - 1820t_1 + 273t_2 - 12t_3 = 16 \cdot (9360 - 1820t_1 + 273t_2 - 12t_3) - 30 \cdot \left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} \right)$$

que possui como solução particular

$$\left(9360 - 1820t_1 + 273t_2 - 12t_3, \frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$$

e

$$S_4 = \left\{ \left(9360 - 1820t_1 + 273t_2 - 12t_3 - \frac{30}{2}t_4, \frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} \right) \mid t_1, t_2, t_3 \text{ e } t_4 \in \mathbb{Z} \right\}$$

como solução geral de (4).

Assim, pode-se concluir que

$$S = \left\{ \left(9360 - 1820t_1 + 273t_2 - 12t_3 - 15t_4, \frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} - 8t_4, \right. \right. \\ \left. \left. 720 - 140t_1 + 21t_2 - t_3, -36 + 7t_1 - t_2, 6 - t_1 \right) \mid t_1, t_2, t_3 \text{ e } t_4 \in \mathbb{Z} \right\}$$

é a solução geral da equação $32x - 60y - 24z + 42w = 14u = 12$.

Agora, a partir da solução geral obtida, é possível encontrar uma solução particular qualquer para a equação.

Tomando $t_1 = 7, t_2 = 4, t_3 = 2$ e $t_4 = 11$, obtém-se

$$u = -1$$

$$w = -36 + 7 \cdot 7 - 4 = 9$$

$$z = 720 - 140 \cdot 7 + 21 \cdot 4 - 2 = -178$$

$$y = \frac{9360 - 1820 \cdot 7 + 273 \cdot 4 - 12 \cdot 2}{2} - 8 \cdot 11 = -1244$$

$$x = 9360 - 1820 \cdot 7 + 273 \cdot 4 - 12 \cdot 2 - 15 \cdot 11 = -2477$$

ou seja,

$$S = \{(-2477, -1244, -178, 9, -1)\}$$

que é uma solução particular da equação dada.

Logo,

$$32 \cdot (-2477) - 60 \cdot (-1244) - 24 \cdot (-178) + 42 \cdot 9 + 14 \cdot (-1) = 12.$$

3 RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS ATRAVÉS DO PROCESSO DAS SUCESSIVAS EXTRAÇÕES DE INTEIROS

Segundo MENEZES (1971) cálculo indeterminado vem a ser a procura do número ilimitado ou indeterminado de valores de cada incógnita de uma equação isolada de mais de uma incógnita, ou de um sistema de equações onde o número de equações é inferior ao número de incógnitas.

Análise indeterminada do 1º grau vem a ser a procura somente das soluções inteiras de uma equação do 1º grau com mais de uma incógnita, ou de um sistema do 1º grau de m equações com $m + n$ incógnitas, quando todas as equações têm coeficientes inteiros. Essa preocupação de achar somente as soluções inteiras decorre da existência de problemas dos quais resulta o cálculo indeterminado do 1º grau, e que só admitem soluções inteiras. (MENEZES, 1971)

3.1 Soluções inteiras de $ax + by = c$

3.1.1 Condição de existência de soluções inteiras

A equação $ax + by = c$ admite uma infinidade de soluções inteiras quando os coeficientes das incógnitas a e b , em valores absolutos, são números primos entre si.

Exemplo 13. $5x - 3y = 12$, admite uma infinidade de soluções inteiras, por que os coeficientes das incógnitas, em valor absoluto, 5 e 3, são primos entre si.

São exemplos de soluções inteiras:

$$\begin{cases} x = -3 \\ y = -9 \end{cases}, \begin{cases} x = 0 \\ y = -4 \end{cases}, \begin{cases} x = 3 \\ y = 1 \end{cases}, \begin{cases} x = 6 \\ y = 6 \end{cases}, \text{etc.}$$

Exemplo 14. $4x + 6y = 11$, não admite nenhuma solução inteira, porque 4 e 6 não são primos entre si.

Teorema 3. A equação $ax + by = c$, de coeficientes a, b e c primos entre si, não admite nenhuma solução inteira quando a e b não são primos entre si.

Demonstração. É sempre possível, em nome do segundo princípio da equivalência suprimir qualquer fator comum aos elementos a, b e c , tornando-os, assim, primos entre si.

Supõe-se, agora, que a e b ainda têm um divisor comum d , de sorte que $a = dq_1$ e $b = dq_2$, e a equação dada passa a ter o aspecto:

$$dq_1x + dq_2y = c.$$

Atribuindo-se a x e y valores inteiros, o primeiro membro dessa igualdade, por ser a soma de dois múltiplos de d , vem a ser um múltiplo de d , enquanto o segundo membro c não é múltiplo de d , visto ter sido previamente considerado que a, b e c são primos entre si. Conclui-se, portanto, que a equação dada não pode ter nenhuma solução inteira.

Teorema 4. A equação $ax + by = c$, de coeficientes a, b e c primos entre si, admite uma infinidade de soluções inteiras quando a e b também são primos entre si.

Demonstração.

1ª parte: A equação admite uma solução inteira.

Resolvendo-se a equação $ax + by = c$ em relação a x , por exemplo, tem-se:

$$x = \frac{c - by}{a} \quad (3.1)$$

Deseja-se provar que, atribuindo-se em (3.1) à incógnita y , sucessivamente, os valores inteiros consecutivos $0, 1, 2, 3, \dots, (a - 1)$, haverá apenas um desses valores dados a y que propiciará a divisão exata de $c - by$ por a (de resto nulo), formando com esse quociente completo encontrado uma solução inteira da equação proposta. Atribuindo-se a y cada um dos referidos valores, obtém-se para $c - by$:

$$c, c - b, c - 2b, c - 3b, \dots, c - (a - 1)b.$$

Dividindo-se esses diferentes dividendos por a , de modo a manter sempre positivos os restos achados para essas divisões, todos esses restos devem ser diferentes entre si e inferiores ao divisor a , um será forçosamente zero, revelando que, ao valor inteiro dado a y nesse caso, corresponde um valor inteiro para x , e os dois valores inteiros de x e y constituem a solução inteira de $ax + by = c$.

Se assim não fosse, então entre os restos achados, dois deles seriam iguais a r , correspondendo aos valores m_1 e m_2 atribuídos a y ; logo:

$$c - bm_1 = aq_1 + r$$

$$c - bm_2 = aq_2 + r.$$

Subtraindo-se da primeira a segunda dessas duas igualdades, membro a membro e termo a termo, tem-se:

$$b(m_2 - m_1) = a(q_1 - q_2), \text{ ou } \frac{b(m_2 - m_1)}{a} = q_1 - q_2$$

O segundo membro dessa última igualdade é um número inteiro (soma dos números inteiros q_1 e q_2); então, o primeiro membro também deve ser inteiro, isto é, $m_2 - m_1$ deve ser divisível por a , uma vez que b não é divisível por a por ser primo com a . Ora, $m_2 - m_1$ não pode ser divisível por a por que, se m_1 e m_2 são inferiores a a (pertencentes que são a sequência $0, 1, 2, 3, \dots, a - 1$), a diferença $m_2 - m_1$ também é inferior a a , com mais forte razão.

Conclui-se, pois, que todos os restos são diferentes entre si, e um deles tem de ser nulo.

2ª parte: A equação admite uma infinidade de soluções.

Sabe-se que $ax + by = c$ já possui uma solução inteira $\begin{cases} x = x_0 \\ y = y_0 \end{cases}$, quando a e b são primos entre si.

Assim, deve-se ter a identidade $ax_0 + by_0 = c$. Substituindo-se c por $ax_0 + by_0$ na expressão (3.1) de x , obtém-se:

$$x = \frac{ax_0 + by_0 - by}{a}; \text{ ou } x = x_0 - b \cdot \left(\frac{y - y_0}{a} \right).$$

Note que, para x ser inteiro, deve-se ter $\frac{y - y_0}{a} = t$, sendo t um número inteiro. Então, dessas duas últimas expressões decorrem, para x e y , as fórmulas gerais:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}$$

Atribuindo-se a t a infinidade de valores inteiros do campo real, isto é, os números inteiros entre $-\infty$ e $+\infty$, ter-se-á a infinidade de soluções inteiras (pares de valores inteiros de x e y) que satisfazem à equação dada.

Observações.

1ª. A resolução de $ax + by = c$ em números inteiros consistirá, essencialmente, em achar-se uma solução inteira qualquer $x = x_0$ e $y = y_0$.

2ª. A infinidade de soluções inteiras decorre das fórmulas gerais $x = x_0 - bt$ e $y = y_0 + at$, de fácil memorização.

3.2 Cálculo das soluções inteiras

Para obterem-se as soluções inteiras da equação geral $ax + by = c$, em que a, b e c são números inteiros primos entre si, sendo a e b também primos entre si, há o processo denominado processo de sucessivas extrações de inteiros, o qual pode ser resumido às seguintes regras:

1ª. Tirar o valor da primeira incógnita (a de coeficiente menor, em valor absoluto), obtendo-se uma fração.

2ª. Extrair os inteiros contidos nessa fração e igualar a fração própria restante a uma incógnita auxiliar t_1 , constituindo-se, assim, uma equação auxiliar com duas incógnitas (x ou y e t_1).

3ª. Tirar o valor da segunda incógnita nessa equação auxiliar, obtendo-se outra fração.

4ª. Extrair os inteiros contidos nessa fração e igualar a fração própria restante a uma incógnita auxiliar t_2 , constituindo-se, assim, uma outra equação auxiliar com duas incógnitas (t_1 e t_2).

5ª. Tirar o valor da incógnita auxiliar t_1 nessa equação auxiliar, obtendo-se uma fração.

6ª. Prosseguir nessa marcha de extrair inteiros e de introduzir incógnitas auxiliares $t_3, t_4, \dots$, até que se chegue a uma última equação auxiliar em que, pelo menos, uma das incógnitas tenha o coeficiente igual a 1, e obtém-se imediatamente o valor dessa incógnita desde que se faça a outra incógnita igual a zero.

7ª. Retornar às incógnitas da equação dada, através das expressões de todas as incógnitas auxiliares, em sucessivas substituições de valores numéricos, a fim de obter-se uma primeira solução inteira $x = x_0$ e $y = y_0$.

8ª. Calcular a infinidade de soluções inteiras através das fórmulas gerais conhecidas:

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at \end{cases}$$

Para $t = 0, \pm 1, \pm 2, \pm 3, \pm 4, \dots$

9ª. Quando nas sucessivas extrações de inteiros aparecer um fator comum às parcelas do numerador, colocá-lo em evidência para simplificar as operações que se seguirem.

Exemplo 15. Encontrar as soluções inteiras da equação $61x + 47y = 313$.

Solução.

1ª. Resolução da equação dada em relação a uma das suas incógnitas: em relação a y (incógnita de menor coeficiente, em valor absoluto):

$$y = \frac{313 - 61x}{47}$$

2ª. Extração de inteiros e introdução da incógnita auxiliar t_1 :

$$\frac{313}{47} = 6 + \frac{31}{47} \text{ ou } 313 = 47 \cdot 6 + 31; \text{ e } \frac{61x}{47} = x + \frac{14x}{47}, \text{ ou } 61x = 47x + 14x$$

Então,

$$y = \frac{47 \cdot 6 + 31 - 47x - 14x}{47}, \text{ ou } y = 6 - x + \frac{31 - 14x}{47}; \text{ ou}$$

$$y = 6 - x + t_1 \tag{3.2}$$

e

$$t_1 = \frac{31 - 14x}{47}; \text{ ou } 14x + 47t_1 = 31 \text{ (equação auxiliar)} \tag{3.3}$$

3ª. Resolução da equação auxiliar (3.3):

Em relação a x (incógnita de menor coeficiente, em valor absoluto):

$$x = \frac{31 - 47t_1}{14}$$

4ª. Extração de inteiros e introdução da incógnita auxiliar t_2 :

$$\frac{31}{14} = 2 + \frac{3}{14}, \text{ ou } 31 = 14 \cdot 2 + 3; \text{ e } \frac{47t_1}{14} = 3t_1 + \frac{5t_1}{14}, \text{ ou } 47t_1 = 14 \cdot 3t_1 + 5t_1$$

Então,

$$x = \frac{14 \cdot 2 + 3 - 14 \cdot 3t_1 - 5t_1}{14}; \text{ ou } x = 2 - 3t_1 + \frac{3 - 5t_1}{14}; \text{ ou}$$

$$x = 2 - 3t_1 + t_2 \quad (3.4)$$

e

$$t_2 = \frac{3 - 5t_1}{14}; \text{ ou } 5t_1 + 14t_2 = 3 \text{ (equação auxiliar)} \quad (3.5)$$

5ª. Resolução da equação auxiliar (3.5):

Em relação a t_1 (incógnita de menor coeficiente, em valor absoluto):

$$t_1 = \frac{31 - 14t_2}{5}$$

6ª. Extração de inteiros e introdução da incógnita auxiliar t_3 :

$$\frac{3}{5} = 0 + \frac{3}{5}; \text{ ou } 3 = 0 + 3; \text{ e } \frac{14t_2}{5} = 2t_2 + \frac{4t_2}{5}, \text{ ou } 14t_2 = 5 \cdot 2t_2 + 4t_2; \text{ ou}$$

$$t_1 = -2t_2 + t_3 \quad (3.6)$$

e

$$t_3 = \frac{3 - 4t_2}{5}; \text{ ou } 4t_2 + 5t_3 = 3 \text{ (equação auxiliar)} \quad (3.7)$$

7ª. Resolução da equação auxiliar (3.7):

Em relação a t_2 (incógnita de menor coeficiente, em valor absoluto):

$$t_2 = \frac{3 - 5t_3}{4}$$

8ª. Extração de inteiros e introdução da incógnita auxiliar t_4 :

$$\frac{3}{4} = 0 + \frac{3}{4}, \text{ ou } 3 = 0 + 3; \text{ e } \frac{5t_3}{4} = t_3 + \frac{t_3}{4}, \text{ ou } 5t_3 = 4t_3 + t_3$$

Então,

$$t_2 = \frac{0+3-4t_3-t_3}{4}; \text{ ou } t_2 = -t_3 + \frac{3-t_3}{4}; \text{ ou}$$

$$t_2 = -t_3 + t_4 \quad (3.8)$$

e

$$t_4 = \frac{3-t_2}{4}; \text{ ou } t_3 + 4t_4 = 3 \quad (3.9)$$

A equação (3.9) é a última equação auxiliar por que uma das suas incógnitas, pelo menos, tem coeficiente igual a 1.

9ª. Cálculo da primeira solução inteira $x = x_0, y = y_0$:

$$\text{Fazendo-se } t_4 = 0 \text{ em (5), surge } t_3 + 0 = 3; \text{ ou } \begin{cases} t_3 = 3 \\ t_4 = 0 \end{cases} \quad (3.10)$$

$$\text{Levando-se (9) em (7), surge } t_2 = -3 + 0, \text{ ou } t_2 = -3 \quad (3.11)$$

$$\text{Levando-se (10) e (9) em (5), surge } t_1 = 6 + 3, \text{ ou } t_1 = 9 \quad (3.12)$$

$$\text{Levando-se (11) e (10) em (3), surge } x = 2 - 27 - 3, \text{ ou } x = -28 \quad (3.13)$$

$$\text{Levando-se (12) e (11) em (1), surge } y = 6 + 28 + 9, \text{ ou } y = 43$$

$$\begin{cases} x_0 = -28 \\ y_0 = 43 \end{cases}$$

10ª. Cálculo da infinidade de soluções inteiras (fórmulas gerais de x, y)

$$\begin{cases} x = -28 - 47t \\ y = 43 + 61t \end{cases}$$

para $t = 0, \pm 1, \pm 2, \pm 3, \pm 4, \dots$

3.3 Soluções inteiras de m equações com $m + 2$ incógnitas

3.3.1 Condição de existência de soluções inteiras

O sistema de m equações com $m + 2$ incógnitas (1 equação com 3 incógnitas) admite uma infinidade de soluções inteiras quando são primos entre si os coeficientes das incógnitas de cada equação.

Exemplo 16. $4x - 2y + 5z = 17$ admite uma infinidade de soluções inteiras porque 4, -2, 5, em valores absolutos, são primos entre si.

De fato assim é por que se, em $ax + by + cz = d$, por exemplo, os coeficientes das incógnitas admitissem um divisor comum diferente da unidade, para quaisquer valores inteiros dados às incógnitas, o primeiro membro da equação seria um múltiplo triplo do referido divisor, enquanto o segundo membro não admite o mencionado divisor (a, b, c e d são sempre supostos primos entre si).

3.3.2 Cálculo das soluções inteiras de 1 equação com 3 incógnitas

Exemplo 17. Achar as soluções inteiras da equação $18x - 7y + 13z = 39$.

1ª. Existência de soluções inteiras da equação

A equação dada admite uma infinidade de soluções inteiras por que os coeficientes das incógnitas, 18, -7, 13, em valores absolutos, são primos entre si.

2ª. Resolução da equação dada $18x - 7y + 13z = 39$ (3.14)

a) Em relação a y (incógnita de menor coeficientes, em valor absoluto):

$$\begin{aligned} y &= \frac{18x + 13z - 39}{7} = 2x + z - 5 + \frac{4x + 6z - 4}{7} \\ &= 2x + z - 5 + 2 \cdot \frac{2x + 3z - 2}{7}; \text{ ou} \\ y &= 2x + z - 5 + 2t_1 \end{aligned} \quad (3.15)$$

e

$$t_1 = \frac{2x + 3z - 2}{7}, \text{ ou } 2x + 3z - 7t_1 = 0 \quad (3.16)$$

b) Resolução da equação auxiliar (3.16):

Em relação a x (incógnita de menor coeficiente em valor absoluto):

$$\begin{aligned} x &= \frac{2 - 3z + 7t_1}{2} = 1 - z + 3t_1 + \frac{t_1 - z}{2}; \text{ ou} \\ x &= 1 - z + 3t_1 + t_2 \end{aligned} \quad (3.17)$$

e

$$t_2 = \frac{t_1 - z}{2}; \text{ ou } z - t_1 + 2t_2 = 0 \quad (3.18)$$

A equação (3.18) é a última equação auxiliar, por que uma das suas incógnitas, pelo menos, tem coeficiente igual a 1.

c) Resolução da última equação auxiliar (3.18):

$$z = t_1 - 2t_2 \quad (3.19)$$

d) Expressões de x, y, z em função de t_1 e t_2 :

Levando-se (3.19) em (3.17):

$$x = 1 - (t_1 - t_2) + 3t_1 + t_2; \text{ ou } x = 1 + 2t_1 + 3t_2 \quad (3.20)$$

Levando-se (3.20) e (3.19) em (3.15):

$$y = 2(1 + 2t_1 + 3t_2) + t_1 - 2t_2 - 5 + 2t_1; \text{ ou } y = -3 + 7t_1 + 4t_2 \quad (3.21)$$

e) Cálculo da infinidade de soluções inteiras do sistema:

$$\begin{cases} x = 1 + 2t_1 + 3t_2 \\ y = -3 + 7t_1 + 4t_2 \\ z = t_1 - 2t_2 \end{cases}$$

para quaisquer valores inteiros atribuídos arbitrariamente a t_1 e t_2 .

Exemplos de soluções inteiras:

$$\text{Para } t_1 = 0 \text{ e } t_2 = 0, \begin{cases} x = 0 \\ y = -3 \\ z = 0 \end{cases}; \text{ para } t_1 = 0 \text{ e } t_2 = 1, \begin{cases} x = 4 \\ y = 1 \\ z = -2 \end{cases}; \text{ etc.}$$

Observação. Se fossem reclamadas somente as soluções inteiras positivas da equação dada, cumpriria discutir os valores a serem dados a t_1 e t_2 para obtenção daquelas soluções, através da imposição de serem positivas as expressões de x, y, z em função de t_1 e t_2 . Isto é:

a) Condições para que x, y, z sejam positivos:

$$\begin{cases} 1 + 2t_1 + 3t_2 > 0 \\ -3 + 7t_1 + 4t_2 > 0 \\ t_1 - t_2 > 0 \end{cases} \text{ ou } \begin{cases} t_2 > \frac{-1 - 2t_1}{3} \\ t_2 > \frac{3 - 7t_1}{4} \\ t_2 < \frac{t_1}{2} \end{cases}$$

b) Discussão dos valores inteiros a serem atribuídos às incógnitas auxiliares t_1 e t_2 :

Para evitar qualquer contradição entre os limites de t_2 , deve-se ter o seguinte:

$$\frac{-1 - 2t_1}{3} < t_2 < \frac{t_1}{2} \quad \text{e} \quad \frac{3 - 7t_1}{4} < t_2 < \frac{t_1}{2}$$

ou, com mais forte razão:

$$\begin{cases} \frac{-1 - 2t_1}{3} < \frac{t_1}{2}; \text{ ou } -2 - 4t_1 < 3t_1; \text{ ou } 7t_1 > -2; \text{ ou } t_1 > -\frac{2}{7} \\ \frac{3 - 7t_1}{4} < \frac{t_1}{2}; \text{ ou } 6 - 14t_1 < 4t_1; \text{ ou } 18t_1 > 6; \text{ ou } t_1 > \frac{1}{3} \end{cases}$$

$\therefore \frac{1}{3}$ é o limite de t_1 , e $t_1 = 1, 2, 3, \dots$

$$\text{Para } t_1 = 1, \begin{cases} t_2 > \frac{-1-2}{3} = -1 \\ t_2 > \frac{3-7}{4} = -1 \\ t_2 < \frac{1}{2} \end{cases} \quad \text{ou} \quad \left\{ -1 < t_2 < \frac{1}{2} \quad \text{ou} \quad t_2 = 0, \text{ isto é:} \right.$$

$$\begin{cases} t_1 = 1 \\ t_2 = 0 \end{cases} \therefore \begin{cases} x = 1 + 2 + 0 = 3 \\ y = -3 + 7 + 0 = 4, \\ z = 1 - 0 = 1 \end{cases} \quad \text{1º exemplo de solução inteira positiva}$$

$$\text{Para } t_1 = 2, \begin{cases} t_2 > \frac{-1-4}{3} = -\frac{5}{3} = -1\frac{2}{3} \\ t_2 > \frac{3-14}{4} = -\frac{11}{4} = -2\frac{3}{4} \\ t_2 < 1 \end{cases} \quad \text{ou} \quad \left\{ -1\frac{2}{3} < t_2 < 1 \text{ ou } t_2 = -1 \text{ e } t_2 = 0, \text{ isto é:} \right.$$

$$\begin{cases} t_1 = 2 \\ t_2 = -1 \end{cases} \therefore \begin{cases} x = 1 + 4 - 3 = 2 \\ y = -3 + 14 - 4 = 7, \\ z = 2 + 4 = 6 \end{cases} \quad \text{2º exemplo de solução inteira positiva}$$

e

$$\begin{cases} t_1 = 2 \\ t_2 = 0 \end{cases} \therefore \begin{cases} x = 1 + 4 + 0 = 5 \\ y = -3 + 14 + 0 = 11, \\ z = 2 - 0 = 2 \end{cases} \quad \text{3º exemplo de solução inteira positiva}$$

E assim por diante.

Exemplo 17. (veja [\[2\]](#)) Determine as soluções inteiras da equação:

$$11x + 8y - 13z = 50.$$

Solução. Observe que, para que essa equação tenha soluções inteiras, qualquer divisor comum de 11, 8 e 3 deve ser também um divisor de 50.

Primeiramente, identifica-se o termo da equação com coeficiente de menor valor absoluto, nesse caso o termo $8y$. Isola-se o valor da variável escrevendo:

$$y = \frac{50 - 11x + 13z}{8}.$$

Divide-se os valores absolutos dos coeficientes 50, 11 e 13 por 8 e obtém-se os quocientes 6, 1 e 1 e restos 2, 3 e 5, respectivamente. Por isso, a fração que aparece na igualdade anterior pode ser escrita na forma:

$$y = 6 - x + z + \frac{2 - 3x + 5z}{8}.$$

Separa-se a equação anterior em duas, introduzindo uma variável auxiliar $t_1 \in \mathbb{Z}$.

$$y = 6 - x + z + t_1 \text{ e } \frac{2 - 3x + 5z}{8} = t_1$$

A equação com a variável auxiliar é equivalente a $2 - 3x + 5z = 8t_1$. Isola-se a variável que tem o menor coeficiente em módulo:

$$x = \frac{2 + 5z - 8t_1}{3}$$

Divide-se 5 e 8 por 3, obtendo quocientes 1 e 2 e restos 2 e 2, respectivamente. Logo, a última equação é equivalente a:

$$x = z - 2t_1 + \frac{2 + 2z - 2t_1}{3} = z - 2t_1 + 2 \left[\frac{1 + z - t_1}{3} \right]$$

Introduzindo a variável auxiliar $t_2 \in \mathbb{Z}$ e separando a equação anterior em duas:

$$x = z - 2t_1 + 2t_2 \text{ e } t_2 = \frac{1 + z - t_1}{3}, \text{ que equivale a } 1 + z - t_1 = 3t_2$$

Como a equação auxiliar anterior, $1 + z - t_1 = 3t_2$, tem uma variável (x, y ou z) com coeficiente de valor absoluto igual a 1, isola-se o valor dessa variável e faz as substituições nas equações anteriores para obter a solução do problema:

$$z = t_1 + 3t_2 - 1$$

$$x = z - 2t_1 + 2t_2 = (t_1 + 3t_2 - 1) - 2t_1 + 2t_2 = -t_1 + 5t_2 - 1$$

$$y = 6 + z - x + t_1 = 6 + (t_1 + 3t_2 - 1) - (-t_1 + 5t_2 - 1) + t_1 = 3t_1 - 2t_2 + 6$$

Obtém-se dessa forma a solução geral da equação dada:

$$x = -t_1 + 5t_2 - 1, y = 3t_1 - 2t_2 + 6, z = t_1 + 3t_2 - 1, \text{ com } t_1 \text{ e } t_2 \in \mathbb{Z}.$$

Determinados problemas exigem soluções positivas. Nesses casos, pode-se determinar a solução geral da equação segundo o exemplo anterior e depois exigir que cada variável tenha um valor positivo. No caso do exemplo anterior,

$$\begin{cases} -t_1 + 5t_2 - 1 > 0 \\ 3t_1 - 2t_2 + 6 > 0 \\ t_1 + 3t_2 - 1 > 0 \end{cases} \text{ que equivale a } \begin{cases} t_1 < 5t_2 - 1 \\ t_1 > \frac{2t_2 - 6}{3} \\ t_1 > -3t_2 + 1 \end{cases} \text{ que implica}$$

$$\begin{cases} \frac{2t_2 - 6}{3} < 5t_2 - 1 \\ -3t_2 + 1 < 5t_2 - 1 \end{cases} \text{ , cuja solução é } t_2 > -\frac{3}{13} \text{ e } t_2 > \frac{1}{4}, \text{ ou seja, } t_2 > \frac{1}{4}.$$

Logo, pode-se ter soluções positivas da equação para os valores inteiros de t_2 : 1, 2, 3, ... Substituindo $t_2 = 1$ em um dos sistemas de desigualdades anterior, obtém-se:

$$\begin{cases} t_1 < 4 \\ t_1 > -\frac{4}{3} \\ t_1 > -2 \end{cases}$$

Assim, tem-se para t_1 : -1, 0, 1, 2 ou 3. Escolhendo, por exemplo, $t_1 = 3$ e $t_2 = 1$, substituindo na solução geral da equação, obtém-se $x = 1, y = 13, z = 5$.

4 EXPLORANDO O ENSINO DE EQUAÇÕES DIOFANTINAS LINEARES NO ENSINO MÉDIO

Neste capítulo, será descrita uma sequência de atividades didáticas que irá explorar o ensino das equações diofantinas lineares e algumas questões acerca deste assunto que podem e devem ser desenvolvidos na educação básica. A sequência de atividades didáticas que será descrita ao longo deste capítulo é destinada a alunos do ensino médio, estando presentes em diversos problemas da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas) e diversos vestibulares de questões solucionáveis através de equações diofantinas lineares e a necessidade de apresentar estas questões aos alunos do ensino médio. Além disso, subentende-se que alunos desse nível de escolaridade já possuem uma boa base para compreenderem a exploração de situações-problema que recaem em equações diofantinas lineares.

Nesse sentido, vale observar que as equações diofantinas lineares são estudadas de forma implícita no ensino fundamental, ao estudar as equações lineares com duas variáveis, o qual é feito geralmente após o estudo de equações do 1º grau e antes de estudar os sistemas de equações lineares, quando uma determinada situação requer que restringimos as respectivas soluções ao conjunto dos números inteiros. Vale ressaltar que numerosas situações-problema do dia a dia requerem soluções inteiras e que podem ser modeladas via equações lineares com duas variáveis, ou seja, por equações diofantinas lineares (SILVA, 2013).

Dessa forma, nessa sequência de atividades didáticas serão descritas três atividades, para serem trabalhadas com os alunos em sala de aula, envolvendo situações-problema que incidem principalmente em equações diofantinas lineares e estão presentes em vestibulares ou provas da OBMEP. Tendo em vista que a motivação para a realização de uma determinada atividade, para a maioria dos alunos, está relacionada com uma avaliação, recomenda-se ao professor que a avaliação dos alunos seja feita principalmente por sua participação no desenvolvimento das atividades e para o cumprimento das referidas atividades, o professor poderá solicitar aos alunos que formem duplas, trios, ou até mesmo pequenos grupos de quatro alunos (fica a critério do professor). Com isso, pretende-se obter um maior envolvimento dos alunos na resolução dos problemas propostos nas atividades.

Por fim, para cada uma das três atividades propostas, será feita a apresentação da situação-problema, recomendações metodológicas ao professor sobre como proceder em sala

de aula e a devida resolução da questão através do método tradicional de resolução, utilizando o algoritmo de Euclides e o método apresentado no capítulo 3, utilizando o processo das sucessivas extrações de inteiros.

4.1 Descrição da primeira atividade

A primeira atividade da sequência remete a uma questão presente no vestibular da Universidade Federal do Ceará (UFC-CE), no ano de 2004, sendo que a resolução de tal questão recai sobre equações diofantinas lineares, e o aluno que tivesse estudado tal conteúdo no ensino médio teria plenas condições de resolvê-la.

Etapas 1: Apresentação da atividade

Nesse momento, o professor entrega uma cópia da atividade a cada dupla ou trio formado. Recomenda-se, antes que os alunos iniciem a resolução da atividade, que o professor faça uma leitura detalhada e compartilhada com os alunos da questão, objetivando esclarecer eventuais dúvidas com relação ao enunciado. Para então, pedir aos alunos para resolverem as questões de tal atividade com atenção, em que, ao final deste primeiro momento de aplicação da primeira atividade, serão recolhidas com as respectivas respostas.

Atividade 1

(UFC-CE/2004) Um poliedro convexo só tem faces triangulares e quadrangulares. Se ele tem 20 arestas e 10 vértices, então, o número de faces triangulares é:

- a) 12
- b) 11
- c) 10
- d) 9
- e) 8

Etapas 2: Recomendações metodológicas

Sugere-se ao professor, nesse primeiro momento, deixar os alunos à vontade na resolução da questão, ou seja, não fazendo nenhuma interferência. Recolhendo as atividades com as respectivas soluções ao final da aula. Dessa forma, de posse destas soluções, o professor poderá analisar quais as dificuldades apresentadas pelos alunos e em quais assuntos. Assim o docente vai dispor de um diagnóstico qualitativo para subsidiar suas intervenções

para a próxima aula. Logo, é viável que o professor responda todas as questões dos alunos, e assim, no segundo momento, faça uma discussão direcionada visando atender, sanar ou diminuir as dificuldades apresentadas. O professor deve solicitar que os alunos apresentem no quadro negro (ou na lousa) suas estratégias de resolução, favorecendo com isto, uma interação e participação dos alunos na resolução da atividade, onde o professor poderá fazer interferências nas resoluções apresentadas, com o intuito de contribuir por meio das correções quando necessário, ou seja, auxiliando na construção e na evolução dos conceitos estudados nesta atividade. Dessa forma, acredita-se tornar a aula mais interessante tanto para o professor quanto para os alunos, tornando-lhes agentes na construção do seu próprio conhecimento matemático, em que eles deixam de serem sujeitos passivos, para serem sujeitos ativos na sua aprendizagem em matemática. Sendo assim, recomenda-se ao professor atenção nas possíveis dificuldades previstas e possíveis contribuições para os alunos na resolução da atividade.

Etapa 3: Resolução da atividade

Solução através do método tradicional (algoritmo de Euclides). (veja [\[10\]](#))

Escrever uma equação diofantina linear $3x + 4y = 40$, em que x representa a face triangular e y representa a face quadrangular. O número 40 representa o dobro do número de arestas, que são 20, pois cada aresta é contada duas vezes.

Vamos inicialmente encontrar o $mdc(3,4)$ pelo algoritmo de Euclides:

	1	2	1
4	3	1	1
1	1	0	

Tabela 7: $mdc(3,4)$.

Como o $mdc(3,4) = 1$, a equação apresenta solução, pois o $mdc(3,4) = 1|12$. Agora pode-se escrever a equação como combinação linear de 3 e 4 da seguinte forma:

$$3.(-1) + 4.1 = 1$$

Multiplicando a equação por 40, tem-se:

$$3.(-40) + 4.(40) = 1.(40)$$

Logo, o par de inteiros $x_0 = -40$ e $y_0 = 40$ é uma solução particular da equação proposta, e $x > 0$ e $y > 0$, pois existem faces triangulares e quadrangulares.

$$x = x_0 + b \cdot t = -40 + 4 \cdot t$$

$$y = y_0 - a \cdot t = 40 - 3 \cdot t$$

$$-40 + 4 \cdot t > 0 \quad \text{e} \quad 40 - 3 \cdot t > 0$$

Resolvendo as inequações, tem-se:

$$10 < t < 13,33$$

$$t = \{11, 12, 13\}$$

Pela relação de Euler sabe-se que $V + F = A + 2$, encontra-se $F = 12$ *faces*. Sabe-se que $x + y = 12$, então $(-40 + 4 \cdot t) + (40 - 3 \cdot t) = 12$, logo $t = 12$. Sabe-se que x representa o número de faces triangulares.

Assim,

$$x = -40 + 4 \cdot t$$

$$x = -40 + 4 \cdot (12)$$

$$x = -40 + 48$$

$$x = 8 \text{ faces triangulares}$$

Observação. Se substituir todos os candidatos a t nas respectivas equações $x = -40 + 4 \cdot t$ e $y = 40 - 3 \cdot t$, encontram-se os pares ordenados (4,7), (8,4) e (12,1) que satisfazem a equação, mas não ao problema, uma vez que a soma das faces devem totalizar 12. Portanto, a única solução compatível com o problema é para $t = 12$, ou seja, o par ordenado (8,4), correspondendo a 8 faces triangulares e 4 faces quadrangulares. Resposta letra E.

Solução através do método de sucessivas extrações de inteiros.

Escrever uma equação diofantina linear $3x + 4y = 40$, em que x representa a face triangular e y representa a face quadrangular. O número 40 representa o dobro do número de arestas, que são 20, pois cada aresta é contada duas vezes.

Primeiramente, identifica-se o termo da equação com coeficiente de menor valor absoluto; nesse caso, o termo $3x$. Isola-se o valor da variável escrevendo:

$$x = \frac{40 - 4y}{3}$$

Divide-se os valores dos coeficientes 40 e 4 por 3 e obtém-se os quocientes 13 e 1 e restos 1 e 1, respectivamente. Por isso, a fração que aparece na igualdade anterior pode ser escrita dessa forma:

$$x = 13 - y + \frac{1 - y}{3}$$

Separa-se a equação anterior em duas, introduzindo uma variável auxiliar $t_1 \in \mathbb{Z}$.

$$x = 13 - y + t_1 \quad \text{e} \quad \frac{1 - y}{3} = t_1$$

A equação com a variável auxiliar é equivalente a $1 - y = 3t_1$.

Como a equação auxiliar anterior, $1 - y = 3t_1$, tem uma variável (x ou y) com coeficiente de valor absoluto igual a 1, isola-se o valor dessa variável e faz as substituições nas equações anteriores para obter a solução do problema.

$$y = -3t_1 + 1$$

$$x = 13 - y + t_1 = 13 - (-3t_1 + 1) + t_1 = 12 + 4t_1$$

Obtém-se dessa forma a solução geral da equação dada: $x = 4t_1 + 12$ e $y = -3t_1 + 1$, com $t_1 \in \mathbb{Z}$.

Pela relação de Euler sabe-se que $V + F = A + 2$, encontra-se $F = 12$ *faces*. Sabe-se que $x + y = 12$, então, $(4t_1 + 12) + (-3t_1 + 1) = 12$, logo $t_1 = -1$. Sabe-se que x representa o número de faces triangulares.

Assim,

$$x = 4t_1 + 12$$

$$x = 4 \cdot (-1) + 12$$

$$x = -4 + 12$$

$$x = 8 \text{ faces triangulares}$$

4.2 Descrição da segunda atividade

Prosseguindo a sequência das atividades, apresenta-se a segunda atividade, a qual traz uma questão presente no portal da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas). A OBMEP é uma ferramenta que permite que as escolas públicas avaliem o conhecimento adquirido pelos seus alunos.

As provas priorizam o raciocínio lógico, aritmética, álgebra, geometria e combinatória, mas devemos lembrar que os professores passam um bom tempo ensinando álgebra elementar aos alunos, e raramente são apresentados problemas com este enfoque. Daí a importância de abordar o assunto sobre equação diofantina linear.

Etapa 1: Apresentação da atividade

No primeiro momento, após entregar uma cópia da atividade a cada dupla ou trio formado, sugere-se que o professor faça uma leitura detalhada e compartilhada com os alunos da questão, objetivando esclarecer eventuais dúvidas com relação ao enunciado. E ao final da aula, recolher as atividades respondidas pelos alunos.

Atividade 2

(EXERCÍCIO PORTAL DA OBMEP) Determine a solução geral, em inteiros, da equação $5x + 9y = 1$.

Etapa 2: Recomendações metodológicas

Orienta-se ao professor, que destine um tempo para que os alunos possam responder a questão sem ajuda do professor e entreguem as suas resoluções ao final. No decorrer da aula, o professor poderá responder as questões junto com os alunos, seguindo a mesma ideia de resolução compartilhada da primeira atividade, em que os alunos são convidados a apresentarem suas soluções no quadro negro (ou na lousa), especialmente nesse momento, aqueles alunos que não foram ao quadro na correção da resolução da atividade 1, objetivando observar além de dificuldades apresentadas, o desempenho tanto, escrito e como na argumentação oral, de um maior número de alunos na resolução dos problemas.

Etapa 3: Resolução da atividade

Solução através do método tradicional (algoritmo de Euclides).

Tomando a equação $5x + 9y = 1$, vamos calcular o $\text{mdc}(9,5)$:

	1	1	4
9	5	4	1
4	1	0	

Tabela 8: $\text{mdc}(9,5)$.

Escrevendo 1 como combinação linear de 9 e 5 tem-se:

$$1 = 5 \cdot 2 + 9 \cdot (-1)$$

Logo, o par de inteiros $x_0 = 2$ e $y_0 = -1$ é uma solução particular da equação dada. Consequentemente, sua solução geral é:

$$\{x = 2 + 9t, y = -1 - 5t\} \text{ com } t \in \mathbb{Z}.$$

Solução através do método de sucessivas extrações de inteiros.

Tomando a equação dada $5x + 9y = 1$.

Primeiramente, identifica-se o termo da equação com coeficiente de menor valor absoluto; nesse caso, o termo $5x$. Isola-se o valor da variável escrevendo:

$$x = \frac{1 - 9y}{5}$$

Divide-se o valor do coeficiente 9 por 5 e obtém-se o quociente 1 e resto 4. Por isso, a fração que aparece na igualdade anterior pode ser escrita dessa forma:

$$x = -y + \frac{1 - 4y}{5}$$

Separa-se a equação anterior em duas, introduzindo uma variável auxiliar $t_1 \in \mathbb{Z}$.

$$x = -y + t_1 \text{ e } \frac{1 - 4y}{5} = t_1$$

A equação com a variável auxiliar é equivalente a $1 - 4y = 5t_1$. Isola-se a variável que tem o menor coeficiente em módulo:

$$y = \frac{-5t_1 + 1}{4}$$

Divide-se 5 por 4, obtendo quociente 1 e resto 1. Logo, a última equação é equivalente a

$$y = -t_1 + \frac{1 - t_1}{4}$$

Introduz a variável auxiliar $t_2 \in \mathbb{Z}$ e separa-se a equação anterior em duas:

$$y = -t_1 + t_2 \text{ e } t_2 = \frac{1 - t_1}{4}$$

Como a equação auxiliar anterior, $y = -t_1 + t_2$, tem uma variável (x ou y) com coeficiente de valor absoluto igual a 1, isola-se o valor dessa variável e faz as substituições nas equações anteriores para obter a solução do problema.

$$y = -t_1 + t_2$$

$$x = -y + t_1 = -(-t_1 + t_2) + t_1 = t_1 - t_2 + t_1 = 2t_1 - t_2$$

Obtém-se dessa forma a solução geral da equação dada: $x = 2t_1 - t_2$ e $y = -t_1 + t_2$, com t_1 e $t_2 \in \mathbb{Z}$.

4.3 Descrição da terceira atividade

Apresenta-se agora, a terceira e última atividade, que trata de um exercício proposto por Gilda de La Rocque e João Bosco Pitombeira, na 19ª Edição da Revista do Professor de Matemática (RPM 19), no qual a resolução recai sobre uma equação diofantina com duas variáveis.

Etapa 1: Apresentação da atividade

Nesta última atividade, recomenda-se ao professor com o objetivo de tirar eventuais dúvidas com relação aos enunciados das questões, seguir o mesmo procedimento inicial da atividade anterior e para realização da mesma, forme pequenos grupos com quatro alunos, pois isso possibilitará um envolvimento maior dos alunos na busca da solução do problema.

Atividade 3

Quantas quadras de basquete e quantas quadras de vôlei são necessárias para que 80 alunos joguem simultaneamente qualquer um dos esportes? (LA ROCQUE; PITOMBEIRA; PUC, Rio de Janeiro)

Etapa 2: Recomendações metodológicas

Para esta última atividade, sugere-se ao professor que responda a mesma, com base nos avanços e dificuldades apresentadas pelos alunos na resolução dos problemas no desenvolvimento das atividades anteriores, e que valorize mais uma vez, as várias estratégias de resolução dos mencionados problemas e a participação dos alunos em suas respectivas soluções.

Etapa 3: Resolução da atividade

Solução através do método tradicional (algoritmo de Euclides). (veja [\[3\]](#))

As equipes de basquete e vôlei são compostas, respectivamente, de 5 e 6 jogadores. Como precisa-se de duas equipes por quadra, modela-se o problema através da seguinte equação diofantina:

$$12x + 10y = 80$$

em que x e y representam, respectivamente, a quantidade de quadras de vôlei e basquete necessárias para acomodar os 80 jogadores.

Tem-se que o $\text{mdc}(12, 10) = 2$ e a equação dada tem solução, pois $2|80$. Dividindo a equação $12x + 10y = 80$ por 2, obtém-se a equação equivalente $6x + 5y = 40$ em que $\text{mdc}(6, 5) = 1$.

Escrevendo 1 como combinação linear de 6 e 5 tem-se:

$$6 \cdot 1 + 5 \cdot (-1) = 1$$

Multiplicando a equação por 40, obtém-se:

$$6 \cdot (40) + 5 \cdot (-40) = 40$$

Logo, o par de inteiros $x_0 = 40$ e $y_0 = -40$ é uma solução particular da equação proposta. Consequentemente, sua solução geral é dada por:

$$\begin{cases} x = x_0 + bt = 40 + 5t \\ y = y_0 - at = -40 - 6t \end{cases}, \text{ com } t \in \mathbb{Z}.$$

Como o número de quadras é natural deve-se restringir nossa resposta de modo que escolhendo t sejam satisfeitas as desigualdades:

$$x \geq 0 \text{ e } y \geq 0, \text{ assim tem-se } 40 + 5t \geq 0 \text{ e } -40 - 6t \geq 0$$

Isto é:

$$t \geq -8 \text{ e } t \leq -\frac{40}{6} \approx -6,67, \text{ daí tem-se que } -8 \leq t \leq -7$$

O que implica que:

Para $t = -8$, tem-se 0 quadras de vôlei e 8 quadras de basquete.

Para $t = -7$, tem-se 5 quadras de vôlei e 2 quadras de basquete.

Solução através do método de sucessivas extrações de inteiros.

As equipes de basquete e vôlei são compostas, respectivamente, de 5 e 6 jogadores. Como precisa-se de duas equipes por quadra, modela-se o problema através da seguinte equação diofantina:

$$12x + 10y = 80$$

em que x e y representam, respectivamente, a quantidade de quadras de vôlei e basquete necessárias para acomodar os 80 jogadores.

Dividindo a equação $12x + 10y = 80$ por 2, obtém-se a equação equivalente $6x + 5y = 40$.

Primeiramente, identifica-se o termo da equação com coeficiente de menor valor absoluto; nesse caso, o termo $5y$. Isola-se o valor da variável escrevendo:

$$y = \frac{40 - 6x}{5}$$

Divide-se os valores dos coeficientes 40 e 6 por 5 e obtém-se os quocientes 8 e 1 e restos 0 e 1, respectivamente. Por isso, a fração que aparece na igualdade anterior pode ser escrita dessa forma:

$$y = 8 - x + \frac{(-x)}{5}$$

Separa-se a equação anterior em duas, introduzindo uma variável auxiliar $t_1 \in \mathbb{Z}$.

$$y = 8 - x + t_1 \quad \text{e} \quad \frac{(-x)}{5} = t_1$$

A equação com a variável auxiliar é equivalente a $-x = 5t_1$.

Como a equação auxiliar anterior, $-x = 5t_1$, tem uma variável (x, y ou z) com coeficiente de valor absoluto igual a 1, isola-se o valor dessa variável e faz as substituições nas equações anteriores para obter a solução do problema.

$$-x = 5t_1$$

$$x = -5t_1$$

$$y = 8 - x + t_1 = 8 - (-5t_1) + t_1 = 8 + 6t_1$$

Obtém-se dessa forma a solução geral da equação dada: $x = -5t_1$ e $y = 8 + 6t_1$, com $t_1 \in \mathbb{Z}$.

Como o número de quadras é natural devemos restringir nossa resposta de modo que escolhendo t sejam satisfeitas as desigualdades:

$$x \geq 0 \text{ e } y \geq 0, \text{ assim tem-se } -5t_1 \geq 0 \text{ e } 8 + 6t_1 \geq 0$$

Isto é:

$$t \leq 0 \text{ e } t \geq -\frac{8}{6} \approx -1,33, \text{ daí tem-se que } -1 \leq t \leq 0$$

O que implica que:

Para $t = 0$, tem-se 0 quadras de vôlei e 8 quadras de basquete.

Para $t = -1$, tem-se 5 quadras de vôlei e 2 quadras de basquete.

CONSIDERAÇÕES FINAIS

A educação é fundamental para o desenvolvimento de uma pessoa, estado ou nação. Entretanto, melhorar a qualidade da educação de modo geral, depende de como é conduzido esse processo, o que ainda há muito a se fazer. Sabe-se que a deficiência na formação dos professores e os escassos recursos materiais são questões que se repetem há décadas. São muitas as dificuldades no ensino de maneira geral, e quando falamos de matemática então, as dificuldades parecem aumentar exponencialmente.

Espera-se com esse trabalho que após a aplicação de algumas aulas sobre equações diofantinas lineares, o aluno seja capaz de identificar problemas, não só matemáticos, mas também de outros ramos do conhecimento, que possam ser modelados e em seguida resolvidos por meio dessas equações.

Diante das conclusões obtidas, percebe-se a importância desse conteúdo que poderia estar no currículo do ensino médio, sabendo que a base necessária para trabalhá-lo é abordada desde o ensino fundamental. Acredita-se que ao se falar de equações diofantinas no ensino médio o professor instiga o aluno a relacionar as situações-problema com equações de reta da forma $ax + by = c$ e dessa forma faça com que o aluno entenda que este tipo de equação facilita a resolução de muitos problemas da vida cotidiana.

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ALVES, Lucinda Freese. Aplicações de Equações Diofantinas e um Passeio pelo Último Teorema de Fermat. Jataí, 2017.
- [2] ANDRADE, Lenimar Nunes. Mais sobre resolução de equações em números inteiros. Revista do Professor de Matemática 79. UFPB, João Pessoa, 2021.
- [3] BORGES, Fábio Vieira de Andrade. Equações diofantinas lineares em duas incógnitas e suas aplicações. Goiânia, 2013.
- [4] BOYER, Carl B. História da Matemática. Revista por Uta C. Merzabach; tradução Elza F. Gomide. Edgard Blucher, São Paulo, 2003.
- [5] CAMPOS, Giseli D. Maciano. Equações Diofantinas Lineares. Cuiabá, MT, 2013.
- [6] DOMINGUES, Hygino Hugueros. Fundamentos da Aritmética. 2. ed. rev. Florianópolis: Ed. da UFSC, 2017.
- [7] FERREIRA, Hugo Brener Oliveira; DOMINGUES, José Sérgio. Equações diofantinas lineares: fundamentação matemática e um algoritmo de resolução. Revista Científica IFMG, Campus Formiga, Formiga, v.1, n.1, p.22-32, jul/dez. 2013.
- [8] HEFEZ, Abramo. Aritmética, Coleção PROFMAT, 1ª edição. Rio de Janeiro, 2014.
- [9] LA ROCQUE, Gilda; PITOMBEIRA, João Bosco. Uma equação diofantina e suas resoluções. Revista do Professor de Matemática 19. PUC, Rio de Janeiro, 2021.
- [10] LEITE, Kalama Guimarães. Equação diofantina linear: aplicações no ensino médio. Macapá, 2014.
- [11] MENEZES, Darcy Lela. Abecedário da Álgebra. 1º Volume - Ciclo Ginásial, 4ª edição. Livraria Nobel, São Paulo, 1971.
- [12] SILVA, Adriano Valeriano. Uso das equações diofantinas lineares no ensino fundamental. Maceió, 2013.