UNIVERSIDADE FEDERAL DO AMAPÁ
DEPARTAMENTO DE CIÊNCIAS EXATAS
COLEGIADO DE MATEMÁTICA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

ELIAZE DA SILVA BRAGA
RENATO CARDOSO DO CARMO

APLICAÇÕES DE EQUAÇÕES DIOFANTINAS

MACAPÁ
2018

ELIAZE DA SILVA BRAGA
RENATO CARDOSO DO CARMO

APLICAÇÕES DE EQUAÇÕES DIOFANTINAS

Trabalho de Conclusão de Curso (TCC) apresentado ao curso de Matemática, como requisito parcial para obtenção do Título de Licenciatura Plena em Matemática, Departamento de Ciências Exatas da Universidade Federal do Amapá - UNIFAP.
Orientador: Professor Me Sérgio Barbosa de Miranda.

MACAPÁ
2018

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Central da Universidade Federal do Amapá
Bibliotecária Orinete Costa Souza CRB-11/920

306.85
S586c
Braga, Eliaze da Silva
Aplicações de equações diofantinas / Eliaze da Silva Braga, Renato Cardoso do Carmo ; orientador, Sérgio Barbosa de Miranda. - Macapá, 2018. 43 f.

Trabalho de Conclusão de Curso (Graduação)- Fundação Universidade Federal do Amapá, Coordenação do Curso de Licenciatura em Matemática.

1. Equação diofantina. 2. Divisibilidade. 3.Congruência linear. I. Carmo, Renato Cardoso do. II. Miranda, Sérgio Barbosa de, orientador. III. Fundação Universidade Federal do Amapá. IV. Título.

ELIAZE DA SILVA BRAGA
RENATO CARDOSO DO CARMO

APLICAÇÕES DE EQUAÇÕES DIOFANTINAS

A banca examinadora aprova a Monografia defendida à mesma, como parte da exigência para a obtenção do grau de Licenciado em Matemática, pela Universidade Federal do Amapá – UNIFAP.

MACAPÁ
2018

Profº Me. Sérgio Barbosa de Miranda
Orientador - Universidade Federal do Amapá

Profº Me Márcio Lobato Bahia
Membro-Universidade Federal do Amapá

Profº Me Welber Aires de Oliveira
Membro-Universidade Federal do Amapá

AGRADECIMENTOS

Primeiramente, agradecemos a Deus por nos ter concedido força e determinação para buscarmos a realização de mais um sonho.

A família por toda dedicação, paciência e incentivo proporcionado durante a caminhada.

Aos professores que sempre nos apoiaram e estavam dispostos a ajudar e contribuir para um melhor aprendizado.

Aos colegas de classe pelo companheirismo.

Enfim, agradecemos a todos que participaram direto ou indiretamente desta etapa de nossas vidas.

A maravilhosa disposição e harmonia do universo só pode ter tido origem segundo o plano de um Ser que tudo sabe e tudo pode. Isso fica sendo a minha última e mais elevada descoberta.

Isaac Newton

RESUMO

O trabalho apresenta um estudo relacionado a equação diofantina e suas aplicações. Para chegar ao estudo das equações diofantinas, foi preciso uma abordagem preliminar dos conteúdos de divisibilidade no conjunto dos números inteiros e congruência linear como métodos de resolução. A partir das definições e métodos de soluções de equações diofantinas são expostos alguns problemas que ilustram a potencialidade da aplicação desta ferramenta.

Palavras-chave: Equação diofantina. Divisibilidade. Congruência linear.

ABSTRACT

The work presents a study related to the diophantine equation and its applications. In order to arrive at the study of Diophantine equations, a preliminary approach was required to the contents of divisibility in the set of integers and linear congruence as methods of resolution. From the definitions and methods of solutions of diophantine equations are presented some problems that illustrate the potentiality of the application of this tool.

Keywords: Diophantine equation. Divisibility. Linear congruence.

LISTA DE FIGURAS

Sumário

INTRODUÇÃO

O trabalho tem por finalidade a utilização das equações diofantinas como uma importante ferramenta na solução de problemas aritméticos, abordando conceitos da teoria dos números, promovendo uma integração da aritmética com a álgebra.

A principio faremos uma breve referencia histórica acerca do matemático Diofanto de Alexandria, denotando sua vida e contribuição para o desenvolvimento da matemática. Em seguida, faremos estudos preliminares dos conteúdos de teoria dos números que servirá de base nos estudos do referido tema, como divisibilidade no conjunto dos números inteiros, suas propriedades e proposições, máximo divisor comum (mdc) e algoritmo de Euclides, destacando também, Congruência Linear como ferramenta de resolução.

Nos capítulos posteriores faremos um estudo qualitativo em cima das equações diofantinas lineares e sua resolução, como condições de existências de soluções e de que forma podemos determiná-las, destacando sempre que nosso principal interesse é pelas soluções inteiras.

No último capítulo faremos a aplicação do estudo acima referido em busca de solucionar situações-problemas, evidenciando a praticidade do método de equações diofantinas.

Portanto, este trabalho tem objetivo de expressar a importância do estudo das equações Diofantinas Lineares, e quando colocada em prática se torna uma ferramenta muito forte na resolução de problemas desta e de outras áreas que podem levar o leitor a um alto nível de raciocínio e habilidades.

Capítulo 1

CONCEITOS INICIAIS

Para inicio deste trabalho, vamos abranger um pouco da história do matemático Diofanto de Alexandria, que é o autor das Equações Diofantinas, tema de abordagem principal desta monografia.

Em sequência, abordaremos também um pouco da parte teórica, mais precisamente de Divisibilidade em $\mathbb{Z}$, Máximo Divisor Comum, Algoritmo da Divisão de Euclides e Congruência Linear.

Pra melhor compreensão sobre as primeiras manifestações algébricas; faremos menção de uma pequena divisão acerca da álgebra, por Sr.G.H.F Nesselmem (1842) *destaca-se três momentos distintos.*

- **Primitivo**

  Tudo é completamente escrito em palavras. Ou seja, não havia abreviações ou simbologia.

- **Intermediario**

  É onde se adota algumas abreviações.

- **Final**

  Nesse momento as resoluções são expressas numa espécie de taquigrafia matemática, formada por símbolos que aparentemente fazem pouca relação com os entes que representavam (Ives ,p 206).

É fato que não há chance de definir uma linha clara de definição exata sobre o desenvolvimento da álgebra na história da matemática. Visto que houve inúmeras contribuições distintas para a formação da álgebra que se estuda atualmente.

Por volta de 2000 a.C a aritmética babilônica parecia ter evoluído para uma álgebra retórica desenvolvida. Eles resolviam equações lineares e quadráticas com duas incógnitas, tanto pelo método equivalente ao de substituição numa fórmula geral, como pelo método de completar quadrados. A álgebra naquela época era utilizada para resolver problemas por meio de equações que ainda, nos dias de hoje, requerem uma considerável habilidade

numérica, e nota-se ainda que os babilônicos eram infatigáveis construtores de tábuas de cálculos, calculistas extremamente hábeis e certamente mais fortes em álgebra do que em geometria. (Eves, 2004,p.63)

1.1 Diofanto de Alexandria

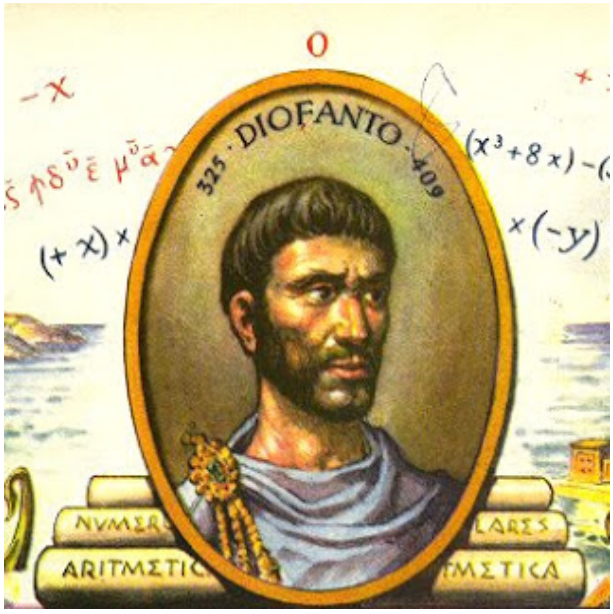

Figura 1.1: Imagem de Diofanto com um escrito de um epitáfio em seu túmulo
Fonte: Imagens públicas do google

Considera-se que por volta de 250 d. C. Diofanto de Alexandria passou a desempenhar sua contribuição nos campos da Álgebra e Teoria dos Números. A verdade é que pouco se sabe em relação a vida de Diofanto, sendo incerto até mesmo o período em que viveu. Mas acredita-se que nasceu 200 d. C. e morreu em cerca de 284 d. C. em Alexandria. Uma tradição, relatada em uma coleção de problemas chamada "antologia grega", e descrita 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 concedeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Aí! Infeliz, criança; depois de chegar à metade da vida de seu pai, o destino frio o levou. Depois de consolar sua dor com a ciência dos números por quatro anos ele terminou sua vida" [Cohen e Dranbkin, 1958; p.27]*
>
> *(Boyer; p. 133)*

Se o enigma é historicamente exato, Diofante viveu oitenta e quatro anos.

A aritmética de Diofante era um tratado caracterizado por um alto grau de habilidade matemática e de engenho. Neste aspecto, sua obra pode ser comparado aos grandes clássicos da idade Alexandrina anterior; no entanto, quase nada tem em comum com esses ou, na verdade, com qualquer matemática grega tradicional. Representa essencialmente um novo ramo e usa uma abordagem diferente, desvinculado dos métodos geométricos, assemelha-se a álgebra babilônica em muitos aspectos mas, enquanto os matemáticos babilônicos se ocupavam principalmente com soluções aproximadas de equações determinadas de até terceiro grau, a aritmética de Diofante e quase toda dedicada à resolução exata de equações tanto determinadas quanto indeterminadas. Devido à ênfase dada na aritmética à solução de problemas indeterminados, o assunto, as vezes chamado análise indeterminada, tornou-se conhecido como análise Diofantina.

Seguramente Diofanto escreveu três tratados: Aritmética, em 13 livros dos quais 6 sobreviveram, Sobre Números Poligonais, do qual restaram fragmentos, e Porismas, que foi perdido. Seu tratado Aritmético (no grego, significa "ciência dos números") é uma obra-prima, pioneira no tratamento do difícil assunto a que hoje chamamos de Teoria dos Números, sem deixar qualquer dúvida de que seu autor era um gênio do mais alto nível. Apesar de Euclides e outros já terem feito algumas descobertas importantes nessa área, Diofanto realizou avanços incomparáveis, mostrando em seu livro sucessivos exemplos das melhores qualidades de um grande matemático.

1.2 Divisibilidade em $\mathbb{Z}$

Definição 1.1. *Dados $a, b \in Z$ e $b \neq 0$, dizemos que b divide a, ou que a é um múltiplo de b, ou ainda que b é um divisor de a se, e somente se existe $c \in Z$ tal que $a = bc$.*

Note que o c da definição é uma solução da equação $bx = a$. Esta equação pode não ter solução em $\mathbb{N}$, por exemplo, $2x = 7$ não tem solução em $\mathbb{Z}$, mas sempre tem solução em $\mathbb{Q}$.
Por esse motivo, só estudaremos divisibilidade em $\mathbb{Z}$.

Destacamos quatro consequências imediatas dessa relação.

1. Para todo $a \in \mathbb{Z}$, 1 divide a; já que $a = 1.a$.
2. Para todo $a \in \mathbb{Z}$, a divide a; já que $a = a.1$.
3. Para todo $a \in \mathbb{Z}$, a divide 0; já que $0 = a.0$.
4. Para todo $a, d \in \mathbb{Z}$, d divide a implica que $|d| \leq |a|$.

A partir de agora usaremos a notação $a|b$ para indicar que a divide b. Note que $a|b \Leftrightarrow b = ac$, $c \in \mathbb{Z}$. Se $b \neq 0$, o inteiro c nas condições da definição é único.
De acordo com a definição de divisibilidade apresentamos as seguintes proposições.

Proposição 1.1. *Se $a|1$, então $a = \pm 1$.*

Demonstração. De fato, se a divide 1, existe um $q \in \mathbb{Z}$ tal que $1 = qa$. O que implica que $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, ou seja $a = \pm 1$. □

Proposição 1.2. *Se a, b, c e d são inteiros com $a \neq 0$ e $b \neq 0$, tais que $a|b$ e $c|d$, então $ac|bd$.*

Demonstração. Existem $x, y \in \mathbb{Z}$ tais que, se $a|b$ então $b = xa$ e se $c|d$ então $d = yc$. Multiplicando-se as equações membro a membro temos que $bd = ac(xy)$, daí $ac|bd$. □

Proposição 1.3. *Se a, b e c são inteiros com $a \neq 0$ e $b \neq 0$, tais que $a|b$ e $b|c$, então $a|c$.*

Demonstração. Existem $x, y \in \mathbb{Z}$, tais que, se $a|b$ então $b = ax$ e se $b|c$, então $c = by$. Assim, $c = a(xy)$, portanto, $a|c$. □

Proposição 1.4. *Sejam a e b inteiros e diferentes de zero, se $a|b$ e $b|a$, então $a = \pm b$.*

Demonstração. Existe $x, y \in \mathbb{Z}$, tais que se $a|b$, então $b = ax$ e também se $b|a$, então $a = by$. Logo $a = a(xy)$ o que implica $xy = 1$, assim $x|1$, e daí temos que $x = \pm 1$ e que $a = \pm b$. □

Proposição 1.5. *Sejam a e b inteiros e diferentes de zero, se $a|b$ então $|a| \leq |b|$.*

Demonstração. Existe $x \in \mathbb{Z}$ com $x \neq 0$ tal que se $a|b$, então $b = ax$, ou seja $|b| = |a|\,|x|$. Como $x \neq 0$, temos que $|x| \geq 1$, desse modo segue que $|a| \leq |b|$. □

Proposição 1.6. *Se a, b, c, x e y são inteiros com $a \neq 0$, tais que se $a|b$ e se $a|c$, então $a|(bx + cy)$.*

Demonstração. Existe u, $v \in \mathbb{Z}$ tais que se $a|b$, então $b = au$ e se $a|c$, então $c = av$. Logo, quaisquer que sejam os inteiros x e y temos que $bx+cy = (au)x+(av)y = a(ux)+a(vy) = a(ux + vy)$, o que implica que $a|(bx + cy)$. □

1.3 Máximo Divisor Comum

O conceito de Máximo Divisor Comum é bastante usado nas mais variadas áreas do conhecimento. Com essa ferramenta somos capazes, por exemplo, de prever alinhamentos de corpos celestes, estudar o ciclo de vida de alguns seres vivos, construir, de modo a garantir o mínimo de desperdício, mosaicos de azulejos que podem ser utilizados na arquitetura, dentre outros. *(Freitas, Carlos Wagner Almeida; p. 78).*

Neste trabalho, é muito importante a caracterização de Máximo Divisor Comum, pois compreende uma considerável parcela da Teoria dos Números.

O conjunto $D(a, b)$ de todos os divisores comuns de a e b é limitado superiormente, pois se $a \neq 0$ para todo elemento $c \in D(a, b)$ temos que $c \leq |a|$. Logo $D(a, b)$ tem máximo. Chama-se máximo divisor comum de a e b o maior de seus divisores comuns, $mdc(a, b) = maxD(a, b)$.

Dados a, $b \in \mathbb{Z}$ diz-se que um inteiro d é Máximo Divisor Comum entre a e b se, e somente se são válidas as seguintes condições.

1. $d \geq 0$
2. $d|a$ e $d|b$

3. Para todo número inteiro d', se $d'|a$ e $d'|b$, então $d'|d$.

Exemplo 1.1. *Sejam $a = 12$ e $b = 4$, determine o $mdc(12, 4)$.*

Solução: Sabemos que o divisor de um número inteiro é todo o número inteiro que ao dividir tal número, resultará em uma divisão exata. Com essa informação vamos determinar o conjunto dos divisores de $a = 12$ e de $b = 4$, sendo denotados por D_{12} e D_4. Assim, $D_{12} = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $D_4 = \{\pm1, \pm2, \pm4\}$. Como o $mdc(12, 4)$ é o maior inteiro que divide 12 e 4, para encontrar o máximo divisor comum entre esses números , basta determinar a intersecção $D_{12} \cap D_4$ e tomar o maior número em módulo desse conjunto. Logo, $D_{12} \cap D_4 = \{\pm1, \pm2, \pm4\}$ e $máx(D_{12} \cap D_4) = 4$. Portanto, o $mdc(12, 4) = 4$.

1.4 Algoritmo da Divisão de Euclides

Teorema 1.1. *(Algoritmo da Divisão de Euclides) Para quaisquer a, $b \in \mathbb{Z}$, com $b > 0$, existe um único par de inteiros q e r, de modo que $a = bq + r$, onde $0 \leq r < b$.*

Demonstração. Será dividida em duas partes.

1. Prova da existência:

   Seja b um número inteiro positivo não nulo. Se $a \in \mathbb{Z}$, então a é multiplo de b ou está compreendido entre dois múltiplos consecutivos de b, isto é, $bq \leq a < b(q+1)$. Se $bq \leq a$, então $a = bq + r$, onde $r \in \mathbb{Z}$ e $r \geq 0$. Se $a < b(q + 1)$, temos que $bq + r < bq + b$, daí $r < b$. Logo, podemos afirmar que $a = bq + r$, com $0 \leq r < b$.

2. Prova de Unicidade

Suponhamos que existam inteiros q_1, q_2, r_1, r_2, onde $q_1 \neq q_2$ e $r_1 \neq r_2$, com $r_1 > r_2$ e que satisfaçam as igualdades: $a = bq_1 + r_1$, com $0 \leq r_1 < b$ e $a = bq_2 + r_2$, com $0 \leq r_2 < b$. Se $b > r_1$ e $b > r_2$, então $b > r_1 - r_2$ e temos que $a = bq_1 + r_1 = bq_2 + r_2$ o que implica que $b(q_2 - q_1) = r_1 - r_2$. Fazendo $k = (q_2 - q_1)$, temos que $r_1 - r_2 = bk$ com $k \in \mathbb{Z}$, mostrando que $b|(r_1 - r_2)$.

Portanto, $b \leq (r_1 - r_2)$ é absurdo, pois contradiz a hipótese. Logo, $r_1 = r_2$ e concluímos também que $b(q_2 - q_1) = 0$. Se $b \neq 0$, temos $(q_2 - q_1) = 0$, mostrando que $q_2 = q_1$. □

Proposição 1.7. *Quaisquer que sejam a, $b \in \mathbb{Z}$, existem $d \in \mathbb{Z}$ que é o máximo divisor comum de a e b.*

Demonstração. O caso em que $a > 0$ e $b > 0$.

Seja $k = \{ax + by; x, y \in \mathbb{Z}\}$. Tomando os elementos estritamente positivos de k. Seja d o menor desses elementos.

Vamos mostrar que d é o máximo divisor comum entre a e b.

1. Como $d \in \mathbb{K}^+$, então $d \geq 0$.

2. Como $d \in \mathbb{K}$, então existem x_0 e $y_0 \in \mathbb{Z}$ tais que;

   $d = ax_0 + by_0$

   Aplicando o algoritmo da divisão aos elementos a e d;

   $a = dq + r$, com $0 \leq r \leq d$

   Das duas últimas igualdades teremos;

   $a = (ax_0 + by_0)q + r$

   $a = ax_0q + by_0q + r$

   $r = a(1 - x_0q) + b(-y_0)q$

   Dessa forma $r \in \mathbb{K}$, $r \geq 0$. Como $r < d$ e d é o menor elemento de $\mathbb{K}$, temos:

   $r = d = 0$;

   Onde

   $a = dq \Longrightarrow d|a$

   Aplicando o algoritmo da divisão aos elementos b e d.

   $b = dq' + r'$, com $0 \leq r' < d$

   $b = (ax_0 + by_0)q' + r'$

   $r' = b - by_0q' - ax_0q'$

   $r' = b(1 - q'y_0) + a(-x_0)q'$

   Logo, $r' = 0 \Longrightarrow b = dq' \Longrightarrow d|b$

3. Se $d'|a$ e $d'|b$, temos;

   $a = d'k$

   $b = d'q$

   $ax_0 = d'kx_0$ e $by_0 = d'ky_0$

   $ax_0 + by_0 = d'(kx_0 + qy_0)$

   $d = d'(kx_0 + qy_0)$

   Portanto, $d'|d$ o que implica que $d = mdc(a, b)$

□

Lema 1.1. *Sejam a e b dois inteiros positivos e $a = bq + r$, com $0 \leq r < b$. Então $mdc(a, b) = mdc(b, r)$.*

Demonstração. Com efeito, se $a = bq + r$, então $r = a - bq$. Seja k um divisor comum de a e de b, então $k|a$ e $k|b$. Assim, $k|r$, ou seja, k é um divisor comum de b e de r. Reciprocamente, como $a = bq + r$, temos que todo divisor comum de b e de r é divisor comum de b e de a. Assim, o conjunto de divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e de r. Logo, $mdc(a, b) = mdc(b, r)$. □

Demostrado esse resultado, podemos enunciar e provar o algoritmo de Euclides:

Teorema 1.2. *Sejam a e b inteiros positivos, com $a \leq b$. Usando sucessivamente o algoritmo da divisão, segue do lema 1 que o problema de achar o $mdc(a, b)$ reduz-se a achar o $mdc(b, r)$.*

Demonstração. Naturalmente, repetindo esse processo e fazendo divisões sucessivas, teremos:

$a = bq_1 + r_1$, com $0 \leq r_1 < b$

$b = r_1q_2 + r_2$, com $0 \leq r_2 < r_1$

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

$r_{n-2} = r_{n-1}q_n + r_n$, com $0 \leq r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1} + r_{n+1}$, com $r_{n+1} = 0$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões deve ser exata. Suponhamos então que r_{n+1} seja o primeiro resto nulo, como está indicado antes. Do lema 1, temos que:

$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = ... = mdc(r_{n-1}, r_n)$

Demonstramos que, nesse processo o máximo divisor comum de a e b é o último resto diferente de zero. □

É usual o seguinte dispositivo de cálculo no emprego do algoritmo de Euclides para encontrar o $mdc(a, b)$ de acordo com o Teorema 2:

Geralmente, para dividir a por b utilizamos o seguinte esquema:

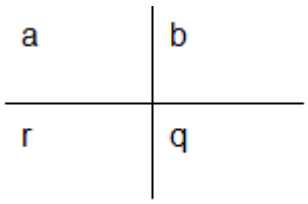

Figura 1.2: Esquema de divisão usual
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

Mudando o esquema temos;

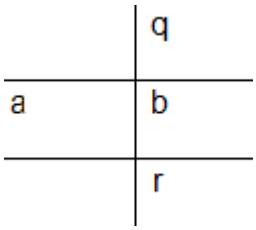

Figura 1.3: Esquema de divisão de Euclides
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

Aplicando o dispositivo prático do cálculo do $mdc(a, b)$ dispomos os números;

	q_1	q_2	q_3	...	...	q_n	q_{n+1}
a	b	r_1	r_2		r_{n-2}	r_{n-1}	r_n
	r_1	r_2	r_3			r_n	0

Figura 1.4: Dispositivo de cálculo do *mdc*
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

O procedimento exposto se traduz na seguinte REGRA:

Para se "achar" o *mdc* de dois inteiros a e b positivos, divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até encontrar um resto nulo. O último resto não nulo é o máximo divisor comum procurado.

Teorema 1.3. *(Bézout)*

Sejam a e b dois números inteiros não nulos simultaneamente e seja $d = mdc(a, b)$; nestas condições, existem inteiros r e s tais que;

$d = ra + sb$

Demonstração. Consideremos o conjunto $A = \{(ma + nb) > 0; \quad m, \quad n \in \mathbb{Z}\}$. Note que $A \neq \emptyset$, logo pelo PBO existe $d_1 = minA > 0$. Como $d_1 \in A$, então existem r e $s \in \mathbb{Z}$, tais que; $d_1 = ra + sb$. E observando que $d|a$ e $d|b$ resultam que $d|d_1$, daí temos $d \leq d_1$.

Com essa afirmação, obtemos $d_1|a$ e $d_1|b$. Suponha que d_1 não divide nem a e nem b, assim existiriam números inteiros q, q' e t, t', tais que;

$a = qd_1 + t, \quad com \quad 0 < t < d$

$b = q'd_1 + t', \quad com \quad 0 < t' < d$

Segue-se;

$t = a - qd_1 = a - q(ra + sb) = a - qra - qsb = (1 - qr)a + (-qs)b$

$t' = b - q'd_1 = b - q'(ra + sb) = b - q'ra - q'sb = (-q'r)a + b(1 - q's)$

Como $0 < t, t' < d_1$ temos que $t, t' \in A$, absurdo, pois $0 < t < d_1 = minA$. Portanto, d_1 é divisor comum positivo de a e b, logo $d_1 \leq d$ e então $d_1 = d$.

□

Além de servir de ferramenta computacional para o cálculo do mdc, a divisão euclidiana tem consequências teóricas importantes. O algoritmo de Euclides também pode ser usado para achar a expressão do $mdc(a, b) = r_n$ como combinação linear de a e de b. Para isso basta eliminar sucessivamente os restos r_{n-1}; r_{n-2}; ;...; r_3; r_2; r_1 entre as n primeiras igualdades do **Teorema 1.2**.

Exemplo 1.2. *Achar o* $mdc(963, 657)$ *pelo algoritmo de Euclides e sua expressão como combinação linear de* 963 *e* 657*.*

Solução: Aplicando as divisões sucessivas, temos:

	1	2	6	1	4
963	657	306	45	36	9
	306	45	36	9	0

Figura 1.5: $mdc(963, 657)$
. Fonte: BISPO, Dinguiston S. **Equação Diofantina Linear e suas Aplicações**

$963 = 657.1 + 306$, então $306 = 963 - 657.1$

$657 = 306.2 + 45$, então $45 = 657 - 306.2$

$306 = 45.6 + 36$, então $36 = 306 - 45.6$

$45 = 36.1 + 9$, então $9 = 45 - 36.1$

$36 = 9.4 + 0$

Portanto, o $mdc(963, 657) = 9$ e a sua expressão como combinação linear de 963 e 657 se obtém eliminando os restos 36, 45 e 306 entre as quatro primeiras igualdades anteriores do seguinte modo:

$9 = 45 - 36 = 45 - (306 - 45.6) = -306 + 7.45 = -306 + 7(657 - 306.2) = 7.657 - 15.306 = 7.657 - 15(963 - 657) = 963(-15) + 657.2$

Assim, a expressão do $mdc(963, 657) = 9$ como combinação linear é:

$963x + 657y = 9$, onde $x_0 = -15$ e $y_0 = 2$.

Definição 1.2. *Diz-se que dois números inteiros* a *e* b *são primos entre si se, e somente se,* $mdc(a, b) = 1$*.*

Teorema 1.4. *Os números inteiros* a *e* b *são primos entre si se, e somente se, existem* r*,* $s \in \mathbb{Z}$ *tais que:*

$ra + sb = 1$

Demonstração. ($\Longrightarrow$) Como a e $b \in \mathbb{Z}$ são primos entre si, por definição temos que $mdc(a,b) = 1$. Fazendo uso do teorema de Bézout existem $r, s \in \mathbb{Z}$, tais que:

$ra + sb = 1$

($\Longleftarrow$) Suponhamos que $d = mdc(a,b)$ e ainda temos que existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$. Como $d|a$ e $d|b$ isso implica $d|(ra + sb)$ daí $d|1$ o que resulta $d = 1$, assim o $mdc(a,b) = 1$.

Portanto a e b são primos entre si.

□

Teorema 1.5. *(Euclides)*

Sejam a, b e $c \in \mathbb{Z}$ tais que $a|(b.c)$. Se $mdc(a,b) = 1$, então $a|c$.

Demonstração. Como $a|(bc)$ temos que existe $k \in \mathbb{Z}$ tal que $bc = ak$.

De $mdc(ab) = 1$, temos que existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$. Multiplicando por c e substituindo (bc) nesta última igualdade, obtemos:

$c = rac + sbc$

$c = rac + sak$

$c = (rc + sk).a$

$c = (xa)$; $x \in \mathbb{Z}$

Logo a divide 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. Inicialmente nota-se que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, pois d é um divisor comum de a e b.

Agora como $mdc(a,b) = d$, então existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = d$. Dividindo ambos os membros desta igualdade por d, temos que:

$\left(\frac{a}{d}\right) x_0 + \left(\frac{b}{d}\right) y_0 = 1$

Pelo **Teorema 1.4:** os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, assim, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

□

Exemplo 1.3. *Note que $mdc(12, 30) = 6$, daí pelo corolário acima temos que $mdc\left(\frac{12}{6}, \frac{30}{6}\right) = mdc(2,5) = 1$.*

Teorema Fundamental da Aritmética

Um número natural é um número primo quando ele tem exatamente dois divisores naturais distintos: o número 1 e ele mesmo. Já nos inteiros um número $p \in \mathbb{Z}$ é primo se ele tem exatamente quatro divisores distintos: ± 1 e $\pm p$. Se um número inteiro tem módulo maior que 1 e não é primo, diz-se que é **composto**. Por convenção, os números 0, 1 e -1 não são considerados primos nem compostos. O Teorema Fundamental da Aritmética coloca em evidência o papel dos números primos na estrutura dos inteiros. Ele nos assegura que um número pode ser expresso como um produto de números primos de modo único, a menos da ordem desses fatores primos.

Teorema 1.6. *Todo número inteiro maior do que* 1 *se escreve como o produto único de números primos, a menos da ordem desses fatores primos.*

Demonstração. Vamos supor que o teorema seja falso. Seja n o menor inteiro maior do que 1 que não pode ser escrito como produto de primos.

Note que n não pode ser primo, pois se fosse seria a sua própria decomposição em fatores primos. Assim n seria composto podendo ser escrito como $n = ab$, com $0 < a < n$ e $0 < b < n$. Nesse caso, a e b podem ser decomposto em produtos primos, pois ambos são menores que n, já que pela hipótese o menor número que não pode ser decomposto em fatores primos é o n. Logo teríamos;

$a = p_1.p_2.p_3.p_4...p_n$ onde $p_1, p_2, p_3, p_4...p_n$ são números primos não necessariamente distintos e.

$a = q_1.q_2.q_3.q_4...q_n$ onde $q_1, q_2, q_3, q_4...q_n$ são números primos não necessariamente distintos. Daí tem;

$n = ab = p_1.p_2.p_3.p_4...p_n...q_1.q_2.q_3.q_4...q_n$

Dessa forma teríamos n escrito como produto de primos, o que contraria a escolha do n.

Logo todo inteiro maior do que 1 se escreve como produto de números primos. □

1.5 Congruência

Definição 1.3. *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulos m se m divide a diferença $a - b$.*

Notação: $a \equiv b(mod \quad m) \iff m|(a - b)$

Em outros termos a é congruente a b módulo m se, e somente se, existe um inteiro k tal que $a = b + km$.

Se m não divide a diferença de a e b, então dizemos que a é incongruente b módulo m.

Proposição 1.8. $a \equiv b(mod \quad m) \iff$ *a e b deixam o mesmo resto na divisão por m.*

Demonstração. ($\Longrightarrow$) Se a e b deixam o mesmo resto quando divididos por m, temos;

$a = qm + r$ e $b = pm + r$, com $0 \leq r \leq |m|$

Isso acontece para certos p e q inteiros.

$a - b = qm - pm$

$a - b = (q - p)m \Longrightarrow m|(a - b)$

($\Longleftarrow$) Se $m|(a - b)$, então existe $k \in \mathbb{Z}$ tal que;

$a - b = km$

$a = km + b$

Por outro lado, a divisão euclidiana garante que existem q e r pertencentes a $\mathbb{Z}$ tais que;

$a = qm + r$, com $0 \leq r < |m|$

Assim, temos;

$km + b = qm + r$

$b = (k - q)m + r$, com $0 \leq r < |m|$

Note que a unicidade do resto da divisão euclidiana garante que a e b deixam o mesmo resto quando divididos por m. □

Exemplo 1.4. $3 \equiv 24(mod \quad 7)$, *pois* $\quad 7|(3 - 24)$, *donde que* $-21 = 7(-3)$.

Proposição 1.9. *Seja $m \neq 0$ um inteiro e a, b, $c \in \mathbb{Z}$. Então a congruência módulo m satisfaz;*

1. Reflexibilidade: $a \equiv b(mod \quad m)$

   Demonstração. Note que $m|0$, pois existe $c \in \mathbb{Z}$ tal que $0 = mc(0 = m0)$.

   Assim, $m|(a - a) \Longrightarrow a \equiv a(mod \quad m)$. □

2. Simetria: Se $a \equiv b(mod \quad m)$, então $b \equiv a(mod \quad m)$.

   Demonstração. Se $a \equiv b(mod \quad m)$, então para algum $k_1 \in \mathbb{Z}$ temos $a = b + k_1 m$. Daí,

   $b = a - k_1 M$

   $b = a + (-k_1)M$

   Assim, existe um inteiro $x = -k_1$ tal que $b = a + xm$. Logo, por definição $b = a(mod \quad m)$. □

3. Transitividade: Se $a \equiv b(mod \quad m)$ e $b \equiv c(mod \quad m)$, então $a \equiv c(mod \quad m)$.

   Demonstração. Como $a \equiv b(mod \quad m)$ e $b \equiv c(mod \quad m)$, então existe k_1 e k_2 inteiros, tais que;

   $a - b = k_1 m$ e $b - c = k_2 m$

   Somando membro a membro das duas últimas equações obtemos;

   $a - c = (k_1 + k_2)m$

   Portanto $a \equiv c(mod \quad m)$

   □

A relação de congruência módulo m é uma relação de equivalência, pois acabamos de mostrar que ela é reflexiva, simétrica e transitiva.

Observações:

1. Dois inteiros quaisquer são congruentes módulo 1.
2. Dois inteiros são congruentes módulo 2, se ambos são pares ou ambos ímpares.
3. $a \equiv 0(mod \quad m)$ se, e somente se, $m|a$.

Exemplo 1.5. *Mostrar que se* $a \equiv 7(mod \quad 12)$*, então* $a \equiv 3(mod \quad 4)$ *para todo* $a \in \mathbb{Z}$*.*

Solução: Note que $a \equiv 12(a-7)$ o que implica que $a - 7 = 12k$, $k \in \mathbb{Z}$. Pelas propriedades operatórias, fazemos;

$a - 3 - 4 = 12k$

$a - 3 = 4 + 12k$

$a - 3 = 4(1 + 3k)$

Assim, $a - 3 = 4x$, tal que $x \in \mathbb{Z}$

Temos que $4|(a-3)$, por definição de congruência, obtemos $a \equiv 3(mod \quad 4)$.

Teorema 1.7. *Se a, b, c, m são inteiros tais que* $a \equiv b(mod \quad m)$*, então;*

1. $(a + c) \equiv (b + c)(mod \quad m)$.

   Demonstração. Como $a \equiv b(mod \quad m)$, então para algum $k \in \mathbb{Z}$, temos $a - b = km$;

   Note que $a - b = (a + c) - (b + c)$, assim escrevemos $(a + c) - (b + c) = km$ e isso implica $(a + c) \equiv (b + c)(mod \quad m)$. □

2. $(a - c) \equiv (b - c)(mod \quad m)$

   Demonstração. Note que $(a - c) - (b - c) = a - b$ e ainda $a - b = km$;

   Fazendo;

   $(a - c) - (b - c) = km \Longrightarrow (a - c) \equiv (b - c)(mod \quad m)$. □

3. $ac \equiv bc(mod \quad m)$

   Demonstração. Por hipótese temos $a - b = km$, para algum $k \in \mathbb{Z}$. Como $c \in \mathbb{Z}$, podemos escrever $ac - bc = (ck)m$, o que implica $ac \equiv bc(mod \quad m)$. □

Teorema 1.8. *Se a, b, c, d, m inteiros tais que* $a \equiv b(mod \quad m)$ *e* $c \equiv d(mod \quad m)$*, então;*

1. $(a + c) \equiv (b + d)(mod \quad m)$

   Demonstração. Como $a \equiv b(mod \quad m)$ e $c \equiv d(mod \quad m)$ segue que;

   $a - b = k_1 m$

   $c - d = k_2 m$

   Somando membro a membro, obtemos;

   $(a + c) - (b + d) = (k_1 + k_2)m$

   Portanto,

   $(a + c) \equiv (b + d)(mod \quad m)$. □

2. $(a - c) \equiv (b - d)(mod \quad m)$

Demonstração. Por hipótese temos;

$a - b = k_1 m$

$c - d = k_2 m$

Subtraindo membro a membro, obtemos;

$(a - c) - (b - d) = (k_1 - k_2)m$

Portanto,

$(a - c) \equiv (b - d)(mod \quad m)$. □

Proposição 1.10. *Seja m um inteiro fixo e sejam a, b, c inteiros arbitrários. Se $mdc(c, m) = 1$, então $ac \equiv bc(mod \quad m) \Longrightarrow a \equiv b(mod \quad m)$.*

Demonstração. Se $ac \equiv bc(mod \quad m)$, temos que $m|(a - b)c$;

Como o $mdc(c, m) = 1$, pelo Teorema de Euclides $m|(a-b)$,então $a \equiv b(mod \quad m)$. □

Proposição 1.11. *Considere a, b, k, m inteiros, com $k > 0$ e $a \equiv b(mod \quad m)$, então $a^k \equiv b^k(mod \quad m)$.*

Demonstração. Fazendo uso da seguinte identidade:

$a_k - b_k = (a - b)(a_{k-1} + a_{k-2}b + a_{k-3}b_2 + ... + ab_{k-2} + b_{k-1})$

Como $a \equiv b(mod \quad m)$, então $m|(a - b)$ e para algum $q \in \mathbb{Z}$, temos;

$a - b = mq$

Das duas últimas igualdades concluímos que:

$a^k - b^k = mx$, com $x \in \mathbb{Z}$

Portanto,

$m|(a^k - b^k) \Longrightarrow a^k \equiv b^k(mod \quad m)$. □

Proposição 1.12. *Sejam a, b, c, m inteiros e $ac \equiv bc(mod \quad m)$, então $a \equiv b(mod \quad \frac{m}{d})$, com $mdc(m, c) = d$.*

Demonstração. De $ac \equiv bc(mod \quad m)$, temos que $ac - bc = c(a - b) = km$;

Dividindo membro a membro por d, obtemos;

$\frac{c}{d}(a - b) = \frac{m}{d}k$

Assim,

$\frac{m}{d}|\frac{c}{d}(a - b)$

Note ainda que,

$\left(\frac{m}{d}, \frac{c}{d}\right) = 1$.

Fazendo uso do Teorema de Euclides, temos que;

$\frac{m}{d}(a - b) \Longrightarrow a \equiv b(mod \quad \frac{m}{d})$. □

Definição 1.4. *Se h, k são dois inteiros com $h \equiv k(mod \quad m)$ dizemos que k é um resíduo de h módulo m.*

Definição 1.5. *O conjunto dos inteiros $\{r_1, r_2, ..., r_n\}$ é um sistema completo de resíduos módulo m se:*

1. *r_1 for incongruente a r_j módulo m, para todo $i \neq j$.*

2. *Para todo inteiro k existe um $r_i, i = 1, 2, ..., n$ tal que $k \equiv r_i (mod \quad m)$.*

Observações:

O sistema completo de resíduos mais simples que podemos obter é:

$\{0, 1, 2, ..., m-1\}$

Mas não é o único possível.

Os $r_1, r_2, ..., r_m$ são congruentes módulo m em alguma ordem, aos números;

$\{0, 1, ..., m-1\}$

Exemplo 1.6. *1. Para $m = 5$, $\{0, 1, 2, 3, 4\}$ é o conjunto dos menores restos não negativos módulo 5.*

2. $\{-14, -13, 18, 24, 500\}$ é um sistema completo de resíduo módulo 5.

Teorema 1.9. *Se k inteiros $r_1, r_2, ..., r_k$ formam um sistema completo de resíduos módulo m, então $k = m$.*

Demonstração. Primeiro vamos mostrar que os inteiros $t_0, t_1, ..., t_{m-1}$, com $t_i = i$ sendo $0 \leq i < m - 1$.

Formando de fato um sistema completo de resíduos módulo m.

Sabemos que pela divisão euclidiana, para cada n inteiro, existe um único par de inteiros q e s tal que;

$n = mq + s \Longrightarrow n - s = mq; \quad 0 \leq s < m$

Assim temos $n \equiv s(mod \quad m)$, sendo que $s \in t_i$.

Note que $|t_i - t_j| \leq m - 1, \quad 0 \leq i, j \leq m - 1$. O que implica que t_i é incongruente a t_j módulo m para $i \neq j$.

Pois se $t_i \equiv t_j (mod \quad m) \Longrightarrow m|(t_i - t_j)$. O que acarretaria $t_i - t_j = mk$, para algum k inteiro.

Assim,

$|t_i - t_j| > m$ e isso não acontece.

De fato, t_i é incongruente t_j módulo m, com $i \neq j$.

Portanto, o conjunto $\{t_0, t_1, ..., t_{m-1}\}$ é um sistema completo de resíduos módulo m. Com isso, cada r_i é congruente a exatamente um dos t_i, isso nos garante que,

$k < m - 1 \Longrightarrow k \leq m$

Como o conjunto $\{r_1, r_2, ..., r_k\}$, por hipótese forma um sistema completo de resíduos módulo m, por definição, cada t_i é congruente a exatamente um dos r_i e isso implica;

$m - 1 < k \Longrightarrow m \leq k$

Portanto,

$k = m$.

□

Teorema 1.10. *Se $r_1, r_2, ..., r_m$ é um sistema completo de resíduos módulo m, a e b são inteiros com $mdc(a, m) = 1$, então;*

$ar_1 + b, \quad ar_2 + b, ..., ar_m + b$

Também é um sistema completo de resíduos módulo m.

Demonstração. Fazendo uso do teorema anterior.

Agora vamos mostrar que quaisquer dois inteiros do conjunto;

$ar_1 + b, \quad ar_2 + b, ..., ar_m + b$

São incongruentes módulo m.

Suponhamos que $(ar_i + b) \equiv (ar_j + b)(mod \quad m)$, fazendo uso de propriedades de congruência, temos;

$ar_i \equiv ar_j(mod \quad m)$

Mas como $mdc(a, m) = 1$, temos;

$r_i \equiv r_j(mod \quad m)$

Implicando em $i = j$ (absurdo), pois o conjunto $\{r_1, r_2, ..., r_m\}$ é sistema completo de resíduo. Logo;

$ar_i + b \equiv ar_j + b(mod \quad m)$ para $i \neq j$.

Portanto, o conjunto $ar_1 + b, \quad ar_2 + b, ..., ar_m + b$ é sistema completo de resíduo. □

A congruência módulo m permite a identificação de todos os números que deixam o mesmo resto quando divididos por m. Isso nos permite a criação de outros sistemas numéricos. Apresentaremos em seguida um exemplo que ilustra bem as potencialidades desta ferramenta.

Exemplo 1.7. *Encontrar o resto* 6^{2009} *quando dividido por* 37.

Solução: Veja que $6^2 = 36 \equiv (mod \quad 37)$ e assim $6^{2009} = 6(6^2)^{1004} \equiv 6(-1)^{1004} = 6(mod \quad 37)$.

Dessa forma, o resto da divisão é 6, pois $6^{2009} - 6$ é múltiplo de 37.

1.6 Congruência Linear

Chama-se de congruência linear em uma variável uma congruência da forma,

$ax \equiv b(mod \quad m)$, onde x é uma incógnita.

Se x_0 é uma solução de $ax \equiv b(mod \quad m)$ e $x_1 \equiv x_0(mod \quad m)$, então x_1 é também solução. De fato, pois se $x_1 \equiv x_0(mod \quad m)$, então $ax_1 \equiv ax_0 \equiv a_x \equiv b(mod \quad m)$. Note que se um membro da classe de equivalência é solução então todo membro também é. Se x_0 é uma solução da congruência linear $ax \equiv b(mod \quad m)$, então todos os inteiros $x_0 + km$, onde k é um inteiro arbitrário, também são soluções da congruência linear. Note que pela definição de congruência $ax_0 \equiv b(mod \quad m)$ se e somente se, o n divide $ax_0 - b$. Assim, existe um inteiro y tal que $ax_0 - b = my$. (Desse modo, o problema de encontrar todas as soluções de uma congruência linear é idêntico ao de obter todas as soluções da equação diofantina $ax_0 - my = b$).

Duas soluções x_0 e x_1 da congruência $ax \equiv b(mod \quad m)$ congruente módulo m, isto é, $x_0 \equiv x_1(mod \quad m)$ não são consideradas soluções distintas. O número de soluções da congruência é dado pelo número de soluções mutuamente incongruente módulo m,

ou seja, quando falamos do número de soluções da congruência linear $ax \equiv b(mod \quad m)$ estamos contando somente aquelas que são incongruente módulo m. Por exemplo, $x = 2$ e $x = 7$ satisfazem a congruência linear $4x \equiv 3(mod \quad 5)$. Como $2 \equiv 7(mod \quad 5)$, tratamos 2 e 7 como a mesma solução da congruência linear $4x \equiv 3(mod \quad 5)$.

Definição 1.6. *Dizemos que uma solução x_0 de $ax \equiv b(mod \quad m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

Teorema 1.11. *Sejam a, b inteiros positivos e $mdc(a, b) = d$. Se d não divide c, então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por;*

$x = x_0 + \left(\frac{b}{d}\right) k$

$y = y_0 - \left(\frac{a}{d}\right) k$;

Onde k é um inteiro.

Demonstração. Se d não divide c, então a equação $ax + by = c$ não possui solução, pois como o $mdc(a, b) = d$ implica que $d|a$ e $d|b$. Assim d deveria dividir c, já que c está escrito como combinação linear de a e b.

Suponha que $d|c$ pelo Teorema 3 (Bezout) existem inteiros n_0 e m_0 tais que;

$an_0 + bm_0 = d$

De $d|c$ existe um inteiro k tal que $c = kd$. Multiplicando ambos os membros da igualdade acima por k, obtemos;

$a(n_0k) + b(m_0k) = kd = c$

Assim, o par (x_0, y_0), sendo $x_0 = n_0k$ e $y_0 = m_0d$ é uma solução de $ax + by = c$. Note que é fácil verificar que os pares da solução da equação $ax + by = c$ é da forma;

$x = x_0 + \left(\frac{b}{d}\right) k$

$y = y_0 - \left(\frac{a}{d}\right) k$

Veja que

$ax + by = a(x_0 + \left(\frac{b}{d}\right) k) + b(y_0 - \left(\frac{a}{d}\right) k) = ax_0 + \left(\frac{ab}{d}\right) k + by_0 - \left(\frac{ab}{d}\right) k = ax_0 + by_0$

Note que acabamos de mostrar que a partir de uma solução particular (x_0, y_0), podemos gerar infinitas soluções.

Agora só basta mostrar que toda solução da equação $ax + by = c$ é da forma

$x = x_0 + \left(\frac{b}{d}\right) k$

$x = y_0 - \left(\frac{a}{d}\right) k$

Vamos supor que (x, y) é a solução de $ax + by = c$ e ainda (x_0, y_0) é uma solução particular $ax_0 + by_0 = c$.

Subtraindo as duas últimas igualdades, temos;

$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0$

O que implica em $a(x - x_0) = b(y - y_0)$. Como o $mdc(a, b) = d$ podemos escrever que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Dividindo a igualdade acima acima por d.

$\frac{a}{d}(x - x_0) = \frac{b}{d}(y - y_0) \Longrightarrow \frac{b}{d}|\frac{a}{d}(x - x_0)$

Usando o Teorema de Euclides $\frac{b}{d}|(x - x_0)$, portanto existe um k inteiro tal que;

$x - x_0 = k\frac{b}{d} \Longrightarrow x = x_0 + \frac{b}{d}k$

Substituindo x na equação acima, obtemos;

$y = y_0 - \frac{b}{d}k$.

□

Teorema 1.12. *A congruência linear* $ax \equiv b(mod \quad m)$ *tem solução se, e somente se,* d *divide* b*, sendo* $d = mdc(a, m)$*.*

Demonstração. ($\Longrightarrow$) Por hipótese temos $ax \equiv b(mod \quad m)$, assim $m|(ax - b)$

$ax - b = mk$, sendo $k \in \mathbb{Z}$

$-b = mk - ax$

$b = ax - mk$ (1)

Como o $mdc(a, m) = d$, então $d|a$ e $d|m$. Assim, existem $p, q \in \mathbb{Z}$ tais que;

$a = dpm = dq$

Substituindo as duas últimas equações na expressão (1), obtemos;

$b = ax - mk$

$b = (dp)x - (dq)k$

$b = d(px - kq)$

$b = d(r)$ tal que $r \in \mathbb{Z}$. Dessa forma, $d|b$.

($\Longleftarrow$) Sabemos que uma equação da forma $ax + by = c$, onde a, b, c são inteiros é chamada de equação diofantina linear. Se x é solução de congruência $ax \equiv b(mod \quad m)$, existe $y \in \mathbb{Z}$ tal que o par (x, y) é solução da equação diofantina $ax + by = c$. Isso nos leva a dizer que a congruência linear $ax \equiv b(mod \quad m)$ é equivalente a equação diofantina $ax - my = b$.

Por hipótese temos $d|b$, assim o Teorema 11 nos garante que a equação diofantina $ax - my = b$ possui infinitas soluções. Assim, existem $x_0, y_0 \in \mathbb{Z}$ tais que;

$ax_0 - my_0 = b$

$my_0 = ax_0 - b$

$m|(ax_0 - b)$

Por definição de congruência obtemos $ax_0 \equiv b(mod \quad m)$, sendo x_0 solução da congruência.

□

Teorema 1.13. *Sejam* a, b, m *inteiros tais que* $m > 0$ *e* $mdc(a, m) = d$*. No caso em que* d *não divide* b *a congruência* $ax \equiv b(mod \quad m)$ *não possui nenhuma solução e quando* $d|b$ *possui exatamente* d *solução incongruente módulo* m*.*

Demonstração. Sabemos que o inteiro x é solução de $ax \equiv b(mod \quad m)$ se, e somente se existe um inteiro y tal que $ax = b + my$, ou seja, $ax - my = b$. Sabemos que de acordo com o teorema 11, esta equação não possui nenhuma solução caso d não divide b e se $d|b$, então a dita equação possui infinitas soluções dadas por;

$x = x_0 - \left(\frac{m}{d}\right)k$

$y = y_0 - \left(\frac{a}{d}\right)k$

Onde (x_0, y_0) é uma solução particular de $ax - my = b$

Assim a congruência $ax \equiv b(mod \quad m)$ possui infinitas soluções dadas por; $x = x_0 - \left(\frac{m}{d}\right) k$

Estamos interessados em saber o número de soluções incongruentes. Tome x_1, x_2 soluções congruentes módulo m. Então $x_0 - \left(\frac{m}{d}\right) k_1 \equiv x_0 - \left(\frac{m}{d}\right) k_2(mod \quad m)$.

O que implica $\left(\frac{m}{d}\right) k_1 \equiv \left(\frac{m}{d}\right) k_2(mod \quad m)$. E como $\left(\frac{m}{d}\right) | m$ e $mdc\left(\frac{m}{d}, m\right) = \frac{m}{d}$, temos que pela proposição 11, o cancelamento é permitido.

$k_1 \equiv k_2(mod \quad m)$

Observação: O m foi substituído por $d = m|\frac{m}{d}$.

Assim, concluimos que as soluções incongruentes serão obtidas ao tomarmos $x = x_0 - \left(\frac{m}{d}\right) k$, onde k percorre um sistema completo de resíduos módulo d.

□

Teorema 1.14. *Se o $mdc(a, m) = 1$, então a congruência linear $ax \equiv b(mod \quad m)$ tem exatamente uma solução incongruente.*

Demonstração. Seja C um sistema completo de resíduos módulo m. Pelo Teorema 10 o conjunto $(ax; x \in \mathbb{C})$ é também um sistema completo de resíduos módulo m. Por definição existe um único elemento $x_0 \in \mathbb{C}$ tal que ax_0 é congruente a um inteiro dado b módulo m, ou seja, $ax_0 \equiv b(mod \quad m)$. Portanto, a congruência linear $ax \equiv b(mod \quad m)$, onde $mdc(a, m) = 1$, tem exatamente uma solução incongruente, a saber, $x \equiv x_0(mod \quad m)$.

□

Teorema 1.15. *Se $ac \equiv bc(mod \quad m)$ e $mdc(c, m) = d$, então $a \equiv b(mod \quad \frac{m}{d})$.*

Demonstração. Se $ac \equiv bc(mod \quad m)$, então $m|(ac - bc)$; isto é, $m|c(a - b)$. Como o $mdc(c, m) = d$, então $c = dc'$ e $m = dm'$. Assim, temos;

$dm'|dc'(a - b)m'|c'(a - b)$, onde $mdc(c'm') = 1$. Portanto, $m'|(a - b)$.

E daí, $a \equiv b(mod \quad m')$;

Isto é, $a \equiv b(mod \quad \frac{m}{d})$.

□

Exemplo 1.8. *Resolver a congruência linear $36x \equiv 53(mod \quad 131)$.*

Solução: Como o $mdc(36, 131) = 1$, pelo Teorema 14, a congruência linear tem exatamente uma solução incongruente. Como $53 \equiv -78(mod \quad 131)$, pela transitividade de relação de congruência,

$36x \equiv -78(mod \quad 131)$

Pela proposição 11;

$6x \equiv -13(mod \quad 131)$

Usando a propriedade transitiva e simétrica da relação de congruência e o fato de que;

$-144 \equiv -13(mod \quad 131)$

Obtemos;

$6x \equiv -144(mod \quad 131)$

Outra vez, pela proposição 11,

$x \equiv -24(mod \quad 131)$
$x \equiv 107(mod \quad 131)$.

CAPÍTULO 2

EQUAÇÕES DIOFANTINAS LINEARES

Uma **equação diofantina linear** em duas variáveis é uma expressão da forma $ax + by = c$, na qual a, b, c são inteiros, com a e b não simultaneamente nulos e cujas soluções estão restritas ao conjunto dos números inteiros. Uma solução dessa equação é então um par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = c$.

A resolução de muitos problemas de aritmética depende da resolução de equação do tipo $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$. É claro que se $a = 0$ ou $b = 0$, a equação tem resolução imediata.

Por exemplo, se $a = 0$ e $b \neq 0$, então existe solução inteira e $a|c$ e, neste caso a solução geral é dada por $x \in \mathbb{Z}$ e $x = \frac{c}{a}$.

Mas, antes de procurar uma solução para a equação diofantina, é conveniente saber se essa existe. Por isso, desenvolvemos aqui resultados que possibilitem a nós respondermos as seguintes perguntas;

- Quais são as condições para que essa equação possua solução?
- Quantas são as soluções?
- Como calcular as soluções, caso existam?

O resultado a seguir dá a condição necessária e suficiente para a existência de soluções de uma dada equação diofantina linear. Dada uma equação diofantina do primeiro grau de duas incógnitas x, y tais que, $ax+by = c$, onde a, b e $c \in \mathbb{Z}$. Afim de obter a solução de tais equações determinarão todos os pares ordenados $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Indicaremos por A o conjunto de todos os pares ordenados $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ tais que $ax_0+by_0 = c$. Assim, todo elemento de A é chamado de **Solução Inteira** da equação diofantina. Sempre iremos supor que a, b não sejam simultaneamente nulos, pois se $a = b = 0$ a equação diofantina $ax+by = c$ tem solução se, e somente se, $c = 0$ e, neste caso, $A = \mathbb{Z} \times \mathbb{Z}$. Apresentaremos agora uma condição para que o conjunto-solução A não seja vazio, isto é, que a equação diofantina admita solução.

2.1 Condição de Existência de Solução

Teorema 1.16. *A equação diofantina linear $a.x + b.y = c$ possui solução inteira se, e somente se, $mdc(a, b)|c$.*

Demonstração. ($\Longrightarrow$) Suponhamos que (x_0, y_0) seja uma solução da equação, isto é;

$ax_0 + by_0 = c$.

Seja o $mdc(a, b) = d$ por definição de máximo divisor comum, temos que $d|a$ e $d|b$, então d divide qualquer combinação linear formada pelos inteiros a e b. Portanto, $d|(ax_0 + by_0) = c$.

($\Longleftarrow$) Seja $mdc(a, b) = d$. Se $d|c$, então $c = dm$ para algum inteiro m. Além disso, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = d$.

Logo, $a(x_0m) + b(y_0m) = dm = c$ e, portanto, (mx_0, my_0) é uma solução da equação. □

Observação 1:

No caso em que $mdc(a, b) = d$ e $d|c$, a equação diofantina linear $ax + by = c$ admite um número infinito de soluções.

Observação 2:

Na Geometria Analítica, a equação $ax + by = c$ representa uma reta r. Ao procurarmos soluções em $\mathbb{Z}$ da equação $ax + by = c$, estamos perguntando se a reta r, por ela representada, contém pontos que tenham ambas as coordenadas inteiras. O Teorema 1.15 nos diz que existem equações dessa forma sem soluções inteiras, por exemplo, a equação $12x + 8y = 7$ não tem soluções inteiras, já que o $mdc(12, 8) = 4$ que não divide 7. Fica, então, provado o fato surpreendente que a reta r de equação $12x+8y = 7$ consegue evitar todos os pontos do plano cartesiano tal que o par (x, y) tenha coordenadas inteiras.

2.2 Soluções da Equação $ax + by = c$

Seja (x_0, y_0) uma solução particular da equação diofantina linear $ax+by = c$, em que $a, b \neq 0$. Então qualquer solução inteira dessa equação é dada por;

$x = x_0 + \frac{b}{d}k$

$y = y_0 - \frac{a}{d}k$

Onde $mdc(a, b) = d$ e k é um inteiro qualquer.

Demonstração. Consideremos a equação diofantina;

$ax + by = c$, com $ab \neq 0$

Primeiro vamos mostrar que se (x_0, y_0) é solução particular da equação, então o par $(x_0 + \frac{b}{d}k, \quad y_0 - \frac{a}{d}k)$ é também solução para qualquer inteiro k.

De fato, como $a = \frac{a}{d}d$ e $b = \frac{b}{d}d$;

Fazendo:

$a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) = ax_0 + a\frac{b}{d}k + by_0 - \frac{a}{d}k = ax_0 + by_0 = c$.

Portanto, $(x_0 + \frac{b}{d}k, \quad y_0 - \frac{a}{d}k)$ é também solução da equação diofantina dada. Agora vamos mostrar que se (x, y) é solução da equação diofantina:

$$ax + by = c, \text{ com } a, b \neq 0;$$

Então existe um inteiro k tal que

$$x = x_0 + \frac{b}{d}k$$
$$y = y_0 - \frac{a}{d}k$$

é a solução geral.

Note que vale se (x_0, y_0) e (x, y) são soluções da equação, então temos;

$ax + by = ax_0 + by_0 \Longrightarrow a(x - x_0) = b(y_0 - y) \Longrightarrow \frac{a}{d}d(x - x_0) = \frac{b}{d}d(y_0 - y)$

$\Longrightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$.

Veja que $\frac{b}{d}$ divide o lado direito da igualdade e também o lado esquerdo. E ainda $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, pois o $mdc(a, b) = d$. Assim, pelo Teorema de Euclides $\frac{b}{d}|(x - x_0)$. Logo, existe um inteiro k tal que;

$x - x_0 = \frac{b}{d}k \Longrightarrow x = x_0 + \frac{b}{d}k$

Tomando x e substituindo na igualdade acima, obtemos y;

$\frac{a}{d}(x_0 - (x_0 + \frac{b}{d}k) = \frac{b}{d}(y_0 - y)$

$\frac{a}{d}\frac{b}{d}k = \frac{b}{d}(y_0 - y)$

$\frac{a}{d}k = y_0 - y$

$y = y_0 - \frac{a}{d}k$. □

Proposição 1.13. *Se (x_0, y_0) é solução da equação diofantina linear $ax + by = c$, então o par $(x_0 + bt, y_0 - at)$ também é solução dessa equação, para qualquer inteiro t.*

Demonstração. Como (x_0, y_0) é solução da equação $ax + by = c$, temos que $ax_0 + by_0 = c$. Assim, para qualquer inteiro t, vale:

$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - abt = ax_0 + by_0 = c$

(note que somamos e subtraímos o inteiro abt)

O que implica em $(x_0 + bt, y_0 - at)$ também ser uma solução da equação. □

Demonstração. Considere $d = mdc(a, b) = 1$, caso contrário divida a equação por "d" e saberemos que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Sendo $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ solução, temos;

$ax + by = c = ax_0 + by_0$

$ax - ax_0 = by_0 - by$

$a(x - x_0) = b(y_0 - y)$

Daí $a|b(y_0 - y)$, mas a não divide b, logo $a|(y_0 - y)$, temos $y_0 - y = at$ implicando em $y = y_0 - at$, com $t \in \mathbb{Z}$.

Analogamente, $b|a(x - x_0)$ e b não divide a, temos então $b|(x - x_0)$ o que resulta em $x - x_0 = bt$ e ainda $x - x_0 = bt$

□

Corolário 1.2. *Se $mdc(a, b) = 1$, e se a, b são relativamente primos, então a equação $ax + by = c$ sempre tem soluções inteiras para qualquer que seja c.*

Demonstração. Resolver a equação diofantina linear $ax + by = c$, com a, b e c inteiros e $mdc(a, b) = 1$, equivale encontrar inteiros r e s tais que $ar + bs = 1$. Para isso, vamos fazer o uso do algoritmo de Euclides.

Sejam a, b inteiros com $b > 0$. Pelo algoritmo da divisão, existem q e r com $0 \leq r < b$, únicos tais que $a = bq + r$. Se p é divisor comum de a, b, então $p|a$ e $p|b$. Como $p|b$, implica que $p|bq$.

Fazendo-se $a - bq = r$, como $p|a$ e $p|bq$, logo $p|c$. Assim p é divisor comum também de b, r, isto é, $mdc(a, b) = mdc(b, r)$. Reciprocamente se $p|b$ e $p|r$, como $a = bq + r$, então $p|a$. Portanto, o $mdc(a, b) = mdc(b, r)$. Assim, concluímos que existem, de fato, r e s inteiros tais que $ar + bs = 1$.

Para efeito de encontrar soluções inteiras, apenas o caso em que o $mdc(a, b) = 1$ nos interessa. Pois se a equação possui solução e o máximo divisor comum for diferente de 1, isto é, $(d \neq 1)$ basta dividir ambos os membros da equação por d, assim nos deparamos no caso de coeficientes a e b relativamente primos, e com o segundo membro ainda um número inteiro.

Na busca de soluções inteiras de uma equação diofantina no primeiro grau, a saber, $ax + by = n$, vimos que podemos tomar o $mdc(a, b) = 1$ e assim descobrir uma solução inteira dessa equação equivale a encontrar inteiros r e s tais que $ar + bs = 1$. Para determinar uma solução particular em que a e b são números relativamente pequenos procede-se por inspeção. Se não for possível esse método, para encontrarmos os números r e s utilizamos o algoritmo de Euclides para cálculo do $mdc(a, b) = d$. Com a aplicação desse algoritmo, obtemos inteiros m_0 e n_0 tais que $am_0 + bn_0 = mdc(a, b) = d$. Multiplicando-se em ambos os lados dessa igualdade, obtém-se:

$\left(\frac{n}{d}m_0a\right) + \left(\frac{n}{d}n_0b\right) = \left(\frac{n}{d}d\right) \Longrightarrow \left(\frac{n}{d}m_0\right)a + \left(\frac{n}{d}n_0\right)b = n$

Portanto, o par ordenado dado por $x_0 = \left(\frac{n}{d}m_0\right)$ e $y_0 = \left(\frac{n}{d}n_0\right)$ é a solução particular da equação. □

Satisfeita a condição de existência de solução para uma equação diofantina linear, para descobrir as soluções gerais deve-se inicialmente obter uma solução particular da mesma. E a partir dela encontrar todas as soluções da equação. Mas para isso fazemos uso do algoritmo de Euclides. Usualmente, o algoritmo para dividir dois números inteiros é dado por:

a	b
r	q

Figura 1.6: Esquema de divisão usual
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

Na forma do algoritmo de Euclides, fica;

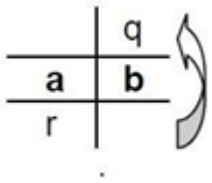

Figura 1.7: Esquema de divisão de Euclides
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

Generalizando, obtemos:

	q_1	q_2	q_3	...	...	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	r_n
$b.q_1$	$r_1.q_2$	$r_2.q_3$	...	...	$q_n.\ r_{n-1}$	$q_{n+1}.\ r_n$	
$r_1 = a - b.q_1$	$r_2 = b - r_1.q_2$	$r_3 = r_1 - r_2.q_3$	...	...	$r_n = r_{n-2} - q_n.\ r_{n-1}$	$r_{n-1} - q_{n+1}.\ r_n = 0$	

Figura 1.8: Generalização do algoritmo de Euclides
Fonte: MILIES, Francisco César Polcino. **Uma Introdução à Matemática**

2.3 Resolução de equações diofantinas por congruência linear

A teoria das congruências lineares pode ser usada como uma forma de obter as soluções de uma equação diofantina linear caso elas existam. Uma solução de uma equação diofantina linear é par de inteiros (x_0, y_0) que satisfaz a equação $ax_0 + by_0 = c$, onde $ax_0 - c = -by_0$. O que implica na congruência $ax_0 \equiv b(mod \quad m)$.

Determinaremos agora uma solução qualquer $x = x_0$ da congruência $ax \equiv c(mod \quad m)$, depois substituímos x_0 na equação $ax + by = c$ afim de encontrar o valor correspondente y_0 tal que $ax_0 + by_0 = c$. Apresentaremos agora um exemplo de resolução de Equações Diofantinas utilizando congruência linear.

Exemplo 1.9. *Determine a solução geral diofantina* $12x + 25y = 331$ *por congruência linear.*

Solução: Como o $mdc(12, 25) = 1$ e $1|331$, então a equação diofantina possui solução.
$12x - 331 = 25(-y)$
Daí;
$12x \equiv 331(mod \quad 25) \Longrightarrow 331 \equiv 12.13(mod \quad 25) \Longrightarrow 12x \equiv 12.13(mod \quad 25)$
Por fim;
$x \equiv 13(mod \quad 25)$

Assim, $x_0 = 13$ é uma solução particular da equação diofantina linear. Substituindo este valor na equação, obtemos $y_0 = 7$.

A solução geral é:

$x = 13 + 25t$

$y = 7 - 12t$

Com $t \in \mathbb{Z}$.

CAPÍTULO 3

APLICAÇÕES

Neste capítulo, abordaremos a aplicação do estudo de equação diofantina em busca de soluções de problemas aritméticos.

3.1 Situações-Problema

Problema 1:

Uma certa empresa, paga para cada funcionário R$ 600,00 em tíquetes de alimentação, com valores de R$ 60,00 e R$ 120,00 cada tíquete. De quantas formas pode ser organizado o carnê de tíquetes de um funcionário?

Solução:

Se denotarmos a quantidade de tíquetes de R$ 60,00 por x e R$ 120,00 por y, modelando o problema, temos;

$60x + 120y = 600$, onde o $mdc(60, 120) = 60|600$

Portanto, pelo teorema 1.15 a equação possui solução.

Utilizando o corolário 1.1 e dividindo a equação por 60, temos a equivalência;

$x + 2y = 10$

Onde o $mdc(1, 2) = 1|10$

Pelo Teorema 1.3, podemos escrever 1 como combinação linear de 1 e 2.

$x_0 + 2y_0 = 1$

Daí, temos;

$1(-1) + 2 = 1$

Multiplicando a equação por 10, temos;

$1(-10) + 2(10) = 10$

Logo, temos as soluções particulares;

$x_0 = -10$ e $y_0 = 10$

Assim, as soluções são dadas pela fórmula;

$x = x_0 + \frac{b}{d}k$

$y = y_0 - \frac{a}{d}k$

Onde $d = mdc(a, b)$, e $k \in \mathbb{Z}$

Como o $mdc(1, 2) = 1$, então a solução fica;

$x = -10 + 2k$

$y = 10 - k$, $k \in \mathbb{Z}$

Como o problema busca apenas as soluções não negativas, deve ser satisfeitas as desigualdades:

$x \geq 0$ e $y \geq 0$

Assim,

$-10 + 2k \geq 0$ e $10 - k \geq 0 \Longrightarrow k \geq 5$ e $k \leq 10$, $k \in \mathbb{Z}$

Para $\{k \in \mathbb{Z}; 5 \leq k \leq 10\}$, temos 6 possibilidades de organizar o carnê:

Para $k = 5$, temos um carnê com 0 tíquetes de R$ 60,00 e 5 tíquetes de R$120,00.

Para $k = 6$, temos um carnê com 2 tíquetes de R$ 60,00 e 4 tíquetes de R$120,00.

Para $k = 7$, temos um carnê com 4 tíquetes de R$ 60,00 e 3 tíquetes de R$120,00.

Para $k = 8$, temos um carnê com 6 tíquetes de R$ 60,00 e 2 tíquetes de R$120,00.

Para $k = 9$, temos um carnê com 8 tíquetes de R$ 60,00 e 1 tíquetes de R$120,00.

Para $k = 10$, temos um carnê com 10 tíquetes de R$ 60,00 e 0 tíquetes de R$120,00.

Problema 2:

O cinema do Amapá Garden Shopping disponibiliza nas quartas-feiras ingressos com valores de R$ 10,00 pela manhã e R$ 12, 00 pela tarde. De quantas maneiras podem ser vendidos os ingressos para que se tenha um saldo de R$ 200,00 ao final do dia?

Solução:

Se representarmos o número de ingressos da manhã por x e da tarde por y, modelando a equação, temos;

$10x + 12y = 200$, onde $mdc(10, 12) = 2|200$

Utilizando o corolário 1.1 e dividindo a equação por 2, temos a equivalência;

$5x + 6y = 100$

Onde $mdc(6, 5) = 1$

Pelo teorema 1.3 podemos escrever 1 como combinação linear de 5 e 6

$\Longrightarrow 5x_0 + 6y_0 = 1$

Daí basta observar que;

$5(-1) + 6 = 1$

Multiplicando a eq. por 100, temos;

$5(-100) + 6(100) = 100$

Logo, temos as soluções particulares $x_0 = -100$ e $y_0 = 100$

Assim, as soluções são dadas pela fórmula;

$x = -100 + 6k$

$y = 100 - 5k$, $k \in \mathbb{Z}$

Como o problema busca apenas as soluções não negativas, deve ser satisfeitas as desigualdades:

$x \geq 0$ e $y \geq 0$

Assim,

$-100 + 6k \geq 0$ e $100 - 5k \geq 0 \Longrightarrow k \geq 17$ e $k \leq 20$, $k \in \mathbb{Z}$

Para $\{k \in \mathbb{Z}; 17 \leq k \leq 20\}$, temos 4 possibilidades de vendas:

Para $k = 17$, temos pela manhã 2 ingressos de R$ 10,00 e pela tarde 15 ingessos de R$12,00.

Para $k = 18$, temos pela manhã 8 ingressos de R$ 10,00 e pela tarde 10 ingessos de R$12,00.

Para $k = 19$, temos pela manhã 14 ingressos de R$ 10,00 e pela tarde 5 ingessos de R$12,00.

Para $k = 20$, temos pela manhã 20 ingressos de R$ 10,00 e pela tarde 0 ingessos de R$12,00.

Problema 3:

Edson é fã de música, reserva por mês R$ 120,00 para comprar CD's e DVD's. Em média, um CD custa R$ 10,00 e um DVD R$ 15,00. Quais as possibilidades de aquisição dos itens, gastando exatamente R$ 120,00?

Solução:

Representando o número de CD's por x e de DVD's por y, temos a equação $10x+12y = 120$, onde o $mdc(10, 12) = 2|120$.

Utilizando o corolário 1.1 e dividindo a equação por 2, temos a equivalência;

$5x + 6y = 60$, onde $mdc(5, 6) = 1|60$.

Pelo Teorema 1.3, podemos escrever 1 como combinação linear de 5 e 6, implica que $5x_0 + 6y_0 = 1$.

Basta observar que;

$5(-1) + 6 = 1$

Multiplicando por 60, temos;

$5(-60) + 6(60) = 60$

Logo temos as soluções particulares $x_0 = -60$ e $y_0 = 60$

Assim, o conjunto das soluções inteiras é dada pela fórmula;

$x = -60 + 6k$

$y = 60 - 5k$, $\in \mathbb{Z}$

Como o problema busca as soluções inteiras não negativas, deve ser satisfeita as desigualdades $x \geq 0$ e $y \geq 0$.

Assim;

$-60 + 6k \geq 0 \Longrightarrow k \geq 10$ e $60 - 5k \geq 0 \Longrightarrow k \leq 12$.

Para $\{k \in \mathbb{Z}; 10 \leq k \leq 12\}$, temos 3 possibilidades de aquisição para;

$k = 10$, temos 0 CD's e 10 DVD's.

$k = 11$, temos 6 CD's e 5 DVD's.

$k = 12$, temos 12 CD's e 0 DVD's.

Problema 4:

Um fazendeiro deseja comprar filhotes de pato e de galinha, gastando um total de R$ 1770,00. Um filhote de pato custa R$ 31,00 e um de galinha custa R$ 21,00. Quantos de

cada um dos dois tipos o fazendeiro poderá comprar?

Solução:

Se representarmos os filhotes de pato por x e os de galinhas por y, modelando o problema, temos;

$31x + 21y = 1770$, onde $mdc(21, 31) = 1|1770$.

Pelo Teorema 1.3 podemos escrever 1 como combinação linear de 31 e 21, isso implica em $31x_0 + 21y_0 = 1$.

Usando o algoritmo de Euclides:

	1	2	10
31	21	10	1
	10	1	0

Figura 1.9: $mdc(31, 21)$

Logo temos que;

$31 = 21 + 10$

$21 = 2(10) + 1$

Daí;

$10 = 31 - 21$ e $1 = 21 - 10(2) \Longrightarrow 1 = 21 + 10(-2)$

Logo,

$1 = 21 + (31 - 21)(-2) \Longrightarrow 1 = 21 + 31(-2) + 21(2) \Longrightarrow 1 = 31(-2) + 21(3)$

Multplicando a eq. por 1770, temos;

$31(-3540) + 21(5310) = 1770$.

Logo, temos as soluções particulares;

$x_0 = -3540$ e $y_0 = 5310$.

Assim, o conjunto das soluções inteiras é dada pela fórmula;

$x = x_0 + \frac{b}{d}k$

$x = y_0 + \frac{a}{b}k$

$\Longrightarrow x = -3540 + 21k$

$y = -3540 - 31k, k \in \mathbb{Z}$.

Como o problema busca apenas as soluções inteiras, precisamos que as desigualdades sejam satisfeitas:

$x \geq 0$ e $y \geq 0$

$\Longrightarrow -3540 + 21k \geq 0 \Longrightarrow k \geq 169$ e $5310 - 31k \geq 0 \Longrightarrow k \leq 171$.

Para $\{k \in \mathbb{Z}; 169 \leq k \leq 171\}$

Temos 3 possibilidades de compra;

Para,

$k = 169$, temos 9 patos e 71 galinhas.

$k = 170$, temos 30 patos e 40 galinhas.
$k = 171$, temos 51 patos e 9 galinhas.

3.2 Problemas Propostos

1. Em um evento beneficente, foram vendidos R$ 720,00 em ingressos. Sabendo que o valor do ingresso para homens custava R$ 15,00 e para mulheres R$ 8,00, quantos homens e quantas mulheres participaram do evento?

2. Cristhian comprou um número ímpar de canetas e algumas borrachas, gastando R$ 37,40. Sabendo-se que os preços unitários das canetas e das borrachas são, respectivamente, R$ 1,70 e R$ 0,90, determine quantas canetas e quantas borrachas ele comprou.

3. Dois irmãos, Bruce e Mauro, arrecadaram R$ 61,00 na venda de peixes. Sabendo que Bruce cobrou R$ 10,00 por peixe e Mauro cobrou R$ 7,00. Determine as possíveis quantidades que cada um vendeu?

4. Um agricultor deve fazer uma plantação de eucaliptos e pinus. Cada muda de eucalipto custa R$ 0,30 e cada muda de pinus custa R$ 0,40. Sabendo que o agricultor dispõe de R$ 3500,00 para compra mudas e que irá plantar no mínimo 1000 mudas de cada espécie, qual é o número máximo e o número mínimo de mudas que se pode comprar?

5. 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?

4 CONSIDERAÇÕES FINAIS

Nesse trabalho, buscou-se o favorecimento de entendimento ao leitor sobre um principio histórico, conceitual e prático do conteúdo de Equações Diofantinas Lineares e suas aplicações.

É viável reparar que Diofanto de Alexandria teve uma contribuição muito grande para a história da matemática, contribuindo para a abertura de novos horizontes, principalmente a álgebra, pois o mesmo foi precursor no desenvolvimento da notação algébrica, em que algumas operações eram representadas por suas abreviações. Independentemente de não ter sido o primeiro a ocupar-se com equações indeterminadas ou solucionar equações quadráticas de forma não geométrica é possível considerar que Diofanto foi precedente a iniciar os passos em direção a uma estrutura da simbologia algébrica que estudamos nos dias de hoje.

Percebe-se que a estratégia algébrica usada para a resolução de problemas compostos neste trabalho, encoraja o leitor a analisar o processo de aprendizagem do conteúdo algébrico e refinar seus conhecimentos.

Espera-se que este trabalho tenha uma grande contribuição para o leitor na absorção de conhecimentos e na resolução de problemas em Teoria dos Números, mais precisamente em equações diofantinas lineares.

REFERÊNCIAS

[1] BOYER, Carl B. **História da matemática**, Uta C. Merzbach; [tradução de Helena Castro]. São Paulo: Blucher, 2012.

[2] OLIVEIRA, José Plinio. **Introdução à Teoria dos Números**. Coleção Matemática Universitária. 1998. Campinas-SP.

[3] MILIES, Francisco César Polcino. **Uma Introdução à Matemática** / Francisco César Polcino Milies, Sônia Pitta Coelho.- 3 ed.2. reimpr.- São Paulo: Editora da Universidade de São Paulo, 2006. - (Acadêmica; 20)

[4] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro** - Projeto Euclides, IMPA, 2010.

[5] BISPO, Dinguiston S. **Equação Diofantina Linear e suas Aplicações**. - Vitória da Conquista-BA / UESB-2013.

[6] FREITAS, Carlos Wagner Almeida. **Equações Diofantinas** / Carlos Wagner Almeida Freitas - 2015.

[7] EVES, Howard. **Introdução à História da Matemática** / Howard Eves, tradução Hygin H. Domingues. 5ª ed. - Campinas, SP: Editora da Unicamp, 2011.

[8] SOUZA, Romário Sindrone de. **Equações Diofantinas Lineares, quadráticas e aplicações** / Romário Sindrone de Souza. - Rio Claro, 2017.