Ricardo Vieira Lima

Equações Diofantinas

São João del-Rei
Dezembro de 2017

Ricardo Vieira Lima

Equações Diofantinas

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Matemática, da Universidade Federal de São João del-Rei, como requisito parcial à obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. Ronaldo Ribeiro Alves

São João del-Rei, 22 de Dezembro de 2017.

Banca Examinadora

Orientador: Prof. Dr. Ronaldo Ribeiro Alves

Prof. Dr. Francinildo Nobre Ferreira

Prof[a]. Ms. Marianna Resende Oliveira

São João del-Rei
Dezembro de 2017

Agradecimentos

Agradeço primeiramente a Deus, que esteve presente em todos os momentos da minha vida.

Aos meus pais, Geraldo e Maria Rosália, por tudo que fizeram por mim.

Aos meus avós que, apesar de não estarem aqui do meu lado, tenho certeza que de algum lugar eles acompanharam o desenvolvimento deste trabalho. Dedico este em memória a minha avó Tunica e meu avô Alderico, que, junto com meus pais, foram os grandes responsáveis por minha formação pessoal.

À minha amada Letícia, pelo companheirismo e pelo apoio principalmente nas horas difíceis.

Ao meu orientador e professor Dr. Ronaldo Ribeiro Alves, pela orientação e confiança.

À professora Dr^{a}. Viviane Cristina Almada, por toda sua dedicação ao curso de Matemática e uma das grandes responsáveis por minha formação como docente.

Aos colegas de turma, por todas as ajudas e os momentos vividos durante a graduação.

Aos professores do DEMAT, pelos ensinamentos durante esses 4 anos.

Resumo

A Aritmética, conhecida também por Teoria Elementar dos Números, é considerada a área mais pura da Matemática e também a mais antiga. Além disso, é atraída não só por pesquisadores da área, mas também por diversas pessoas de várias áreas devido a sua característica instigante, que os leva, a partir da observação de casos particulares, levantar hipóteses relativas às generalizações. Neste trabalho trataremos de conceitos que se encontram dentro da Aritmética. Nele apresentamos um estudo detalhado sobre o máximo divisor comum, dando ênfase em uma das suas mais interessantes aplicações, as equações diofantinas. Abordaremos também um dos algoritmos mais utilizados em situações cotidianas, atribuido a Euclides e conhecido como "Algoritmo de Euclides".

Palavras-chave: *Equações diofantinas, Máximo divisor comum, Algoritmo de Euclides.*

Abstract

Arithmetic, also known as Elementary Theory of Numbers, is considered the purest area of Mathematics and also the oldest. In addition, it is attracted not only by researchers from the area, but also by several people from various areas due to its instigating characteristic, which leads them, from the observation of particular cases, to raise hypotheses regarding generalizations. In this work we will deal with concepts that are found within Arithmetic. In it we present a detailed study on the most common divisor, emphasizing one of its most interesting applications, the Diophantine equations. We will also address one of the most used algorithms in everyday situations, attributed to Euclid and known as "Euclidean Algorithm".

Keywords: *Diophantine Equations, Greatest Common Divisor, Euclidean Algorithm.*

Sumário

Introdução

A Teoria dos Números é considerada a mais pura e antiga dentre todas as outras áreas da Matemática. Dentro dessa, existem outras subáreas que classificamos como Teoria Elementar dos Números (conhecida também como Aritmética), Teoria Algébrica dos Números, Teoria Analítica dos Números e Teoria Geométrica dos Números. Apesar de pertencer à Matemática Pura, a Teoria dos Números desperta o interesse de diversos pesquisadores de outras áreas, devido ao seu caráter instigante que os leva a busca de padrões e generalizações.

Nessa direção, tratamos nesse trabalho apenas alguns entre os diversos tópicos existentes relativos à Aritmética, subárea que estuda as principais operações dos números inteiros. Apresentamos um estudo sobre o máximo divisor comum (mdc), destacando uma de suas aplicações, as equações diofantinas lineares. Estas receberam esse nome em homenagem ao matemático grego, considerado o pai da Álgebra, Diofanto de Alexandria. Mas como são caracterizadas tais equações? Definimos uma equação diofantina linear como uma equação que pode ser escrita da forma

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c,$$

com os coeficientes $a_1, a_2, ..., a_n$ não todos nulos sendo estes números inteiros fixos, $x_1, x_2, ..., x_n$ as variáveis a serem determinadas e c uma constante inteira.

Além do interesse pela Aritmética, um outro fator que nos levou a estudar equações diofantinas foram as aplicações em situações do cotidiano. Elas se mostram presentes em problemas dos mais diferentes tipos, estes envolvendo pessoas, quantias, animais e assim por diante. Dessa forma, dedicaremos um capítulo deste trabalho para mostrar alguns problemas cuja resolução recai na solução de uma equação desse tipo.

Sendo assim, o trabalho é constituído da seguinte forma:

No capítulo 1 destacamos um pouco da vida e obra de Diofanto de Alexandria.

No capítulo 2 tratamos de alguns conceitos preliminares necessários para o desenvolvimento da teoria das equações diofantinas lineares. Neste capítulo abordamos conceitos importantes, como, por exemplo, o algoritmo da divisão, que foi desenvolvido por Euclides e possui inúmeras aplicações práticas.

No próximo capítulo, o capítulo 3, é apresentada a teoria sobre as equações dio-

fantinas lineares. Veremos em quais condições estas equações têm solução. Mostraremos como é o processo de determinação das soluções para o caso de duas e três variáveis e, posteriormente, generalizamos para n variáveis.

Ao fim, no capítulo 4, serão expostos alguns problemas que retratam as aplicações desse tipo de equação.

Capítulo 1

História

Antes de falar das equações diofantinas contaremos um pouco da história do matemático que deu nome a estas equações. Nessa direção, destacamos neste capítulo, um pouco da história de Diofanto, um matemático grego que forneceu grandes contribuições para a Matemática, em especial a Álgebra. Para o desenvolvimento do capítulo utilizamos as referências [2], [3] e [10].

Diofanto de Alexandria

Entre o século II a.C. e o século II d.C a Matemática na Grécia passou por um período de estagnação. A última obra importante na área, desenvolvida anteriormente a esse período, foi a coleção Os Elementos, de Euclides de Alexandria. Segundo [2], entre esses séculos, a Matemática Aplicada se destacou. Áreas como a Astronomia, Geografia, Óptica e Mecânica tiveram desenvolvimentos significativos enquanto a Matemática Pura não apresentou nada relevante.

Eis então que aparece Diofanto de Alexandria para quebrar esse período. Este é considerado o maior algebrista grego. Há poucos registros sobre sua vida e obras, porém, a maioria dos historiadores consideram que ele viveu no século III d.C.. Em uma coleção de problemas algébricos do quinto ou sexto século, chamada Antologia Grega, é encontrado um problema que nos fornece alguns detalhes de sua vida, cujo enunciado diz o seguinte :

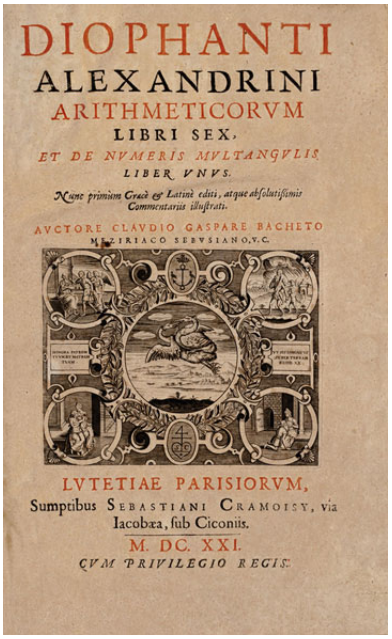
> *"Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem; Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança tardia; depois de chegar à medida de 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."(BOYER apud COHEN e DRABKIN, 2006, pág. 121)*

Se, de fato, as informações presentes no enunciado do problema forem verdadeiras, Diofanto viveu 84 anos. .

De suas poucas obras conhecidas, a mais famosa é a Arithmetica. Esta é uma coleção composta por treze livros dos quais apenas seis conservaram-se. De acordo com [2], a obra é caracterizada por um alto grau de habilidade matemática e de engenho, e, além disso, era exclusiva, ou seja, não havia nada em comum com a matemática grega tradicional já desenvolvida até a época.

Se comparada com a obra mais famosa de Euclides, a coleção Os Elementos, com respeito a estrutura, pode-se ressaltar que o trabalho de Diofanto apresenta grandes diferenças. Enquanto a primeira é constituída de uma teoria formulada por definições, postulados, proposições e teoremas, a Arithmetica apresenta cerca de 150 problemas variados, estudados em termos de exemplos numéricos a fim de encontrar generalidade para cada tipo de problema. Esses problemas estavam ligados a soluções de equações do primeiro e segundo grau.

Figura 1: Página de título da edição de 1621 da Arithmetica, traduzido em latim por Claude Gaspard Bachet de Méziriac



Fonte: *https://en.wikipedia.org/wiki/Diophantus*

Para os problemas presentes em Arithmetica, Diofanto se preocupava em encontrar soluções exatas de equações do primeiro e segundo grau (apenas uma do terceiro grau) determinadas e indeterminadas. O grande algebrista procurava soluções racionais positivas. Além disso, não se preocupava com o número de soluções possíveis, bastava encontrar apenas uma solução que já era suficiente.

Outro ponto que deve ser destacado é que, para a resolução das equações, Diofanto não utilizou "as ferramentas"fornecidas pela geometria desenvolvida até a época, como

muitos, naquele tempo, utilizavam. Tanto [3] como [2] afirmam que a obra é um estágio do desenvolvimento da álgebra conhecido como estágio intermediário e também chamado de álgebra sincopada. Esse estágio é caracterizado por abreviações para as quantidades e operações que se repetem constantemente. Nos seis livros preservados da Arithmetica, Diofanto utilizou as abreviações para as potências de números e para relações e operações, como podemos ver a seguir:

- ς (última letra da palavra arithmos, a quantidade desconhecida)
- ΔY (primeira letra de dynamis, o quadrado da quantidade desconhecida)
- KY (primeira letra de kybos, o cubo)
- $\Delta Y \Delta$ (o quadrado-quadrado) [quarta potência]
- ΔKY (o quadrado-cubo) [quinta potência]
- KYK (o cubo-cubo) [sexta potência]

Em [3], são expostos alguns problemas presentes na grandiosa obra aqui tratada. Os enunciados são os seguintes:

Problema 28, Livro II: Encontre dois números quadrados tais que seu produto acrescido de um deles resulta em um número quadrado.

Problema 6, Livro III: Encontre três números tais que a soma de todos é um quadrado e a soma de dois quaisquer deles também é um quadrado.

Problema 21, Livro IV: Encontre três números em progressão geométrica de maneira que a diferença entre dois quaisquer deles é um número quadrado.

Em suma, Diofanto com sua obra Arithmetica, considerada brilhante por muitos historiadores, forneceu muitas contribuições para o desenvolvimento do que chamamos atualmente de Teoria dos Números, onde as equações diofantinas lineares estão presentes.

Capítulo 2

Conceitos iniciais

Neste capítulo serão apresentados alguns conceitos sobre o conjunto dos números inteiros e a divisibilidade neste conjunto, bem como o máximo divisor comum (mdc) e suas propriedades, essenciais para o desenvolvimento da teoria sobre equações diofantinas lineares. As referências [6], [7], [8] e [11] foram importantes para o desenvolvimento do mesmo.

2.1 Os inteiros

Consideramos o conjunto dos números inteiros como sendo

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

Nesse conjunto, existe um subconjunto que merece destaque, o conjunto dos números naturais

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

2.2 Princípio da Boa Ordenação

O conjunto dos números inteiros possui uma propriedade conhecida como Princípio da Boa Ordenação.

Princípio da Boa Ordenação. Todo subconjunto não-vazio $A \subset \mathbb{Z}$, limitado inferiormente, possui um menor elemento, isto é, existe $n_0 \in A$ tal que para todo $n \in A$, $n_0 \leq n$.

Uma consequência importante do Príncipio da Boa ordenação é o chamado Princípio da Indução Finita, enunciado a seguir:

Princípio da Indução Finita. Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que
i) $a \in S$;
ii) $\forall n, \quad n \in S \Rightarrow n+1 \in S$.
Então $\{x \in \mathbb{Z}; \quad x \geq a\} \subset S$.

A partir do Princípio da Indução Finita, obtemos um método de prova, chamado Prova por Indução Matemática. Esse método consiste em mostrar que uma propriedade é verdadeira. Para isso, primeiramente verificamos que a propriedade é válida para o primeiro caso particular. Na sequência, assumimos que a propriedade é válida para os n primeiros casos e em seguida provamos que a propriedade é válida para o sucessor de n, no caso $n+1$. Em suma, a prova por Indução Finita decorre como abaixo:

Prova por Indução Matemática. Seja $a \in \mathbb{Z}$ e $p(n)$ uma sentença aberta em n. Mostrar que
i) $p(a)$ é verdadeiro;
ii) $\forall n \geq a, \quad p(n) \Rightarrow p(n+1)$ é verdadeiro.
Então, $p(n)$ é verdadeiro para todo $n \geq a$.

A prova por indução pode ser utilizada para verificar algumas propriedades algébricas do conhecido *número de ouro*. Descoberto pelos pitagóricos e com inúmeras aparições em diversas áreas, como a Arquitetura, a Odontologia, as Artes, este também é conhecido por razão áurea, proporção divina ou simplesmente phi. Denotado por ϕ, cujo valor é $\frac{1+\sqrt{5}}{2} \simeq 1,618$, o número de ouro é raiz da equação $x^2 = x+1$. Vamos provar por indução uma dessas propriedades afirma que qualquer potência a partir da segunda do número ϕ é resultado da soma de duas potências anteriores a dada. Vejamos o exemplo abaixo:

Exemplo 2.2.1. Sabendo que $\phi = \dfrac{1+\sqrt{5}}{2}$ é raiz da equação $x^2 = x+1$, prove que, para todo $n \in \mathbb{N}, \quad n \geq 2$,

$$\phi^n = \phi^{n-1} + \phi^{n-2}.$$

Demonstração. Seja $p(n) : \phi^n = \phi^{n-1} + \phi^{n-2}$.

Temos que $p(2) : \phi^2 = \phi + 1$, o que é verdade. Suponhamos $p(n)$ é verdade, ou seja, $\phi^n = \phi^{n-1} + \phi^{n-2}$, para todo número natural n maior que 2. Vamos provar que $p(n+1)$ também é verdade. De fato,

$$\phi^{n+1} = \phi^n.\phi^1$$

Pela hipótese, $\phi^n = \phi^{n-1} + \phi^{n-2}$. Substituindo esse valor na equação anterior, segue que

$$\phi^{n+1} = \phi^n.\phi^1 = (\phi^{n-1} + \phi^{n-2})\phi = \phi^{n-1}.\phi + \phi^{n-2}.\phi = \phi^n + \phi^{n-1}.$$

Isso comprova que a potência $n+1$ de ϕ é resultado da soma das duas potências anteriores a ela. Portanto, concluímos que é verdadeira a igualdade $\phi^n = \phi^{n-1} + \phi^{n-2}$, $n \in \mathbb{N}, \quad n \geq 2$. □

2.3 Divisibilidade

Dados dois números inteiros a e b, dizemos que a divide b, ou que a é um divisor de b, ou também que b é um múltiplo de a, e denotamos por $a \mid b$, se existir um número inteiro k_1 tal que

$$b = k_1 a.$$

Caso contrário, se a não divide b escrevemos $a \nmid b$.

Exemplo 2.3.1. Consideremos os inteiros 13 e 52. Temos que $13 \mid 52$, pois $52 = 13.4$. Por outro lado, $15 \nmid 56$ uma vez que não existe nenhum número inteiro que multiplicado por 15 resulta em 56.

Proposição 2.3.1. *Sejam $a, b, c \in \mathbb{Z}$. Então*
i) $1 \mid a$, $a \mid a$ e $a \mid 0$.
ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. i) Como $a = a.1 = 1.a$, segue que $1 \mid a$ e $a \mid a$. Sabemos que $0 = 0.a$, então $a \mid 0$.
ii) Se $a \mid b$ e $b \mid c$ existem k_1 e k_2 inteiros, tais que $b = ak_1$ e $c = bk_2$. Substituindo o valor de b da primeira equação na segunda obtemos

$$c = bk_2 = (ak_1)k_2 = a(k_1k_2) = ad,$$

com $d = k_1k_2$. Ou seja, $a \mid c$. □

Proposição 2.3.2. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid b + c$. Então, $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração. Suponhamos que $a \mid b + c$. Assim, existe $k_1 \in \mathbb{Z}$ tal que $b + c = ak_1$. Por outro lado, se $a \mid b$, existe $k_2 \in \mathbb{Z}$ de forma que a pode ser representado como $b = ak_2$. Unindo as igualdades, chegamos que

$$ak_2 + c = ak_1$$

Assim, $c = a(k_1 - k_2)$. Portanto $a \mid c$.
A recíproca é análoga.

□

Proposição 2.3.3. *Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$*

$$a \mid (bx + cy)$$

Demonstração. Como $a \mid b$ e $a \mid c$, segue que existem k_1 e k_2, inteiros, tais que $b = ak_1$ e $c = ak_2$. Assim, multiplicando x na primeira igualdade e y na segunda, temos que

$$xb + yc = x(ak_1) + y(ak_2) = a(xk_1 + yk_2),$$

implicando $a \mid bx + cy$. □

Proposição 2.3.4. *Seja $a_1, a_2, ..., a_n \in \mathbb{Z}$. Se $b \mid a_i$, $i = 1, ..., n$, então para todo $x_1, ..., x_n \in \mathbb{Z}$*

$$b \mid \sum_{i=1}^{n} a_i x_i.$$

Demonstração. Se $b \mid a_i$ com $i = 1, ..., n$, logo existe $q_1, ..., q_n \in \mathbb{Z}$ tal que $a_i = bq_i$. Multiplicando a_1 por x_1, a_2 por x_2, e assim sucessivamente até a_n por x_n, com $x_1, ..., x_n$ números inteiros, obtemos

$$a_i x_i = bq_i x_i,$$

com i variando de 1 a n. Fazendo o somatório da última igualdade, então

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} bq_i x_i = b \sum_{i=1}^{n} q_i x_i,$$

o que implica que $b \mid \sum_{i=1}^{n} a_i x_i$. □

Proposição 2.3.5. *Dados $a, b \in \mathbb{Z}$, $b \neq 0$. Se $a \mid b$ então $\mid a \mid \leq \mid b \mid$.*

Demonstração. Pela definição de divisibilidade, se $a \mid b$ existe $k_1 \in \mathbb{Z}$ tal que $b = ak_1$. Observando os módulos, é válida a igualdade $\mid b \mid = \mid a \mid \mid k_1 \mid$. Como $b \neq 0$ temos $k_1 = 0$ e logo $1 \leq \mid k_1 \mid$, implicando que $\mid a \mid \leq \mid a \mid \mid k_1 \mid = \mid b \mid$. □

2.4 Divisão Euclidiana

Euclides enunciou, porém não demonstrou, uma das regras mais importantes dentro da Matemática, a divisão euclidiana, conhecida também como divisão com resto. Esse resultado é visto por todos desde o Ensino Fundamental e aplicado, não somente no interstício escolar, mas em diversas situações do dia a dia.

Teorema 2.4.1. *(Divisão Euclidiana) Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem $q, r \in \mathbb{Z}$ unicamente determinados tais que*

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

Demonstração. Para a prova desse resultado consideremos dois casos: $b > 0$ e $b < 0$.
Caso 1: $b > 0$

Provaremos inicialmente a existência. Como $a \in \mathbb{Z}$ e $b > 0$, temos que a deve ser um múltiplo de b ou estar entre dois múltiplos consecutivos de b. Assim, existe $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q+1)b.$$

Aplicando a distributividade na segunda desigualdade e subtraindo qb na inequação, obtemos

$$0 \leq a - qb < b.$$

Definindo $r = a - qb$, garantimos a existência de q e r.

Para verificarmos a unicidade, suponhamos q', r' tais que

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

A partir disso obtemos que $(bq + r) - (bq' + r') = 0$, e logo, $r' - r = b(q - q')$, implicando que $b \mid r' - r$. Mas $r' < b$ e $r < b$, então $|r' - r| < b$. Assim $r' = r$ e, portanto, $q = q'$, pois $b(q - q') = r' - r = r - r = 0$ então $bq' = bq$ se, e somente se, $q = q'$.
Caso 2: $b < 0$

Para verificarmos o teorema quando $b < 0$ basta considerar $qb \leq a < (q-1)b$. A demonstração é análoga ao caso anterior. □

Na divisão euclidiana, o número q é chamado *quociente* da divisão de a por b e r o *resto* dessa divisão.

É importante observar que o teorema enunciado acima considera números inteiros. Contudo, Euclides quando enunciou essa regra, considerava medidas representadas por números naturais. Segundo [9], a noção de números inteiros veio séculos depois, com Brahmagupta (628 d.C.) interpretando noções de dívidas, entretanto, vários séculos se passaram desde sua aparição até sua aceitação, uma vez que haviam dúvidas quanto a sua veracidade. No século XVI, Stiffel denominava-os de números absurdos e Cardano, de soluções falsas de uma equação.

Exemplo 2.4.1. Na divisão euclidiana de 257 por 13 temos o quociente 19 e resto 10, ou seja,

$$256 = 13(19) + 10.$$

2.5 Máximo divisor comum

Definição 2.5.1. (Divisor comum) Dados $a, b \in \mathbb{Z}$, distintos ou não. Dizemos que um número $d \in \mathbb{Z}$ é um divisor comum de a e de b se $d|a$ e $d|b$.

Exemplo 2.5.1. Vamos considerar os números 120 e 168. Seja $D(120)$ o conjunto dos divisores do número 120 e $D(168)$ o conjunto dos divisores do número 168. Então

$$D(120) = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$

$$D(168) = \{1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 84, 168\}$$

Seja $D(120, 128)$ o conjunto dos divisores comuns de 120 e 168, que é a intersecção dos conjuntos $D(120)$ e $D(168)$. Assim,

$$D(120, 168) = \{1, 2, 3, 4, 6, 12, 24\}$$

Definição 2.5.2. (Máximo divisor comum) Dizemos que um número inteiro $d \geq 0$ é o máximo divisor comum (mdc) de a e b, se:
i) d é um divisor comum de a e b,
ii) E se $c \in \mathbb{Z}$ é um divisor de a e b, então $c|d$.

Denotamos o máximo divisor comum de a e b por $mdc(a, b)$. Este não depende da ordem em que a e b são escolhidos, ou seja, $mdc(a, b) = mdc(b, a)$

Exemplo 2.5.2. Observando o Exemplo 2.5.1, temos que o máximo divisor comum de 120 e 168 é 24. Ou seja,

$$mdc(120, 168) = 24$$

No exemplo anterior identificamos o máximo divisor de dois números relativamente pequenos. Listamos todos os divisores de cada um deles e observamos o maior número que divide ambos. No entanto, e para determinar $mdc(1318955, 690713)$? Devemos proceder da mesma forma como no exemplo anterior? A resposta é não. Euclides propôs um resultado, que além de responder a pergunta, utilizou o mesmo para a prova construtiva da existência do máximo divisor comum. Esse resultado é enunciado no lema a seguir, conhecido como Lema de Euclides:

Lema 2.5.1. *Sejam $a, b, n \in \mathbb{Z}$. Se existe $mdc(a, b - na)$, então, $mdc(a, b)$ existe e*

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

Demonstração. Seja $d = mdc(a, b)$ e $d' = mdc(a, b - na)$. Pela definição $d \mid a$ e $d|b$, logo $d \mid b - na$. Daí segue que $d \mid d'$. Logo, d é divisor comum de a e b. Por outro lado,

$d' \mid a$ e $d' \mid b - na$, então $d' \mid b$. Assim, $d' \mid d$, o que implica em $d = d'$. Portanto, $mdc(a, b) = mdc(a, b - na)$. □

Exemplo 2.5.3. Voltando a pergunta, vamos determinar $mdc(1318955, 690713)$. Aplicando o lema proposto por Euclides, segue que

$$\begin{aligned} mdc(1318955, 690713) &= mdc(690713, 628242) \\ &= mdc(628242, 62471) \\ &= mdc(62471, 3532) \\ &= mdc(3532, 2427) \\ &= mdc(2427, 1105) \\ &= mdc(1105, 217) \\ &= mdc(217, 20) \\ &= 1. \end{aligned}$$

2.5.1 Algoritmo de Euclides

Teorema 2.5.2 (Algoritmo de Euclides)**.** *Sejam $r_0 = a$ e $r_1 = b$ números inteiros não negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_i = q_{i+1} r_{i+1} + r_{i+2}$$

com $i = 0, 1, ..., n-1$ e $r_{n+1} = 0$ então $mdc(a, b) = r_n$, $r_n \neq 0$.

Demonstração. Se $b = 1$, $b = a$ ou $b \mid a$, o $mdc(a, b)$ pode ser facilmente determinado. Suponhamos que $b \neq a$ e $b \nmid a$. Assim temos que

$$a = q_1 b + r_2, \text{ com } 0 < r_2 < b$$

Realizando a segunda iteração, obtemos

$$b = q_2 r_2 + r_3, \ 0 \leq r_2 < b$$

Se $r_2 \mid b$, então $r_2 = mdc(b, r_2)$. Observe que se ocorrer esse caso o algoritmo termina pois, pelo lema de Euclides,

$$r_2 = mdc(b, r_2) = mdc(b, a - q_2 b) = mdc(b, a) = mdc(a, b).$$

Se $r_2 \nmid b$, temos $0 < r_3 < r_2$, donde podemos aplicar novamente o algoritmo da divisão euclidiana. Assim,

$$r_2 = q_3 r_3 + r_4, \ 0 \leq r_3 < r_2.$$

Devemos analisar novamente dois casos, quando $r_3 \mid r_2$ e quando $r_3 \nmid r_2$.

De uma forma geral, se $r_{k+1} \mid r_k$, para algum $k = 0, 1, 2, ..., n-1$, temos que $mdc(r_k, r_{k+1}) = mdc(a, b)$. Por outro lado, se $r_{k+1} \nmid r_k$, $k = 0, 1, 2, ..., n-2$, aplicamos novamente o teorema da divisão euclidiana. É verdade que em algum dos passos esse procedimento irá parar pois, caso contrário, teríamos uma sequência decrescente de números naturais $b > r_1 > r_2 > ...$ que não possui um menor elemento, entrando em contradição com o Princípio da Boa Ordenação.

Suponhamos que $r_{i+1} \mid r_i$ somente para $i = n-1$. Assim obtemos a seguinte sequência:

$$\begin{aligned}
a &= bq_1 + r_2 && 0 < r_2 < b \\
b &= r_2q_2 + r_3 && 0 < r_3 < r_2 \\
r_2 &= r_3q_3 + r_4 && 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1}r_{n-1} + r_n && 0 < r_{n-1} < r_n \\
r_{n-1} &= q_nr_n
\end{aligned}$$

Observemos que $r_{i+1} = r_i - bq_i$, $\forall i = 0, ..., n-1$. Assim, aplicando sucessivas vezes o lema de Euclides, obtemos que

$$r_n = mdc(r_{n-1}, r_{n-2}) = ... = mdc(r_1, r_0) = mdc(a, b)$$

□

Exemplo 2.5.4. Calcule o $mdc(551, 874)$.

Solução. Aplicando as divisões sucessivas, obtemos:

$$\begin{aligned}
874 &= 551 + 323 \\
551 &= 323 + 228 \\
323 &= 228 + 95 \\
228 &= 95(2) + 38 \\
95 &= 38(2) + 19 \\
38 &= 19(2) + 0
\end{aligned}$$

Assim, o $mdc(874, 551) = 19$. □

2.5.2 Propriedades do mdc

Teorema 2.5.3. *(Bachet- Bezout) Sejam $a, b \in \mathbb{Z}$. Existem $x, y \in \mathbb{Z}$ tal que*

$$ax + by = mdc(a, b)$$

Portanto se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então $c|mdc(a, b)$.

Demonstração. Seja

$$I(a, b) = \{xa + yb; \quad x, y \in \mathbb{Z}\},$$

o conjunto das combinações lineares inteiras de a e de b. É fácil ver que $I(a, b) \cap \mathbb{N} \neq \varnothing$. Basta tomarmos $x = a$ e $y = b$ donde segue que $a.a + b.b = a^2 + b^2 \in I(a, b) \cap \mathbb{N}$. Seja $d = ax_0 + by_0$, o menor elemento positivo de $I(a, b)$. Provaremos que d divide todos os elementos de $I(a, b)$. De fato, considere $m = ax + by \in I(a, b)$. Pela divisão euclidiana de m por d, temos que existem $q, r \in \mathbb{Z}$ tal que $m = dq + r$, com $0 \leq r < d$. Assim,

$$r = m - dq = (ax + by) - (ax_0 + by_0)q = a(x - x_0q) + b(y - y_0q) \in I(a, b).$$

Mas $r < d$ e d é o menor elemento positivo de $I(a, b)$. Logo $r = 0$ e, assim $d \mid m$.

Agora, provaremos a segunda afirmação. Pelo que provamos anteriormente, d divide todo número da forma $ax + by$, com $a, b \in I(a, b)$. Segue pela proposição 2.3.3 que que $d \mid a$ e $d \mid b$. Como $d = minI(a, b)$, necessariamente $d \leq mdc(a, b)$. Seja $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$. Então $c \mid ax_0 + by_0 \Leftrightarrow c \mid d$. Tomando $c = mdc(a, b)$ e sabendo que $d \leq mdc(a, b)$, logo

$$c \mid d \Leftrightarrow mdc(a, b) \mid d \Leftrightarrow d = mdc(a, b).$$

□

No próximo exemplo mostramos uma aplicação do teorema acima e também o cálculo do mdc por meio do algoritmo de Euclides.

Exemplo 2.5.5. Calcule o $mdc(551, 874)$ e determine os números inteiros x, y tais que $mdc(551, 874) = 551x + 874y$.

Solução. No exemplo 2.5.4 vimos que o $mdc(874, 551) = 19$. Para determinar os números x, y basta isolar os restos obtidos nas divisões e escrever o algoritmo de trás para frente, fazendo as substituições necessárias. Dessa forma,

$$\begin{aligned} 19 &= 95 - 38(2) = 95 - (228 - 95(2))(2) = (5)95 - 2(228) = \\ &= (5)(323 - 228) - 2(228) = (5)323 - (7)228 = \\ &= (5)323 - (7)(551 - 323) = (12)323 - (7)551 = \\ &= (12)(874 - 551) - (7)551 = 551(-19) + 874(12) \end{aligned}$$

Portanto, $x = -19$ e $y = 12$. □

Corolário 2.5.4. *Quaisquer que sejam $a, b \in \mathbb{Z}$, ambos não nulos, e $n \in \mathbb{N} \setminus \{0\}$, tem-se que*

$$mdc(na, nb) = n.mdc(a, b).$$

Demonstração. A prova decorre facilmente pelo teorema provado acima. Existem $x, y\mathbb{Z}$, tal que

$$mdc(na, nb) = (na)x + (nb)y = n(ax) + n(by) = n(ax + by) = n.mdc(a, b).$$

□

Corolário 2.5.5. *Dados $a, b \in \mathbb{Z}$, ambos não nulos, tem-se que*

$$mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = 1$$

Demonstração. Pelo corolário anterior, tem-se que

$$\begin{aligned} mdc(a,b).mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) &= mdc\left(mdc(a,b)\frac{a}{mdc(a,b)}, mdc(a,b)\frac{b}{mdc(a,b)}\right) \\ &= mdc(a,b) \end{aligned}$$

Logo,

$$mdc\left(\frac{a}{mdc(a,b)}, \frac{b}{mdc(a,b)}\right) = 1$$

□

Definição 2.5.3. Dois números inteiros a e b são denominados primos entre si se o máximo divisor comum entre eles é 1.

Proposição 2.5.6. *Dois números inteiros a e b são primos entre si se, e somente se, existirem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração. ($\Rightarrow$) Sejam a e b primos entre si. Pela relação de Bachet-Bézout, existem $m, n \in \mathbb{Z}$ tal que

$$ma + nb = mdc(a, b) = 1.$$

($\Leftarrow$) Suponha m, n inteiros tais que $ma + nb = 1$. Se $d = mdc(a, b)$, $d \mid ma + nb$, ou seja, $d \mid 1$, que acontece se, e somente se, $d = 1$. □

Teorema 2.5.7. *(Lema de Gauss) Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid bc$ e a e b são primos entre si, então $a \mid c$.*

Demonstração. Se $a \mid bc$, então existe um $k \in \mathbb{Z}$ tal que $bc = ak$. Por hipótese sabemos que $mdc(a, b) = 1$, pois a e b são primos entre si, então, pela proposição anterior, existem m e n tais que

$$ma + nb = 1.$$

Multiplicando os dois lados da igualdade por $c \in \mathbb{Z}$, obtemos

$$c = mac + nbc.$$

Substituindo bc por ak na última igualdade, temos que

$$c = mac + nak = a(mc + nk).$$

Portanto, $a \mid c$.

□

Corolário 2.5.8. *Dados $a, b, c \in \mathbb{Z}$, com b e c não nulos, temos que*

$$b|a \text{ e } c|a \Leftrightarrow \frac{bc}{mdc(b,c)}|a$$

Demonstração. ($\Rightarrow$) Como $b|a$ e $c|a$, existem $m, n \in \mathbb{Z}$ tais que $a = nb = mc$. Logo,

$$n\frac{b}{mdc(b,c)} = m\frac{c}{mdc(b,c)}.$$

Pelo corolário 2.5.4, temos que $mdc\left(\frac{b}{mdc(b,c)}, \frac{c}{mdc(b,c)}\right) = 1$, então

$$\frac{b}{mdc(b,c)} \mid m$$

. Logo, $\frac{b}{mdc(b,c)}c \mid mc$, e, portanto, $\frac{b}{mdc(b,c)}c \mid a$.
($\Leftarrow$) Se $\frac{bc}{mdc(b,c)}|a$, existe $m' \in \mathbb{Z}$, tal que

$$a = m'\frac{bc}{mdc(b,c)} = b\frac{m'c}{mdc(b,c)} = c\frac{m'b}{mdc(b,c)}.$$

Assim, $b \mid a$ e $c \mid a$. □

Exemplo 2.5.6. Prove que:

Se $mdc(a, 2^{n+1}) = 2^n$ e $mdc(b, 2^{n+1}) = 2^n$, então $mdc(a + b, 2^{n+1}) = 2^{n+1}$.

Solução. De $mdc(a, 2^{n+1}) = 2^n$ e $mdc(b, 2^{n+1}) = 2^n$ segue que $2^n \mid a$ e $2^n \mid b$, ou seja, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = 2^n k_1$ e $b = 2^n k_2$. Observemos que k_1, k_2 são ímpares, pois caso contrário $mdc(a, 2^{n+1}) = mdc(b, 2^{n+1}) = 2^{n+1}$. Assim,

$$a + b = 2^n k_1 + 2^n k_2 = 2^n(k_1 + k_2) = 2^n(2k) = 2^{n+1}k.$$

Logo,

$$mdc(a + b, 2^{n+1}) = mdc(2^{n+1}k, 2^{n+1}) = 2^{n+1}.$$

□

Exemplo 2.5.7. A sequência de Fibonacci é definida como sendo a sequência cujo os dois primeiros termos são iguais a 1 e a partir do terceiro, cada um dos termos são iguais a soma dos dois anteriores.Logo a sequência de Fibonacci é da seguinte forma

$$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...)$$

Seja F_{n+1}, F_{n+2}, dois termos dessa sequência. Prove que $mdc(F_{n+1}, F_{n+2}) = 1$, $\forall n \in \mathbb{N} \cup 0$.

Solução. A prova decorre por indução. Se $n = 0$, temos que

$$p(0) : mdc(F_1, F_2) = mdc(1, 1) = 1.$$

Suponhamos que

$$p(n) : mdc(F_{n+1}, F_{n+2}) = 1$$

é verdade. Vamos provar que $p(n + 1)$ é verdade. Pela definição de Fibonacci e o lema de Euclides, temos:

$$mdc(F_{n+1+1}, F_{n+1+2}) = mdc(F_{n+2}, F_{n+3}) = mdc(F_{n+2}, F_{n+2}+F_{n+1}) = mdc(F_{n+2}, F_{n+1}) = 1$$

□

2.6 Generalização do mdc

Podemos generalizar o conceito de mdc através da seguinte definição:

Definição 2.6.1. Um número natural d é dito mdc dos inteiros $a_1, a_2, ..., a_n$, não todos nulos, se satisfazer as condições:
i) d é um divisor comum de $a_1, a_2, ..., a_n$.
ii) Se c é um divisor comum de $a_1, a_2, ..., a_n$, então $c \mid d$.

Este é único e denotado por $mdc(a_1, a_2, ..., a_n)$. A proposição a seguir fornece métodos para o cálculo do mdc de n inteiros utilizando o Algoritmo de Euclides,.

Proposição 2.6.1. *Dados $a_1, a_2, ..., a_n$, números inteiros não todos nulos, existe o mdc e*

$$mdc(a_1, a_2, ..., a_n) = mdc(a_1, a_2, ..., mdc(a_{n-1}, a_n)) = mdc(mdc(a_1, a_2, ..., a_{n-1}), a_n)$$

Demonstração. A prova acontece por indução sobre n. Provamos inicialmente a primeira igualdade. Para $n = 2$, já vimos que é válido. Suponhamos que é a igualdade é válida para n. Vamos provar que é verdade para $n + 1$.

Seja $d = mdc(a_1, ..., mdc(a_n, a_{n+1}))$. Então, pela definição temos que $d \mid a_1$, $d \mid a_2$, $d \mid a_3$, ...,$d \mid a_{n-1}$ e $d \mid mdc(a_n, a_{n+1})$. Logo, $d \mid a_1, ..., d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$. Considere agora c um divisor comum de $a_1, a_2, ..., a_n, a_{n+1}$. Logo, c é um divisor comum de $a_1, a_2, ..., a_{n-1}$ e $mdc(a_n, a_{n+1})$. Portanto, $c \mid d$.

A segunda igualdade é provada também por indução. □

Anteriormente, vimos que podemos escrever o mdc de dois inteiros como uma combinação linear. Do mesmo modo, podemos generalizar esse método para n números inteiros a partir do seguinte teorema:

Teorema 2.6.2. *(Generalização Báchet-Bezout) Sejam $a_1, a_2, ..., a_n$, números inteiros. Existem $x_1, x_2..., x_n \in \mathbb{Z}$ tais que*

$$mdc(a_1, a_2, ..., a_n) = x_1a_1 + x_2a_2 + ... + x_na_n = \sum_{i=1}^{n} a_ix_i.$$

Demonstração. Sejam $a_1, a_2, ..., a_n \in \mathbb{Z}$. Consideremos o conjunto

$$I(a_1, a_2, ..., a_n) = \left\{ \sum_{i=1}^{n} a_ix_i; \quad x_i \in \mathbb{Z} \ \ \forall i = \overline{1, ..., n} \right\}$$

Temos que $I(a_1, a_2, ..., a_n) \cap \mathbb{N} \neq \varnothing$. Para verificarmos esse fato basta tomar $x_i = a_i$, com $i = 1, ..., n$, obtendo assim

$$\sum_{i=1}^{n} a_ia_i = \sum_{i=1}^{n} a_i^2 \in I(a_1, a_2, ..., a_n) \cap \mathbb{N}.$$

Seja $d = \sum_{i=1}^{n} a_ix_i'$, o menor elemento de $I(a_1, a_2, ..., a_n) \cap \mathbb{N}$. A afirmação é que d divide todo elemento de $I(a_1, a_2, ..., a_n)$. De fato, considere $m = \sum_{i=1}^{n} a_ix_i$. Pela divisão

Euclidiana de m por d, existe $q, r \in \mathbb{Z}$ tal que $m = dq + r$, com $0 \leq r < d$. Assim,

$$\begin{aligned} r &= m - dq \\ &= \sum_{i=1}^{n} a_i x_i - q.\sum_{i=1}^{n} a_i x_i' \\ &= \sum_{i=1}^{n} a_i x_i - q.a_i x_i' \\ &= \sum_{i=1}^{n} a_i (x_i - q.x_i') \in I(a_1, a_2, ..., a_n) \end{aligned}$$

Contudo, $r < d$ e d é o menor elemento positivo de $I(a_1, a_2, ..., a_n)$. Logo, $r = 0$ e $d \mid m$.

Mostraremos agora que d é o $mdc(a_1, a_2, ..., a_n)$. Repare que d divide todo elemento de $I(a_1, a_2, ..., a_n)$, assim, $d \mid a_i, \quad \forall i = 1, ..., n$. Como d é o menor elemento positivo de $I(a_1, a_2, ..., a_n)$, necessariamente $d \leq mdc(a_1, a_2..., a_n)$. Por outro lado, $mdc(a_1, a_2, ..., a_n)$ divide todos os elementos de $I(a_1, a_2, ..., a_n)$, então $mdc(a_1, a_2, ..., a_n) \mid d$. Isso acontece se, e somente se, $d = mdc(a_1, a_2, ..., a_n)$. □

Capítulo 3

Equações Diofantinas Lineares

3.1 Equações de duas variáveis

Uma equação diofantina de duas variáveis é dita linear se ela é da forma $ax+by = c$, onde a, b e $c \in \mathbb{Z}$, com a e b não nulos.

Uma solução inteira desse tipo de equação é o par de inteiros x_0, y_0 que satisfaz a igualdade:

$$ax_0 + by_0 = c$$

Vejamos aqui um exemplo simples de equação diofantina:

$$2x + 3y = 60$$

Podemos exprimir facilmente uma solução inteira da equação dada. Consideremos o par $(15, 10)$. Se substituí-lo na equação, obtemos

$$2(15) + 3(10) = 60$$

o que mostra que esse par é uma solução.

Mas sempre as equações diofantinas vão ter soluções inteiras? Pretendemos responder essa pergunta logo abaixo. Porém, antes disso vamos observar a seguinte equação:

$$22x + 52y = 1023$$

Analisando a equação dada é possível verificar que esta não admite soluções inteiras. A justificativa é simples. Suponhamos que x_0, y_0, números inteiros, é uma solução da equação. Assim $22x_0 + 52y_0 = 1023$. Contudo, pelo lado esquerdo da igualdade temos que $22x_0 + 52y_0 = 2(11x_0 + 26y_0) = 2k$, com $k = 11x_0 + 26y_0$. Por outro lado, 1023 é ímpar. Daí segue que essa equação não admite solução inteira.

Uma das condições para que a equação diofantina da forma $ax + by = c$ admita

solução inteira é que $mdc(a, b) \mid c$. Vamos mostrar esse resultado na seguinte proposição.

Proposição 3.1.1. *Uma equação diofantina $ax + by = c$ com a, b e c inteiros, em que $a \geq 0$ ou $b \geq 0$, admite solução se, e somente se, $mdc(a, b) \mid c$.*

Demonstração. ($\Rightarrow$) Considere x_0, y_0, soluções da equação. Assim,

$$ax_0 + by_0 = c.$$

Por outro lado, seja $d = mdc(a, b)$. Então $d \mid a$ e $d \mid b$, ou seja a e b podem ser reescritos como $a = k_1 d$ e $b = k_2 d$, com $k_1, k_2 \in \mathbb{Z}$. Substituindo os valores de a e b na equação acima segue que,

$$c = ax_0 + by_0 = k_1 dx_0 + k_2 dy_0 = d(k_1 x_0 + k_2 y_0) = dq.$$

Portanto, $d \mid c$.

($\Leftarrow$) Considere $d = mdc(a, b)$. Pela relação de Bachet-Bézout, existem inteiros x_0 e y_0 tais que

$$d = ax_0 + by_0.$$

Por hipótese temos que $d \mid c$, ou seja, existe $t \in \mathbb{Z}$ tal que $c = dt$. Segue então que

$$c = dt = (ax_0 + by_0)t = a(x_0 t) + b(y_0 t),$$

com $x_0 t, y_0 t$ solução da equação $ax + by = c$.

□

Exemplo 3.1.1. Sejam F_n, F_{n+1} dois termos da sequência de Fibonacci, sendo n um número natural. As equações diofantinas da forma

$$F_n x + F_{n+1} y = c$$

sempre possuem solução, pois $mdc(F_n, F_{n+1}) = 1$, e $1 \mid c$.

Na proposição acima mostramos as condições para que as equações diofantinas lineares de duas variáveis tenham soluções. Mas como e quantas são as soluções inteiras? É o que vamos mostrar nas próximas proposições.

Proposição 3.1.2. *Seja x_0, y_0 uma solução particular da equação $ax + by = c$. Então essa equação admite infinitas soluções e o conjunto dessas soluções é*

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

com d=mdc(a,b).

Demonstração. Consideremos (x', y') uma solução inteira da equação $ax + by = c$. Então,

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

Reescrevendo a igualdade acima, temos que

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

Seja d o máximo divisor comum de a e b. Logo, $a = dr$ e $b = ds$, com $r, s \in \mathbb{Z}$ e $mdc(r, s) = 1$. Então,

$$r(x' - x_0) = s(y_0 - y').$$

Pela igualdade acima temos que $r \mid s(y_0 - y')$. Como $mdc(r, s) = 1$, necessariamente $r \mid (y_0 - y')$, ou seja, existe um t inteiro tal que $y_0 - y' = rt$. Assim,

$$y' = y_0 - rt = y_0 - \frac{a}{d}t$$

Então, para encontrarmos a forma das soluções x_0, substituímos o valor de y' na equação encontrada anteriormente temos que

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

que é equivalente a

$$a(x' - x_0) = b\left(y_0 - \left(y_0 - \frac{a}{d}t\right)\right).$$

Isso implica em

$$a(x' - x_0) = b\left(\frac{a}{d}t\right).$$

Assim,

$$a(x' - x_0) = \frac{ba}{d}t.$$

Dessa forma,

$$x' - x_0 = \frac{b}{d}t,$$

e, logo,

$$x' = x_0 + \frac{b}{d}t.$$

Por outro lado, o par $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ é solução da equação dada, para todo

$t \in \mathbb{Z}$. De fato, substituindo esses valores na equação, temos

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = \\ &= ax_0 + by_0 = c. \end{aligned}$$

□

Diante do resultado acima podemos concluir que a equação diofantina $ax + by = c$ possui infinitas soluções em $\mathbb{Z}$. Uma consequência imediata dessa proposição pode ser enunciada através do seguinte corolário.

Corolário 3.1.3. *Se a, b são inteiros não nulos e primos entre si, então a equação diofantina $ax + by = c$ tem soluções da forma*

$$S = \{(x_0 + bt, y_0 - at) \mid t \in \mathbb{Z}\}$$

3.1.1 Exemplos

Vejamos alguns exemplos práticos relativos a resolução de equações diofantinas de duas variáveis:

Exemplo 3.1.2. Determine a solução geral da equação diofantina $12x - 27y = 33$.

Solução. Como $mdc(12, 27) = 3$ e $3 \mid 33$, a equação dada tem solução. Podemos reescrevê-la da seguinte forma:

$$4x - 9y = 11.$$

De imediato é fácil ver que $x_0 = 5$ e $y_0 = 1$ é uma solução particular da última equação. Nesse sentido, pela proposição 3.1.2, o conjunto solução dessa equação é

$$S = \{(5 - 9t, 1 - 4t) \mid t \in \mathbb{Z}\}.$$

□

Exemplo 3.1.3. Encontre o conjunto solução de $423x + 198y = 63$.

Solução. Em primeira instância, vamos determinar $mdc(423, 198)$ utilizando o algoritmo de Euclides.

$$\begin{aligned} 423 &= 198(2) + 27 \\ 198 &= 27(7) + 9 \\ 27 &= 9(3) + 0 \end{aligned}$$

Logo, $mdc(423, 198) = 9$ e $9 \mid 63$. Portanto a equação diofantina possui solução. Encontraremos uma solução particular e posteriormente determinaremos a solução geral. Isolando os restos e fazendo as substituições necessárias, obtemos:

$$9 = 198 - 27(7) = 198 - (423 - 198(2))(7) = (-7)423 + (15)198.$$

Observe que $63 = 7.9$ e $(-7)423 + (15)198 = 9$. Multiplicando essa equação por 7 determinamos duas soluções particulares da equação principal. Assim,

$$(-49)423 + (105)198 = 63.$$

onde $x_0 = -49$ e $y_0 = 105$ é uma solução particular. Portanto, segue pela preposição 3.1.2, que o conjunto solução da equação inicial é

$$S = \left\{ \left(-49 + \frac{198}{9}t, 105 - \frac{423}{9}t \right) \mid t \in \mathbb{Z} \right\}.$$

□

3.2 Equações Diofantinas de três variáveis

Dizemos que uma equação diofantina é linear de três variáveis se ela é escrita da forma

$$ax + by + cz = s,$$

em que $a, b, c, z \in \mathbb{Z}$, no qual os coeficientes a, b e c não são nulos.

Vimos na proposição 3.1.1 que uma equação diofantina linear de duas variáveis $ax + by = c$ possui solução se, se somente se, $mdc(a, b) \mid c$. De forma similar, as equações diofantinas de três variáveis admitem solução se, e somente se, o termo a direita da igualdade é divisível pelo máximo divisor comum dos coeficientes a, b e c. Enunciamos esse resultado na seguinte proposição.

Proposição 3.2.1. *A equação diofantina $ax + by + cz = k$ com a, b, c números inteiros não nulos e k um inteiro qualquer admite solução se, e somente se, $mdc(a, b, c) \mid k$.*

É simples determinar uma solução particular para essa equação. Seja $d_1 = mdc(a, b)$. Logo existem $t_1, t_2 \in \mathbb{Z}$ tais que $at_1 + bt_2 = d_1$. Como $mdc(a, b, c) = mdc(d_1, c) = d$, existem t, z_0 inteiros de modo que $d = d_1t + cz_0$. Logo,

$$d = d_1t + cz_0 = (at_1 + bt_2)t + cz_0 = at_1t + bt_2t + cz_0$$

Tomando $x_0 = t_1 t$ e $y_0 = t_2 t$ temos que

$$ax_0 + by_0 + cz_0 = d$$

Pela proposição anterior a equação $ax + by + cz = k$ admite solução se $d \mid k$, ou seja, $k = dq$, para algum q inteiro. Assim,

$$a(x_0 q) + b(y_0 q) + c(z_0 q) = dq = k$$

onde $x_0 q, y_0 q$ e $z_0 q$ são soluções particulares dessa equação.

Contudo, é mais interessante conhecermos uma forma geral para todas as soluções do que apenas casos particulares. Nesse sentido, na proposição a seguir determinaremos o conjunto dessas soluções a partir de soluções particulares. Para isto, reduziremos a equação diofantina de três variáveis a uma de duas variáveis, que sabemos resolver utilizando a teoria desenvolvida até aqui.

Proposição 3.2.2. *Seja x_0, y_0, z_0 uma solução particular da equação $ax + by + cz = k$, com $a \neq 0$, $b \neq 0$ e $c \neq 0$. A equação admite infinitas soluções e o conjunto dessas soluções é*

$$S = \left\{ \left(x_0(l_0 - cs) + \frac{b}{mdc(a,b)} t, y_0(l_0 - cs) - \frac{a}{mdc(a,b)} t, mdc(a,b).s + r \right) \mid \quad l_0, s, t \in \mathbb{Z} \right\}.$$

Demonstração. Considere a equação $ax + by + cz = k$, com $mdc(a,b,c) \mid k$. Podemos reescrevê-la como

$$ax + by = k - cz$$

Para que esta última tenha solução, assumimos que $mdc(a,b) \mid k - cz$. Considere então $z = mdc(a,b)s + r$, $r, s \in \mathbb{Z}$. Logo,

$$\begin{aligned} k - cz &= k - c(mdc(a,b).s + r) \\ &= k - c.mdc(a,b).s - cr \\ &= (k - cr) - cs.mdc(a,b) \end{aligned}$$

Como $mdc(a,b) \mid (k - cr) - cs.mdc(a,b)$ e $mdc(a,b) \mid cs.mdc(a,b)$, necessariamente $mdc(a,b) \mid k - cr$. Assim, existe um número inteiro l tal que $k - cr = mdc(a,b).l$. Com isso segue que

$$mdc(a,b).l + cr = k.$$

Observemos que a equação acima admite solução, pois $mdc(mdc(a,b),c) = mdc(a,b,c)$ e por hipótese $mdc(a,b,c) \mid k$. Dessa maneira, se o par de inteiros (l_0, r_0) satisfaz $mdc(a,b)l_0 +$

$cr_0 = k$, logo $k - cr_0 = mdc(a,b)l_0$. Tomando essa igualdade e combinando algumas equações dadas anteriormente, temos que

$$k - cz = (k - cr_0) - cs.mdc(a,b) = mdc(a,b)l_0 - cs.mdc(a,b) = mdc(a,b)(l_0 - cs)$$

Logo, obtemos a equação diofantina linear de duas variáveis

$$ax + by = mcd(a,b)(l_0 - cs)$$

com solução para qualquer $s \in \mathbb{Z}$.

Seja x_0, y_0 uma solução particular da equação $ax+by = mdc(a,b)$. Isso significa que $ax_0+ay_0 = mdc(a,b)$. Multiplicando essa equação por l_0-cs, temos $(x_0(l_0-cs), y_0(l_0-cs))$ solução particular da equação diofantina

$$a(x_0(l_0 - cs)) + b(y_0(l_0 - cs)) = mdc(a,b)(l_0 - cs).$$

Segue então que a solução geral da equação diofantina pode ser expressa por

$$\begin{aligned} x &= x_0(l_0 - cs) + \frac{b}{mdc(a,b)}t \\ y &= y_0(l_0 - cs) - \frac{a}{mdc(a,b)}t \\ z &= mdc(a,b).s + r \end{aligned}$$

com $t \in \mathbb{Z}$. Portanto, o conjunto solução dessa equação

$$S = \left\{ \left(x_0(l_0 - cs) + \frac{b}{mdc(a,b)}t, y_0(l_0 - cs) - \frac{a}{mdc(a,b)}t, mdc(a,b).s + r_0 \right) \mid \quad r_0, l_0, s, t \in \mathbb{Z} \right\}$$

□

Apesar da demonstração anterior não seguir este viés, é importante ressaltar que em uma equação do formato $ax + by + cz = k$, poderíamos considerar $p = ax + by$ e resolver a equação de duas variáveis $p + cz = k$. A partir desta, determinamos a solução geral, ou seja, o valor de z e o valor de p ($p = p_0 + ct$ e $z = z_0 - t$). Na sequência basta resolvermos $ax + by = p_0 + ct$ que obteremos os respectivos valores das incógnitas x e y. Na próxima seção apresentamos três exemplos mostrando o processo para a determinação da solução geral de equações diofantinas de três variáveis.

3.3 Exemplos

Exemplo 3.3.1. Determine a solução de $56x + 72y + 21z = 317$.

Solução. Reescrevendo a equação acima de tal forma que em um lado da igualdade permaneça apenas as variáveis x e y, obtemos

$$56x + 72y = 317 - 21z.$$

Essa equação admite solução somente se $mdc(56, 72) \mid 317-21z$. No entanto, como $mdc(56, 72) = 8$, para que a equação tenha solução devemos ter $8 \mid 317-21z$. Pela divisão euclidiana, consideremos $z = 8k + r$, de forma que r é o número entre 0 e 7 que satisfaça $8 \mid 317 - 21(8q + r)$. Observemos que

$$317 - 21z = 317 - 21(8q + r) = (39)8 + 5 - 21.8q - 21r = 8(39 - 21q) + (5 - 21r).$$

Logo, $8 \mid 317 - 21z$ se

$$8 \mid 8(39 - 21q) + (5 - 21r),$$

ou seja,

$$8 \mid (5 - 21r)$$

Como r assume valores de 0 a 7, o único valor possível de r tal que $8 \mid 5 - 21r$ é 1. Assim $z = 8q + 1$ e, portanto, $56x + 72y = 296 - 168q$.

Determinaremos agora as soluções particulares dessa equação de duas variáveis. Pelo algoritmo de Euclides,

$$\begin{aligned} 72 &= 56 + 16 \\ 56 &= 16(3) + 8 \\ 16 &= 8(2) + 0 \end{aligned}$$

Reescrevendo 8 a partir do algoritmo, concluímos que

$$8 = 56 - 16(3) = 56 - (72 - 56)(3) = (4)56 + (-3)72.$$

Contudo, temos que $296-168q = 8(37-21q)$ e, multiplicando a igualdade anterior por $37 - 21q$, encontramos as soluções particulares procuradas $x_0 = 148 - 84q$ e $y_0 = -111 + 63q$.

$$56(148 - 84q) + 72(-111 + 63q) = 296 - 168q.$$

Uma vez encontradas soluções particulares, segue, que a solução geral da equação inicial é

$$S = \{(148 - 84q + 9t, -111 + 63q - 7t, 8q + 1) \mid t \in \mathbb{Z}\}.$$

□

Exemplo 3.3.2. Encontre a solução geral para a equação diofantina

$$31x + 49y - 22z = 2.$$

Solução. Observemos inicialmente que $mdc(31, 49, 22) = 1$ e $1 \mid 2$, portanto a equação dada tem solução. Seja $p = 31x + 49y$. Podemos reescrever a equação dada como

$$p - 22z = 2.$$

A partir desse novo formato, temos que $mdc(1, -22) = 1$ e $1 \mid 2$, implicando que esta equação também tem solução. Vamos determina-la utilizando a teoria desenvolvida anteriormente. É fácil perceber que uma solução particular dessa equação é $(-20, -1)$. Assim, pela proposição 3.1.2, temos que a solução geral dessa equação é dada por

$$p = -20 - 22t \qquad z = -1 - t.$$

Contudo, sabemos que $p = 31x + 49y$. Logo, para encontrarmos a solução da equação diofantina dada inicialmente devemos resolver

$$31x + 49y = -20 - 22t \tag{3.1}$$

A equação acima admite solução se, e somente se, $mdc(31, 49) \mid -20 - 22t$. Como $mdc(31, 49) = 1$, decorre que a equação possui solução para todo $t \in \mathbb{Z}$. Determinemos agora a solução geral. Pelo Algoritmo de Euclides, temos que

$$\begin{aligned} 49 &= 31.1 + 18 \\ 31 &= 18.1 + 13 \\ 18 &= 13.1 + 5 \\ 13 &= 5.2 + 3 \\ 5 &= 3.1 + 2 \\ 3 &= 2.1 + 1 \end{aligned}$$

A partir do processo acima, segue que:

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 3(2) - 5 = (13 - 5.2)(2) - 5 = 13(2) - 5(5) = \\ &= 13(2) + (18 - 3)(-5) = 13(7) + 18(-5) = (31 - 18)(7) + 18(-5) = \\ &= 31(7) + 18(-12) = 31(7) + (49 - 31)(-12) = 31(19) + 49(-12) \end{aligned}$$

Multiplicando a igualdade $1 = 31(19) + 49(-12)$ por $-20 - 22t$, temos que

$$31(-380 - 418t) + 49(240 + 264t) = -20 - 22t.$$

Assim, o par $(-380 - 418t, 240 + 264t)$ é uma solução particular da equação (3.1). Logo, pela proposição 3.1.2, o conjunto solução da equação pretendida pode ser expresso por

$$S = \{(-380 - 418t + 49t_1, 240 + 264t - 31t_1, -1 - t) \mid \quad t, t_1 \in \mathbb{Z}\}$$

□

Exemplo 3.3.3. Determine o conjunto das soluções da equação

$$120x + 180y + 84z = 72.$$

Solução. Como $mdc(120, 180, 84) = 12$, a equação acima possui solução, uma vez que $12 \mid 72$. Podemos reescrevê-la da seguinte forma

$$10x + 15y + 7z = 6.$$

Considere $p = 10x + 15y$. Logo,

$$p + 7z = 6.$$

Essa última equação admite solução pois $mdc(1, 7) = 1$, sendo uma solução particular o par $(20, -2)$. Logo, as soluções inteiras p, z são da forma

$$p = 20 + 7t \qquad z = -2 - t,$$

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

Por outro lado, $10x + 15y = p = 20 + 7t$.

Diante disso, devemos encontrar as soluções inteiras da equação

$$10x + 15y = 20 + 7t. \tag{3.2}$$

Para esta admitir soluções inteiras, $mdc(10, 15) = 5$ deve dividir $20 + 7t$. Repare que neste exemplo, ao contrário do exemplo anterior, t não pode assumir qualquer valor inteiro uma vez que $5 \mid 20 + 7t$, que acontece somente se t é um múltiplo de 5. Logo, t é da forma $5k$, sendo k um número inteiro arbitrário.

Dessa forma, a equação (3.2) pode ser expressa por

$$2x + 3y = 4 + 7k$$

a qual possui solução devido 2 e 3 serem primos entre si. Com isso pelo algoritmo de Euclides, decorre que

$$1 = 2(-1) + 3.$$

Multiplicando a equação por $4+7k$, obtemos uma solução particular que é expressa por $(-4-7k, 4+7k)$.

Nesse sentido, em decorrência da proposição 3.1.2, as soluções x, y da equação (3.2) são da forma

$$x = -4 - 7k + 3t_1 \qquad y = 4 + 7k - 2t_1, \quad t_1 \in \mathbb{Z}$$

Levando em consideração que $z = -2 - t = -2 - 5k$, segue, portanto, que o conjunto solução da equação diofantina $120x + 180y + 84z = 72$ é

$$S = \{(-4 - 7k + 3t_1, 4 + 7k - 2t_1, -2 - 5k) \mid \quad k, t_1 \in \mathbb{Z}\}.$$

□

3.4 Generalização: Equações Diofantinas de n variáveis

Uma equação diofantina de n variáveis é uma equação da forma

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n = k,$$

com $a_i \in \mathbb{Z} \setminus \{0\}, \quad \forall i = 1, ..., n.$

Da mesma forma que as equações de duas e três variáveis, é necessário uma condição, enunciada na próxima proposição, para que esta equação diofantina admita solução.

Proposição 3.4.1. *A equação diofantina* $a_1x_1 + a_2x_2 + ... + a_nx_n = k, a_i \in \mathbb{Z}, \quad a_i \neq 0$ $\forall i = 1, ..., n$, *com* $k \in \mathbb{Z}$ *admite solução se, e somente se,* $mdc(a_1, a_2, ..., a_n) \mid k$.

Demonstração. Pelo teorema 2.6.2, vimos que

$$I(a_1, a_2, ..., a_n) = \left\{ \sum_{i=1}^{n} a_i x_i; \quad x_i \in \mathbb{Z} \right\} = mdc(a_1, ..., a_n)\mathbb{Z}.$$

É fato que a equação $a_1x_1 + a_2x_2 + ... + a_nx_n = k$ possui solução se, e somente se, $k \in I(a_1, ..., a_n)$, que é equivalente a $c \in mdc(a_1, ..., a_n)\mathbb{Z}$ que, por sua vez, é o mesmo que $mdc(a_1, ..., a_n) \mid c$. □

3.4.1 Solução Geral

O método para determinar a solução geral de uma equação diofantina solucionável de n variáveis consiste basicamente em reduzir a equação em uma outra equação composta

de duas variáveis, que já sabemos resolver. Com esse procedimento determinaremos o valor da n-ésima incógnita. Após, devemos solucionar uma equação de $n-1$ incógnitas, e, procedendo de forma análoga, obteremos o valor da incógnita de índice $n-1$. Repetindo esse processo consecutivamente, paramos apenas no momento em que nos depararmos com uma equação de duas variáveis do formato $a_1x_1 + a_2x_2 = k$, cuja solução é conhecida. Vamos ilustrar esse método com o seguinte exemplo referente a uma equação diofantina composta por 5 variáveis:

Exemplo 3.4.1. Determine a solução da equação $30x + 42y + 70z + 105u + 26v = 41$.

Solução. Para resolver esse exemplo, primeiramente devemos verificar se a equação possui solução. Como $mdc(30, 42, 70, 105, 26) = 1$, a solução pode ser determinada. Seja

$$p^{(1)} = 30x + 42y + 70z + 105u.$$

Diante disso, a equação que procuramos a solução pode ser reescrita como uma outra de duas variáveis da seguinte forma

$$p^{(1)} + 26v = 41$$

Os valores $p_0 = 15$ e $v_0 = 1$ são soluções particulares desta última equação. Nesse sentido sua solução geral é dada por

$$p^{(1)} = 15 + 26t_0 \qquad v = 1 - t_0, \qquad t_0 \in \mathbb{Z}.$$

Agora, procedemos do seguinte modo: substituímos na solução geral o valor de $p^{(1)}$ considerado no início e verificamos se a equação formada admite solução. Dessa forma,

$$30x + 42y + 70z + 105u = 15 + 26t_0$$

Esta nova equação admite solução se $mdc(30, 42, 70, 105) \mid 15 + 26t_0$. Como $mdc(30, 42, 70, 105) = 1$, a solução pode ser explicitada para qualquer valor t_0. Nesse sentido, podemos considerar

$$p^{(2)} = 30x + 42y + 70z.$$

e proceder como feito no início, de forma que reduzimos a equação de quatro variáveis a uma resolvível de apenas duas. Logo, são soluções da obtida

$$p^{(2)} = -90 + 26t_0 + 105t_1 \qquad u = 1 - t_1, \qquad t_1 \in \mathbb{Z}.$$

Resolveremos agora

$$30x + 42y + 70z = -90 + 26t_0 + 105t_1.$$

Temos que $mdc(30, 42, 70) = 2$ e, para exibirmos uma solução, o lado esquerdo da igualdade deve ser par. Como $2 \mid 90$ e $2 \mid 26t$, devemos apenas determinar um valor para t_1 de modo que a condição seja satisfeita. Assim, t_1 deve ser par, ou seja, $t_1 = 2k, \ \ k \in \mathbb{Z}$. Repare que agora $u = 1 - 2k$. Segue então que a nova equação sempre admite solução

$$30x + 42y + 70z = -90 + 26t_0 + 210k.$$

Por fim, considerando

$$p^{(3)} = 30x + 42y,$$

temos que

$$p^{(3)} + 70z = -90 + 26t_0 + 210k,$$

cujas soluções são

$$p^{(3)} = -160 + 26t_0 + 210k + 70t_2 \qquad z = 1 - t_2, \qquad t_2 \in \mathbb{Z}.$$

Determinado o valor de z, resta apenas resolver a equação

$$30x + 42y = -160 + 26t_0 + 210k + 70t_2.$$

Como $mdc(30, 42) = 6$, devemos escolher um número inteiro t_2 de forma que aconteça $6 \mid -160 + 26t_0 + 210k + 70t_2$. Para que essa condição aconteça, é necessário que $6 \mid 2 + 2t_0 + 4t_2$. Isso implica que podemos tomar $t_2 = t_0 + 1$. Assim devemos modificar o valor de z obtido anteriormente e calcular a solução de

$$30x + 42y = -90 + 96t_0 + 210k.$$

Ora, a equação acima é equivalente a

$$5x + 7y = -15 + 16t_0 + 35k.$$

Como $1 = 5(3) + 7(-2)$, logo

$$5(-45 + 48t_0 + 105k) + 7(30 - 32t_0 - 70k) = -15 + 16t_0 + 35k$$

e, portanto, são soluções particulares dessa equação

$$x_0 = -45 + 48t_0 + 105k \qquad y_0 = 30 - 32t_0 - 70k.$$

Assim, as soluções gerais são

$$x = -45 + 48t_0 + 105k + 7t_3 \qquad y = 30 - 32t_0 - 70k - 5t_3, \qquad t_3 \in \mathbb{Z}.$$

Em suma, os valores obtidos para cada variável podem ser organizados como segue:

$$\begin{cases} x = -45 + 48t_0 + 105k + 7t_3 \\ y = 30 - 32t_0 - 70k - 5t_3 \\ z = -t_0 \\ u = 1 - 2k \\ v = 1 - t_0 \end{cases}$$

□

A partir do exemplo é possível compreender o processo de solução de uma equação com um número qualquer de variáveis. De modo geral, consideremos a equação diofantina solucionável

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n = k.$$

Tome $p^{(1)} = a_1x_1 + ... + a_{n-1}x_{n-1}$. Assim, a equação acima pode ser representada por

$$p^{(1)} + a_nx_n = k.$$

A nova equação admite solução pois $mdc(1, a_n) = 1$ e k é múltiplo de 1. A solução geral é da forma

$$\begin{aligned} p^{(1)} &= p_1 + a_nt_1 \\ x_n &= x'_n - t_1, \qquad\qquad t_1 \in \mathbb{Z} \end{aligned}$$

com p_1, x'_n uma solução particular.

Observe que determinamos o valor da última incógnita. Agora devemos resolver a equação $p^{(1)} = p_1 + a_nt_1$. Podemos reescrever essa expressão como

$$a_1x_1 + a_2x_2 + ... + a_{n-1}x_{n-1} = p_1 + a_nt_1.$$

Esta última equação só admite solução se $mdc(a_1, a_2, ..., a_{n-1}) \mid p_1 + a_nt_1$. Logo, devemos escolher um valor para t_1 de modo que a condição seja satisfeita. Consideremos então $t_1 = t'_1$ de modo que $mdc(a_1, a_2, ..., a_{n-1}) \mid p_1 + a_nt'_1$. Uma observação importante é que, quando determinamos o valor de t_1 como t'_1, a variável x_n será escrita em função do valor determinado, ou seja, $x_n = x'_n - t'_1$. Na verdade, devemos ter $t'_1 = mdc(a_1, ..., a_{n-1})q_1 + r1$, com $0 \leq r_1 < mdc(a_1, ..., a_{n-1})$, r_1 um valor inteiro

determinado e q_1 um inteiro qualquer. Na sequência obtemos:

$$a_1x_1 + a_2x_2 + ... + a_{n-1}x_{n-1} = l_1 + a_n mdc(a_1, ..., a_{n-1})q_1; \qquad l_1 = p_1 + a_n r_1$$

Procedendo de maneira análoga ao passo descrito anteriormente, consideremos $p^{(2)} = a_1x_1 + ... + a_{n-2}x_{n-2}$. Logo,

$$p^{(2)} + a_{n-1}x_{n-1} = l_1 + a_n mdc(a_1, ..., a_{n-1})q_1.$$

Novamente a equação possui solução, uma vez que $mdc(1, a_{n-1}) = 1$. Como esta possui duas variáveis, as soluções são da forma

$$\begin{aligned} p^{(2)} &= p_2 + a_{n-1}t_2 \\ x_{n-1} &= x'_{n-1} - t_2, \qquad\qquad t_2 \in \mathbb{Z} \end{aligned}$$

Observe que determinamos o valor da incógnita de índice $n-1$. Deve-se agora resolver a seguinte igualdade:

$$a_1x_1 + a_2x_2 + ... + a_{n-2}x_{n-2} = p_2 + a_{n-1}t_2$$

Devemos mais uma vez analisar se a equação tem solução. Para que esta possua solução, $mdc(a_1, ..., a_{n-2}) \mid p_2 + a_{n-1}t_2$. Assim, tome um valor para t_2, digamos $t'2$, de tal forma que $t'_2 = mdc(a_1, ..., a_{n-2})q_2 + r_2$, com $0 \leq r_1 < mdc(a_1, ..., a_{n-2})$. Substituindo t'_2 na equação que pretendemos resolver, obtemos

$$a_1x_1 + a_2x_2 + ... + a_{n-2}x_{n-2} = l_2 + a_{n-1}mdc(a_1, ..., a_{n-2})q_2; \qquad l_2 = p_2 + a_{n-1}r_2.$$

Basta agora tomarmos $p^{(3)} = a_1 + a_2 + ... + a_{n-3}$ e procedermos como anteriormente.

Em suma, o método consiste em repetirmos o primeiro passo $n-2$ vezes, determinando os valores das incógnitas x_i, $\quad i = 3, ..., n$, e, a partir do segundo passo é necessário determinarmos os valores de t_{i-1} para que $mdc(a_1, ..., a_{n-i}) \mid p_i + a_{n-i+1}t_i$, com $1 \leq i \leq n-1$. Dessa forma chegaremos em uma equação do tipo

$$a_1x_1 + a_2x_2 = l_{n-3} + a_3 mdc(a_1, a_2, a_3)q_{n-3}; \qquad l_{n-3} = p_{n-3} + a_3 r_{n-3},$$

com r_{n-3} determinado no passo anterior. Dessa forma, basta solucionarmos essa última equação que obteremos valores de x_1 e x_2, que são respectivamente

$$\begin{aligned} x_1 &= x'_1 + \frac{a_2}{mdc(a,b)}t_{n-1} \\ x_2 &= x'_2 - \frac{a_1}{mdc(a,b)}t_{n-1}, \qquad\qquad t_{n-1} \in \mathbb{Z} \end{aligned}$$

Nesse sentido, a solução geral é da seguinte forma

$$\begin{cases} x_1 = x'_1 + \dfrac{a_2}{mdc(a,b)} t_{n-1} \\ x_2 = x'_2 - \dfrac{a_1}{mdc(a,b)} t_{n-1} \\ x_3 = x'_3 - t'_{n-2} \\ \vdots \\ x_n = x'_n - t'_1 \end{cases}$$

com $t'_i = mdc(a_1, a_2, ..., a_n - i)q_i + r_i$.

Capítulo 4

Aplicações: problemas clássicos

4.1 O problema do troco de Frobênius

Ferdinand Georg Frobênius (1849 - 1917) foi um destacado matemático alemão. Estudou por um ano na Universidade de Göttingen e retornou (1868) para sua cidade natal para continuar na Universidade de Berlim. Em Berlim foi orientado em seu doutorado por Weierstrass, um dos membros do corpo docente da tal universidade. Seus principais trabalhos publicados são relativos a teoria e a representação de grupos, como Über Gruppen von vertauschbaren Elementen (1879), produzido juntamente com Stickelberger, um colega de Zürique.

Figura 2: Ferdinand Georg Frobênius

Fonte: *http://www.learn-math.info/portugal/historyDetail.htm?id=Frobenius*

Este famoso matemático propôs um problema, conhecido como *"Frobenius coin problem"*, ou problema do troco de Frobênius, cujo enunciado é de fácil entendimento. Imagine que você necessite sacar dinheiro em um caixa eletrônico que fornece apenas cédulas de 2 e 5 reais. Considerando que existem infinitas cédulas desses tipos nesse caixa, qual a maior quantia que você não poderá sacar? Percebemos que existem quantias que

não podemos sacar, como por exemplo as quantias 1 e 3.

De uma forma geral, o problema de Frobênius pode ser enunciado como segue:

Problema de Frobênius: *Encontre a maior quantia que não pode ser paga com moedas de valores* $a_1, a_2, ..., a_n$ *de forma que* $mdc(a_1, a_2, ..., a_n) = 1$.

Equivalentemente, podemos enunciá-lo da seguinte forma:

Para quaisquer inteiros positivos $a_1, a_2, ..., a_n$ *que satisfaçam* $mdc(a_1, a_2, ..., a_n) = 1$, *determine* $g = g(a_1, a_2, ..., a_n)$, *sendo este o maior inteiro positivo tal que a equação*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = N$$

, *com* $N \in \mathbb{Z}$ *não possui solução inteira negativa, ou seja,* $x_i \geq 0$, $\forall i = 1, ...n$.

O número g, que designamos por $g(a_1, ..., a_n)$, é chamado número de Frobênius do conjunto $(a_1, ..., a_n)$.

4.1.1 O problema em duas variáveis

Trataremos aqui o problema do troco para $n = 2$. Para isso, considere o seguinte enunciado:

Imagine que você está em um país que a moeda oficial é composta por apenas dois valores, digamos a, b. *Consideremos também que esses valores são primos entre si. Qual a maior quantia que não pode ser paga utilizando as respectivas moedas?*

Para determinarmos a quantia procurada, ou seja, o número de Frobênius, necessitaremos de alguns resultados que enunciamos e demonstramos na sequência:

Proposição 4.1.1. *Seja* $a, b \in \mathbb{N}$. *Todo número inteiro* c *pode ser escrito de modo único da seguinte forma:*

$$ma + nb = c, \text{ com } 0 \leq n < b \text{ e } n \in \mathbb{Z}.$$

Demonstração. Pelo teorema de Bachet-Bezout, sabemos que existem inteiros u, v que satisfazem a igualdade

$$ua + vb = mdc(a, b) = 1$$

Multiplicando a igualdade por um número inteiro c, obtemos

$$auc + vbc = c.$$

Pela divisão euclidiana, existem $q, m \in \mathbb{Z}$ tais que $uc = qb + m$, $0 \leq m < b$. Segue então que

$$a(qb + m) + vbc = c \Rightarrow ma + (aq + vc)b = c \Rightarrow ma + nb = c,$$

com $n = qa + vc \in \mathbb{Z}$.

Para provar a unicidade, suponhamos que existam m', n', tais que

$$ma + nb = m'a + n'b, \qquad 0 \leq m, m' < b$$

Decorre então que $(m - m')a = (n' - n)b$, com $|m - m'| < b$. Como $mdc(a, b) = 1$, necessariamente $b \mid m - m'$. Logo $m = m'$. □

Consideremos o conjunto

$$C = \{ax + by; \quad x, y \in \mathbb{N}\}$$

A próxima proposição caracteriza os elementos do conjunto C.

Proposição 4.1.2. *Um certo $c \in C$ se, e somente se, existem inteiros únicos $m, n \in \mathbb{N}$, $m < b$ tal que $c = ma + nb$*

Demonstração. Se $c = ma + nb$, $m, n \in \mathbb{N}$, $c \in C$. Por outro lado, se $c \in C$, existem $x, y \in \mathbb{N}$ tal que

$$c = ax + by.$$

Pela divisão euclidiana, temos $x = bq + m$ com $0 \leq m < b$, logo

$$c = a(bq + m) + by \Rightarrow c = am + b(aq + y).$$

Tomando $n = aq + y$, que pertence a $\mathbb{N}$, obtemos $c = am + bn$.

É verdade que m e n são únicos. Este resultado deriva da proposição anterior. □

Nesse sentido, vamos definir $L = \mathbb{N} - C$. É fácil ver que

$$L = \{ma - nb; \quad m, n \in \mathbb{N}, \quad m < b\}.$$

Para verificar essa afirmação, consideremos $l \in L$. Repare que l não pode ser escrito da forma $ma + nb$, ou seja, não existem $m, n \in \mathbb{N} \cup 0$ tais que $l = ma + nb$. Se m, n fossem determinados então $l \in C$, que é absurdo. Contudo, a proposição 4.1.1 garante que existe um número inteiro, tal que $l = ma + n'b$. Tome então $n' = -n$, $n \in \mathbb{Z}$. Assim, $l = ma - nb$.

A partir destes resultados, podemos começar a discutir a questão levantada por Frobênius. Vemos que, para expressarmos uma solução da equação que determina as

quantias que se podem obter neste país, $ax + by = c$, devemos obter o número de cédulas dos valores a e b, ou seja, os valores x e y. É claro que estes serão naturais e também que, as quantias de dinheiro que podem ser pagas devem pertencer ao conjunto C.

Teorema 4.1.3. *A equação $ax + by = c$, com $mdc(a, b) = 1$ tem solução conjunto dos naturais se, e somente se, $c \notin L$.*

Demonstração. É fato que a equação $ax+by = c$ admite solução nos naturais se, e somente se, $c \in C$. Logo, como $L = \mathbb{N} - C$, $c \notin L$. □

Sendo assim, o próximo corolário responde a questão levantada no início.

Corolário 4.1.4. *O número de Frobênius para o caso em que $n = 2$ é expresso por*

$$g(a, b) = ab - a - b$$

Demonstração. O conjunto que definimos como L é finito diante do fato de que ele é limitado. Observemos que o maior valor contido em L ocorre quando $m = b - 1$ e $n = 1$. Assim,

$$maxL = (b - 1)a - b = ab - a - b.$$

Como $maxL = g(a, b)$, portanto $g(a, b) = ab - a - b$. □

Exemplo 4.1.1. Suponha que em certo país as cédulas possuem valores $F_1, F_2, ..., F_{12}$, sendo estes termos da sequência de Fibonacci. Qual a maior quantia que não podemos sacar de um caixa eletrônico desse país utilizando apenas as cédulas F_{11} e F_{12}?

Solução. Sabemos que $F_{11} = 89$ e $F_{12} = 144$. Logo, a equação que determina as quantias que podem ser pagas com estas células é

$$89x + 144y = c.$$

Basta agora determinarmos $g(89, 144)$.

$$g(89, 144) = 84.144 - 89 - 144 = 12583.$$

□

4.1.2 Solução de uma equação diofantina em $\mathbb{N}$

No problema de Frobênius, temos que a solução da equação que determina o valor de c deve ter soluções naturais, uma vez que as incógnitas, que representam o número de cédulas para cada um dos valores, devem ser positivas ou iguais a zero. Assim como neste problema, existem muitos outros envolvendo equações diofantinas que necessitam

que suas soluções pertençam ao conjunto dos naturais. Nesse sentido, mostraremos como determinar as tais soluções

Em suma, é fácil determinar se a equação $ax + by = c$ possui solução no conjunto dos naturais e, se possui, qual é o formato dessa solução. Se $mdc(a, b) \nmid c$, a equação não possui solução inteira, logo não tem solução natural. Se $mdc(a, b) \mid c$, podemos tomar uma outra equação da forma $Ax+By = C$, com $A = \dfrac{a}{mdc(a,b)}$, $B = \dfrac{b}{mdc(a,b)}$, $C = \dfrac{c}{mdc(a,b)}$. Observe que $mdc(A, B) = 1$. Pelo algoritmo de Euclides, escreva

$$1 = mdc(A, B) = m'A - n'B$$

donde segue que,

$$C = cm'A - cn'B.$$

Pela divisão euclidiana, tome $cm' = qB + m$ com $m < B$. Substituindo este valor na equação anterior obtemos

$$C = (qB + m)A - cn'B = mA + (qA - cn')B.$$

Veja que temos dois casos, se $qA - cn' \geq 0$ e $qA - cn' < 0$. Assim,

$$c = \begin{cases} mA + (qA - cn')B \in C, & se \;\; qA \geq cn' \\ mA - (cn' - qA)B \in L, & se \;\; qA < cn \end{cases}$$

No primeiro caso, a equação admite solução. Definimos então a solução minimal m, n da equação $Ax + By = C$, $m < b$, como sendo a única solução tal que se par de números naturais x, y é solução da equação, então $x \geq m$. Desse modo, enunciamos o seguinte resultado.

Proposição 4.1.5. *Considere a equação $Ax + By = C$, que possui solução natural e $mdc(A, B) = 1$. Seja $x_0 = m$ e $y_0 = n$ a solução minimal. As soluções x, y da equação são dadas por*

$$x = m + tb \qquad y = n - ta, \qquad t \in \mathbb{N}, \;\; n - ta \geq 0.$$

4.2 Outros problemas

Equações diofantinas lineares podem ser aplicadas em várias situações do cotidiano. Diante desse fato, abordaremos nesta seção algumas aplicações. Apresentaremos aqui problemas clássicos, presentes em [3], [5], [6] e [7], mas que consideramos interessantes e que destacam o procedimento de resolução desse tipo de equação.

Problema 1. Em um pátio do DETRAN, sabe-se que há 400 pneus retirados de carros

e motos que foram apreendidos no mês de Setembro. Quantos veículos de cada categoria foram apreendidos sabendo que a diferença entre os dois números é a menor possível?

Solução. Seja C o número de carros e M o número de motos presentes neste pátio. Sabemos que cada carro possui quatro pneus e cada moto, dois pneus. Deste modo o problema pode ser representado pela equação

$$4C + 2M = 400$$

.

Observe que essa equação possui solução pois $mdc(4, 2) \mid 400$. A mesma pode ser reescrita como

$$2C + M = 200$$

Procuremos agora uma solução particular c_0, m_0 para essa equação. Por um lado, temos que $1 = 2 - 1$. Multiplicando a igualdade por 200, segue que

$$200 = 2(200) + 1(-200) = 2(75) + 1(50).$$

Assim $c_0 = 50$ e $m_0 = 100$, são soluções particulares da equação. Diante disso temos que as soluções da equação diofantina são $C = 50 + t$ e $M = 100 - 2t$, com $t \in \mathbb{Z}$.

Sabe-se que $C > 0$ e $M > 0$, o que implica em $-50 < t < 50$. Também, a diferença entre o número de carros e o número de motos podem ser expressa por

$$C - M = -50 + 3t$$

.

Como $-50 = 3(-17) + 1$, devemos ter $t = 17$, para que a diferença $C - G$ seja a menor possível. Assim, o número de carros no pátio (C) é 67 e o número de motos (M) é 66. □

Problema 2. (Proposto por Euler) Uma pessoa comprou cavalos e bois. Foram pagos 31 escudos[1] por cavalo e 20 escudos por boi e sabe-se que todos os cavalos custaram 7 escudos a menos do que todos os bois. Quantos cavalos e quantos bois foram comprados?

Solução. Seja C o número de cavalos, B o número de bois e P o preço pago pela pessoa. Sabemos que a diferença entre preços de bois e cavalos é 7 escudos. Assim,

$$20B - 31C = 7$$

[1] As primeiras moedas cunhadas no Brasil com a figura do rei numa das faces e com as armas da Coroa Portuguesa na outra ficaram conhecidas como série dos escudos. Um escudo equivalia a 1600 réis. *Banco Central do Brasil (2004)- pág. 12*

Observemos que $mdc(20,-31) = mdc(20,31) = 1$, logo a equação acima tem solução. Vamos determinar uma solução particular. Pelo algoritmo de Euclides, temos que

$$\begin{aligned} 31 &= 20+11 \\ 20 &= 11+9 \\ 11 &= 9+2 \\ 9 &= 2(4)+1 \end{aligned}$$

Isolando os restos do algoritmo e fazendo as substituições convenientes, obtemos

$$\begin{aligned} 1 &= 9-2(4) = 9-4(11-9) = (5)9-(4)11 = (5)(20-11)-(4)11 = \\ &= (5)20-(9)11 = (5)20-9(31-20) = (14)20-(9)31 \end{aligned}$$

Multiplicando a ultima expressão por 7, tem-se $(98)20-(63)31 = 7$.

Como $63 = 3.20+3$, podemos reescrever a igualdade como $(5)20-(3)31 = 7$.

Portanto, $B_0 = 5$ e $C_0 = 3$ é uma solução particular (e minimal) da equação diofantina que representa a diferença entre os preços dos animais. Assim, pela teoria desenvolvida até aqui, a solução geral pode ser expressa pelo conjunto

$$S = \{(5+31t, 3+20t) \mid t \in \mathbb{Z}\}$$

Contudo, B e C são positivos, ou seja, $5+31t > 0$ e $3+20t > 0$

Dessas desigualdades, como t é um número inteiro, segue que $t \geq 0$. Assim, para cada valor de t teremos o número de cavalos e bois que foram comprados, como vemos na tabela a seguir:

Tabela 4.1: Número de animais comprados

t	**B**	**C**
0	5	3
1	36	23
2	67	43
3	98	63
4	129	83
5	160	93
6	191	103
$\vdots$	$\vdots$	$\vdots$
n	$5+31n$	$3+20n$

□

Problema 3. (Problema do século XVI) Um total de 41 pessoas entre homens, mulheres e crianças foram a um banquete e juntos gastaram 40 patacas[2]. Cada homem pagou 4 patacas, cada mulher 3 patacas e cada criança um terço de pataca. Quantos homens, quantas mulheres e quantas crianças havia no banquete?

Solução. Consideremos as seguintes equações que modelam o problema:

$$\begin{aligned} H + M + C &= 41 \\ 4H + 3M + \frac{1}{3}C &= 40 \end{aligned}$$

Multiplicando a segunda equação por 3, obtemos $12H + 9M + C = 120$. Contudo, utilizando a primeira equação, obtemos uma equação diofantina de duas variáveis, como segue

$$11H + 8M + (H + M + C) = 11H + 8M + 41 = 120 \Leftrightarrow 11H + 8M = 79$$

Como $mdc(11, 8) = 1$, logo $mdc(11, 8) \mid 79$, e, portanto, a equação tem solução. Pelo algoritmo de Euclides, segue que

$$\begin{aligned} 11 &= 8 + 3 \\ 8 &= 3(2) + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Assim, isolando os restos e fazendo as devidas substituições obtém-se

$$1 = 11(3) + 8(-4).$$

Multiplicado a equação acima por 79 e aplicando o algoritmo da divisão obtemos uma solução particular (e minimal) $H_0 = 5, M_0 = 3$.

$$79 = 11(237) + 8(-316) = 11(8.29 + 5) + 8(-316) = 11(5) + 8(3)$$

Logo, o conjunto solução da equação inicial é dado por

$$S = \{(5 + 8t, 3 - 11t) \mid t \in \mathbb{Z}\}.$$

É fato que

$$5 + 8t > 0 \qquad \text{e} \qquad 3 - 11t > 0.$$

[2]As patacas foram as moedas que circularam por mais tempo no Brasil, de 1695 a 1834. Essa série era composta pelas moedas de prata nos valores de 20, 40, 80, 160, 320 e 640 réis. O valor de 320 réis - pataca - deu nome à série.*Banco Central do Brasil (2004)- pág. 10*

Daí segue que $\frac{-5}{8} < t < \frac{3}{11}$. Como t é inteiro, o único valor possível é $t = 0$. Sendo assim, o número de homens e mulheres presentes no banquete é 5 e 3. Logo o número de crianças é $C = 41 - 8 - 3 = 30$. □

Problema 4. Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas maçãs tinha cada monte?

Solução. Seja m a quantidade de maçãs. Observemos que, inicialmente, m foi dividida em 37 montes, ou seja,

$$m = 37y,$$

com y sendo o número de maçãs em cada monte. Por outro lado, se forem retiradas do total 17 frutas, o restante pode ser acondicionado em 79 caixas, ou seja,

$$m - 17 = 79z,$$

sendo z o número de maçãs dentro de cada caixa. Substituindo o valor de m da primeira igualdade na segunda obtemos

$$37y - 79z = 17.$$

Basta agora calcularmos a solução para esta equação, uma vez que ela admite solução já que $mdc(37, 79) = 1$. Nesse sentido, temos, pelo algoritmo de euclides, que

$$\begin{aligned} 79 &= 37(2) + 5 \\ 37 &= 5(7) + 2 \\ 5 &= 2(2) + 1 \end{aligned}$$

Assim,

$$1 = 5-2(2) = 5-2(37-5(7)) = 5(15)-37(2) = (79-37(2))(15)-37(2) = (-32)37-(-15)79$$

Multiplicando a igualdade acima por 17 e aplicando a divisão euclidiana, obtemos

$$(-544)37 - (-255)79 = ((-7)79 + 9)37 - (-255)79 = (9)37 - (4)79.$$

Dessa forma, encontramos a solução minimal $y_0 = 9$ e $z_0 = 4$. Assim a solução geral é dada por

$$S = \{(9 - 79t, 4 - 37t) \mid t \in \mathbb{N}\}.$$

O único valor possível de t é 0. Portanto, em cada monte foram colocadas 9 maçãs e em cada caixa, 4 maçãs. □

Problema 5. Um parque de diversão cobra $U\$1,00$ a entrada de crianças e $U\$3,00$ a de adultos. Para que a arrecadação de um dia seja $U\$200,00$, qual o maior número de pessoas, entre adultos e crianças, que poderiam frequentar o parque neste dia? Quantas crianças e quantos adultos?

Solução. Consideremos c o número de crianças e a o de adultos. Como cada criança paga $U\$1,00$, cada adulto $U\$3,00$ e o total faturado foi de $U\$200,00$, a equação que modela o problema é

$$1c + 3a = 200.$$

Sabemos que

$$1 = (-2) + 3(1)$$

então, multiplicando a equação anterior por 200 obtemos

$$200 = -400 + 3(200).$$

Pelo algoritmo de Euclides, temos que $-400 = 3(-134) + 2$. Assim,

$$200 = 3(-134) + 2 + 3(200) = 2 + 3(66).$$

Logo, $c_0 = 2$ e $a_0 = 66$ é uma solução particular (também minimal) da equação dada inicialmente. Assim a solução geral pode ser expressa por

$$S = \{(2 + 3t, 66 - t) \mid t \in \mathbb{N} \cup \{0\}\}.$$

Como $2 + 3t > 0$ e $66 - t > 0$, então $1 < t < 66$. Queremos o número máximo de pessoas, então consideramos o valor máximo que t pode assumir. Assim $t = 65$. Dessa forma o número de crianças presentes no parque é 197 e de adultos é 2. □

Problema 6. De quantas maneiras podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?

Solução. Seja x o número de selos de cinco reais e y o número de selos de sete reais. Como deve-se gastar cem reais, então

$$5x + 7y = 100.$$

Sabemos que $1 = 5(3) + 7(-2)$, logo

$$5(300) + 7(-200) = 100$$

Pela divisão euclidiana, $300 = 7(42) + 6$, assim,

$$5(7(42) + 6) + 7(-200) = 5(6) + 7(10)$$

ou seja, $x_0 = 6$ e $y_0 = 10$ é uma solução minimal. Dessa forma, a solução geral é expressa por

$$S = \{(6 + 7t, 10 - 5t) \mid t \in \mathbb{N}\}.$$

Observemos que $6 + 7t > 0$ e $10 - 5t > 0$. Isso implica em $0 < t < 2$. Logo o único valor possível é $t = 1$ e, dessa forma, há somente uma maneira de comprar esses tipos de selo com cem reais. Utilizando o valor encontrado de t concluímos que foram comprados 13 selos de cinco reais e 5 de sete reais. □

Capítulo 5

Considerações Finais

De modo geral, apresentamos neste trabalho um estudo sobre Equações Diofantinas Lineares. Buscamos, através das pesquisas nas bibliografias, reunir os mais diversos resultados a fim de desenvolver um material completo. Inicialmente estudamos de forma detalhada o máximo divisor comum em conjunto com o algoritmo de Euclides, uma vez que esses conceitos são os pilares para a resolução dessas equações. Nesse meio, buscamos generalizar os resultados. Após os resultados obtidos, partimos para o estudo das equações pretendidas.

Para o desenvolvimento da teoria sobre equações diofantinas, consideramos inicialmente as equações de duas variáveis. Estudamos as condições de existência e o formato de suas soluções. Após, abordamos as de três variáveis e, em seguida, generalizamos o método de resolução de uma equação de n variáveis. Ademais, no intuito de destacarmos a aplicabilidade desse tipo de equação, foram resolvidos alguns problemas que chamam a atenção por se referirem a situações do cotidiano.

Por fim, tendo em vista todo o conteúdo abordado aqui, o presente trabalho pode servir como um material complementar para o curso de "Teoria dos Números". Diante das consultas bibliográficas, percebemos que as bibliografias referentes ao ensino sobre esse tópico, destinados aos cursos de graduação, não apresentam todos os resultados que foram apresentados. Um exemplo disso é o método de solução das equações diofantinas com quaisquer número de variável. Nesse sentido, deixamos a cargo do professor adaptar o material.

Referências e bibliografias consultadas

[1] ANDREESCU, T. et al. **An Introduction to Diophantine Equations: A Problem-Based Approach**- New York: Birkhäuser Mathematics, 2010.

[2] BOYER, C. B. **História da Matemática**; tradução Elza F. Gomide- 2ª ed.-São Paulo: EDGARD BLUCHERLTDA, 1996.

[3] BRASIL, Banco Central. **Dinheiro no Brasil / Banco Central do Brasil.** - 2ª ed. - Brasília : BCB, 2004.

[4] DOMINGUES, H. H. **Fundamentos de Aritmética**- 1ª ed.-São Paulo: Atual Editora LTDA, 1991.

[5] EVES, H. **Introdução à História da Matemática**- 1ª ed.- Campinas, SP: EDITORA UNICAMP, 2007.

[6] GONDIM, R. et al. **Aritmética Linear**- Recife: UFREB, 2012.

[7] HEFES, A. **Aritmética**- Coleção PROFMAT- 1ª ed.- Rio de Janeiro: SBM, 2014.

[8] HEFES, A. **Iniciação a Aritmética**- 1ª ed.- Rio de Janeiro: IMPA, 2015.

[9] MARTINEZ, F. B. et al. **Teoria dos Números: Um Passeio com Primos e outros Números Familiares pelo Mundo Inteiro**- 4ª ed- Rio de Janeiro: IMPA, 2015.

[10] MILIES, F.C.P. **Uma introdução à Matemática**- 3ª ed.- São Paulo: Editora da Universidade de São Paulo, 2001.

[11] ROQUE, T. **História da matemática: Uma visão crítica, desfazendo mitos e lendas**- 1ª ed.- Rio de Janeiro: Editora Zahar, 2012.

[12] SANTOS, J. P. O. **Introdução à Teoria dos Números**- 3ª ed- Rio de Janeiro: IMPA, 2007.

[13] http://www.dec.ufcg.edu.br/biografias/FerdGFro.html <Acesso em 26/10/2017 às 14h37min.>