Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Equações Diofantinas: uma abordagem para o Ensino Médio

Rildo Ribeiro

Brasília

2014

Rildo Ribeiro

Equações Diofantinas: uma abordagem para o Ensino Médio

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos do "Programa" de Mestrado Profissional em Matemática em rede Nacional - PROFMAT, para obtenção do grau de MESTRE.

Orientador: Professor Doutor Rui Seimetz

Brasília

2014

Ficha catalográfica elaborada pela Biblioteca Central da Universidade de Brasília. Acervo 1016194.

Ribeiro, Rildo.
R484e Equações Diofantinas : uma abordagem para o Ensino Médio / Rildo Ribeiro. -- 2014.
43 f. ; 30 cm.

Dissertação (mestrado) - Universidade de Brasília, Departamento de Matemática, "Programa" de Mestrado Profissional em Matemática em Rede Nacional, 2014.
Inclui bibliografia.
Orientação: Rui Seimetz.

1. Teoria dos números. 2. Equações diofantinas. 3. Matemática - Problemas, exercícios, etc. 4. Matemática - Estudo e ensino. I. Seimetz, Rui. II. Título.

CDU 511.5

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Equações Diofantinas
Uma abordagem para o Ensino Médio.

por

Rildo Ribeiro*

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 05 de junho de 2014.

Comissão Examinadora:

Prof. Dr. Rui Seimetz – MAT/UnB (Orientador)

Prof. Dr. Ricardo Nunes de Oliveira – MAT/UFG

Prof. Dr. Hélder de Carvalho Matos – MAT/UnB

* O autor foi bolsista CAPES durante a elaboração desta dissertação.

Este trabalho é dedicado às crianças adultas que, quando pequenas, sonharam em se tornar cientistas.

Agradecimentos

Agradeço, primeiramente à Deus que me deu sabedoria e o gosto pela bela Matemática.

Agradeço, também, aos meus pais, Gabriel e Conceição, que me acompanharam nos momentos de estudos, me apoiaram e me deram condições para que o meu objetivo fosse alcançado.

À minha Esposa Rosilene, que me incentivou a fazer a prova de seleção para o PROFMAT e, que nos momentos de desânimo me apoiou e me deu forças para prosseguir.

Aos meus filhos Rildo, Tiago, Bruno, Brenda e Breno que sentiram minha ausência nesse período, mas me encorajaram e me incentivaram orgulhosos de terem um pai mestre.

Aos meus netos Ryan e Ruan que, ainda bebês, nem perceberam o que se passava. Agora, porém, me sentirão mais presente em suas vidas.

À Helen e Conrado, diretora e vice-diretor do Centro de Ensino Médio 10 de Ceilândia, e à Maria Clotilde, vice-diretora do Colégio Marista João Paulo II, por colaborarem nessa jornada.

Aos colegas de trabalho do Colégio Marista João Paulo II, especialmente, Renato Miletti, Débora Aguiar e Eurípedes Braga, que aguentaram minha angústia nos momentos mais difíceis e que com seu incentivo tornaram essa jornada menos árdua.

Às Coordenações da Sociedade Brasileira de Matemática - SBM, do Programa de Mestrado Profissional em Matemática - PROFMAT e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES que viabilizaram pedagogicamente e financeiramente esse projeto. Espero que o exemplo PROFMAT possa, em breve, ser extendido às demais áreas do conhecimento cintífico.

Ao Departamento de Matemática da Universidade de Brasília pela ousadia em admitir um projeto vanguardista como o Programa de Mestrado Profissional em Matemática - PROFMAT e, também, pelos excelentes professores que muito me ensinaram durante minha permanência no Mestrado.

Aos meus colegas de turma que estiveram sempre presentes. Em mais de 2 anos de convivência, contribuíram com dicas e exeperiências de vida para que eu pudesse chegar até o final.

Agradecimento especial ao Professor Lineu da Costa Araújo Neto que muito contribuiu com seus ensinamentos e orientações para o trabalho final. Além de professor, se revelou uma grande pessoa.

Ao professor, orientador e amigo Rui Seimetz que com suas dicas, broncas e carinho me fizeram passar por mais essa etapa acadêmica, um agradecimento mais que especial.

Obrigado, também, àqueles que, também, contribuíram nessa caminhada e não tiveram seus nomes citados. A eles minhas sinceras desculpas.

"Uma grande descoberta envolve a solução de um grande problema, mas há uma semente de descoberta na solução de qualquer problema. Seu problema pode ser modesto; porém, se ele desafiar sua curiosidade e fizer funcionar sua capacidade inventiva, e caso você o resolva sozinho, então você poderá experimentar a tensão e o prazer do triunfo da descoberta."

George Polya

Resumo

O presente trabalho tem como objetivo principal instrumentalizar estudantes e professores para a compreensão e a resolução de problemas que possam ser resolvidos usando-se as Equações Diofantinas com duas ou mais incógnitas. Para isso, foram usadas técnicas como os processos de fatoração e o uso de inequações, que são conteúdos estudados pelos professores do Ensino Fundamental e Médio. Utilizou-se, para isso a apresentação de vários problemas resolvidos para servirem de objeto de estudo por professores e alunos. É apresentada, também, uma introdução à Teoria dos Números, para uma melhor compreensão da resolução das Equações Diofantinas Lineares por meio de exemplos lúdicos e didáticos que estimulam o prazer de estudar Matemática. A conclusão desse trabalho enfatiza a importância da interpretação algébrica e geométrica das Equações Diofantinas Lineares. Ressalta ainda, que a introdução à resolução de problemas dessa área não necessita de conhecimentos avançados, podendo, então, ser feito no Ensino Médio, propiciando, assim, ao estudante o desenvolvimento de suas habilidades de raciocínio.

Palavras-chaves: Teoria dos Números. Equações Diofantinas. Fatoração. Inequações. Resolução de problemas.

Abstract

The main object of the present work aims to equip students and teachers for the understanding and the solution of problems that can be solved by using the Diophantine equations with two or more unknowns. Techniques of factoring and using of inequalities were used as contents studied by teachers in elementary and high school. For this study, it was used the presentation of several issues solved to serve as an object of study for teachers and students. It also presents an introduction to the Theory of Numbers, for a better understanding of the resolution of linear Diophantine equations using it for ludic and educational examples that stimulate the pleasant in mathematics studies. The conclusion of this study emphasizes the importance of algebraic and geometric interpretation of linear Diophantine equations. It also highlights that the introduction of solving problems in this area does not need advanced knowledge, which can be done in high school, allowing students to develop their reasoning skills.

Key-words: Theory of Numbers. Diophantine equations. Factoring. Inequalities. Solution of problems.

Lista de ilustrações

Lista de símbolos

Δ	Letra grega maiúscula Delta
ζ	Letra grega minúscula Zeta
$\in$	Pertence
$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Z}^*$	Conjunto dos Números Inteiros Não Nulos

Sumário

Introdução

A busca por soluções de equações com soluções inteiras foi, e continua sendo, um problema de grande interesse para os matemáticos.

Neste trabalho, apresenta-se um pouco do histórico dessas equações denominadas Equações Diofantinas, em homenagem a Diofanto de Alexandria, matemático pouco conhecido, mas que com seu livro Aritmética, ou melhor parte dele, pois se conhece apenas um percentual coleção, introduziu o uso de símbolos na resolução de equações.

No primeiro capítulo apresenta-se uma referência histórica de Diofanto de Alexandria.

No capítulo 2, há uma breve introdução à Teoria Elementar dos Números. Os conceitos de divisibilidade, de Divisão Euclidiana, de Mínimo Múltiplo Comum e a estrutura do Algorítmo de Euclides são enfatizados, sendo apresentados teoremas e demonstrações com todo o rigor matemático mas, que sem dúvida, tornam-se conteúdos que podem ser introduzidos aos estudantes do Ensino Médio.

Já, no terceiro capítulo, expõem-se técnicas de resolução de Equações Diofantinas que fazem uso de tópicos já trabalhados no Ensino Fundamental e, também, reforçados ou aprofundados no Ensino Médio. O uso da fatoração possibilita a resolução de equações até antes impossíveis de serem resolvidas pelos métodos utilizados anteriormente. Em outras equações, faz-se uso de inequações para limitar o campo de algumas incógnitas e assim reduzir o campo de possíveis soluções. Demonstra-se um teorema que estabelece as condições necessárias e suficientes para que equação diofantina tenha solução. Apresenta-se, também, a solução de todos os exemplos citados no texto.

No capítulo 4 menciona-se um roteiro de atividades para ser utilizado por um professor interessado em trabalhar seus alunos para as Olímpiadas de Matemática ou, desenvolver um tópico mais avançado em Teoria dos Números, ou simplesmente fornecer ferramentas para a resolução de problemas por meio de Equações Diofantinas.

Toda discussão retratada nos capítulos não exige conhecimentos avançados e poderá ser feita em turmas do Ensino Médio e, também, dos últimos anos do Ensino Fundamental.

1 DIOFANTO DE ALEXANDRIA

Neste capítulo, faz-se um histórico sobre Diofanto de Alexandria e de sua principal obra *Aritmética*.

1.1 Diofanto de Alexandria

Pouco se conhece sobre a vida de Diofanto de Alexandria. Não se sabe ao certo o período em que Diofanto viveu, mas a maioria dos historiadores, situa-o no século III da nossa Era (EVES, 2004).

Dentre os matemáticos que estudaram a Teoria dos Números, sem dúvida, Diofanto foi um dos mais importantes. Sua obra *Aritmética*, escrita por volta de 250 d.C., trata principalmente da solução de equações indeterminadas com coeficientes inteiros.

1.2 A obra *Aritmética*

Diofanto escreveu livros como *Porismas* que se perdeu, escreveu sobre os números poligonais e sobre os números fracionários. Há outro trabalho, *Preliminares dos elementos de geometria* que se atribui a Heron, mas se crê que pertence a Diofanto.

Sobre os números poligonais se conhece apenas fragmentos que contém uma generalização da propriedade dos números triangulares que, tomado 8 vezes e somando-lhe a unidade, resulta um quadrado e termina com o problema, não resolvido, de saber quando um número é poligonal.

A sua principal obra é, sem dúvida, *Aritmética* composta de 13 livros, dos quais apenas 6 sobreviveram até aos nossos tempos. Arithmética é uma coleção de problemas sob forma de exemplos numéricos específicos. Foi encontrada em Veneza por Johann Müller (matemático e astrônomo alemão) em 1464 e a primeira tradução se deve a Wilhelm Holzmann (1532-1576). Essa obra representa, essencialmente, um novo ramo à matemática usando um método diferente de tudo que se conhecia na época.

Lins e Gimenez (2005) apontam que Diofanto solucionava os problemas expostos utilizando aplicações numéricas específicas, introduzindo diversas técnicas de resolução, porém sem recorrer à teorização.

Em 1621, aparece a edição de Bachet de Méziriac com o seguinte título: *Diophanti Alexandrini Arithmeticorum libri sex; et de Numeris multangulis liber unus. Nunc primun graece et latini editi atque absolutissimis commentariis illustrati*, Paris 1621 (que contém para além do texto grego e a tradução em latim, esclarecimentos e notas).

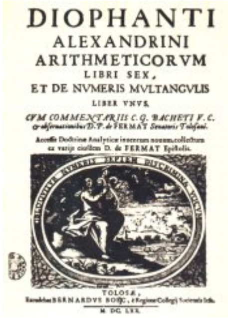

Figura 1 – Capa do Livro *Aritmética*

1.2.1 Livros que compõem a obra *Aritmética*

Da obra *Aritmética*, composta por 13 livros, conhece se apenas 6. Dos outros livros nada se sabe.

No primeiro livro há 39 problemas dos quais 25 são problemas que envolvem equações de 1º grau e 14, de 2º grau.

No segundo livro encontramos 35 problemas. O mais famoso dos problemas deste livro é o de número 8.

Foi em uma cópia do livro *Aritmética*, nas margens desse problema de número 8, no qual se achavam descritas as infinitas soluções da equação pitagórica $x^2 + y^2 = z^2$ que Pierre de Fermat (1601 - 1665) escreveu: *"Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que todavia esta margem não é sufucientemente grande para cabê-la."*

Esta afirmação, conhecida como o *Último Teorema de Fermat*, só foi demonstrada em 1995, pelo matemático inglês Andrew Wiles. Alguns acreditam que a demontração de Fermat não estaria totalmente correta, outros, que seria realmente uma demonstração brilhante, uma vez que Wiles usou conhecimentos sofisticados e modernos em sua demonstração. Na referência [12] o leitor encontrará mais informações sobre esse teorema.

Já o terceiro livro contém 21 problemas. No problema 19 deste livro, pela primeira vez, recorre se à geometria para obter sua solução.

O livro quatro contém 40 problemas. A maioria deles trata dos números cúbicos. Como os gregos não conheciam as fórmulas da equação cúbica, a seleção dos dados de Diofanto faz com que se chegue a uma solução aceitável deste tipo de equação.

O quinto livro consta de 30 problemas, dos quais 28 são de 2º e 3º graus.

O sexto e último livro contém 24 problemas que trazem a resolução de triângulos retângulos de lados racionais.

1.2.2 Importância da obra *Aritmética*

Segundo Roque (2012) a contribuição mais conhecida de Diofanto é ter introduzido uma forma de representar o valor desconhecido em um problema, designando-o como *arithmos*, de onde vem o nome "aritmética".

O livro Aritmética continha uma coleção de problemas que integrara a tradição matemática da época. Já no livro I, ele introduz símbolos, aos quais chama "designações abreviadas", para representar os diversos tipos de quantidade que aparecem nos problemas. O método de abreviação representava a palavra usada para designar essas quantidades por sua primeira ou última letra de acordo com o alfabeto grego. Diofanto usou o símbolo análogo à letra grega ζ para representar a incógnita; para o quadrado da incógnita usou Δ^Y, à qual chamou *dynamis* (quadrado); para cubo da incógnita usou K^Y e chamou-lhe *Kybos*; para a potência de expoente quatro usou $\Delta^Y\Delta$ e chamou-lhe *dynamis-dynamis*; para as potências de expoente cinco e seis usou, respectivamente, ΔK^Y(*dynamis-kybos*) e $K^Y K$ (*kybos-kybos*) (Roque, 2012, p. 232).

1.2.3 Problemas dos Livros *Aritmética*

Problema 1. *Dividir um número dado em dois números de diferença dada.*

a) Resolução proposta por Diofanto (retórica): Seja 80 o número e a diferença 20; achar os números. Supondo *arithmos* o número menor, o maior será $arithmos + 20$; logo, os dois somados dão $2arithmos + 20$, que vale 80. Então, 80 é igual a $2arithmos + 20$. Em seguida, subtrai-se 20 a cada um dos membros ficando $2arithmos = 60$. Logo, o número *arithmos* será 30. Então, *arithmos* é 30 e $arithmos + 20$ é 50.

b) Uma resolução usando as abreviações (mais geral): Supondo ζ o número menor, o maior será $\zeta + 20$; logo, os dois somados dão $2\zeta + 20$, que vale 80. Então, 80 é igual a $2\zeta + 20$. Em seguida vamos subtrair 20 a cada um dos membros ficando 2ζ igual a 60. Logo o número ζ será 30. Então, ζ é igual a 30 e $\zeta + 20$ é igual a 50.

c) Resolução em notação moderna: Supondo x o número menor, o maior será $x+20$; logo, os dois somados dão $2x + 20$, que vale 80. Então, $2x + 20 = 80$. Em seguida vamos subtrair 20 de cada um dos membros $2x + 20 - 20 = 80 - 20$ ficando $2x = 60$. Logo $x = 30$. Portanto, os números são 30 e 50.

Problema 2. *(Problema 8, Livro II)Decompor o quadrado 16 em dois quadrados.*

Resolução proposta por Diofanto: Se quisermos decompor 16 em dois quadrados e supusermos que o primeiro é 1 *arithmo*, o outro terá 16 unidades menos um quadrado de *arithmos* e, portanto, 16 unidades menos um quadrado de *arithmos* são um quadrado. Formemos um quadrado de um conjunto qualquer de *arithmos* diminuído de tantas unidades como tem a raiz de 16 unidades, ou seja, o quadrado de 2 *arithmos* menos 4 unidades. Este quadrado terá 4 unidades de *arithmos* e 16 unidades menos 16*arithmos*, que igualaremos a 16 unidades menos um quadrado de *arithmo* e somando a um e outro lado os termos negativos e restando os semelhantes, resulta que 5 quadrados de *arithmos* equivalem a 16 *arithmos* e, portanto, 1 *arithmo* vale $\frac{16}{5}$; logo, um dos números é $\frac{256}{25}$ e o outro $\frac{144}{25}$, cuja soma é $\frac{400}{25}$, ou seja 16 unidades, e cada um deles é um quadrado.

Problema 3. *(Problema 17, Livro I) Encontrar quatro números cuja soma três a três seja, respectivamente, 22, 24, 27 e 20.*

Problema 4. *(Problema 13, Livro III) Encontrar três números tais que o produto de quaisquer dois somado ao terceiro seja um quadrado.*

Problema 5. *(Problema 15, Livro III) Encontrar três números tais que o produto de quaisquer dois somado à soma deles seja um quadrado.*

2 TEORIA DOS NÚMEROS

Neste capítulo, apresenta-se uma introdução à Teoria dos Números por meio de Definições, Proposições e Teoremas.

2.1 Divisibilidade

Definição 1. *Dados dois números inteiros a e b, dizemos que a divide b, denotando-se por $a|b$, se existir um número inteiro k tal que $b = a \cdot k$. Caso contrário, a não divide b e indica-se $a \nmid b$.*

Proposição 2.1.1. *Sejam $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$. Tem-se que*
i) $1|c$, $a|a$ e $a|0$;
ii) se $a|b$ e $b|c$, então $a|c$.

Demonstração: (i) Decorre imediatamente das igualdades $c = 1 \cdot c$, $a = a \cdot 1$ e $0 = a \cdot 0$. (ii) $a|b$ e $b|c$ implica que existem m e n inteiros tais que $b = a \cdot m$ e $c = b \cdot n$. Substituindo o valor de b da primeira equação na outra, obtemos $c = b \cdot n = (a \cdot m) \cdot n = a \cdot (m \cdot n)$, o que nos mostra que $a|c$. □

Exemplo 2.1.1. *Como* $3|15$ *e* $15|75$*, então* $3|75$.

Proposição 2.1.2. *Se $a, b, c, m, n \in \mathbb{Z}$, $c|a$ e $c|b$, então $c|(ma \pm nb)$.*

Demonstração: Se $c|a$ e $c|b$, então existem inteiros k e w tais que $a = kc$ e $b = wc$. Multiplicando a primeira equação por m e a segunda por n temos $ma = mkc$ e $nb = nwc$. Adicionando-se, membro a membro, obtemos $ma + nb = (mk + nw)c$, o que nos diz que $c|(ma + nb)$. Subtraindo, membro a membro, chegamos a $ma - nb = (mk - nw)c$, o que nos diz que $c|(ma - nb)$. Logo,$c|(ma \pm nb)$ □

Exemplo 2.1.2. *Como* $3|15$, $3|75$*, então* $3|(8 \cdot 15 + 13 \cdot 75)$.

Proposição 2.1.3. *Sejam $a, b, c, d \in \mathbb{Z}$, com $a \neq 0$ e $c \neq 0$. Se $a|b$ e $c|d$, então $ac|bd$.*

Demonstração: Se $a|b$ e $c|d$, então existem inteiros k e w tais que $b = ka$ e $d = wc$. Portanto, $bd = (kw) \cdot (ac)$, o que nos diz que $ac|bd$. □

Exemplo 2.1.3. *Em particular, se $a|b$, então $ac|bc$, $\forall c \in \mathbb{Z}^*$.*

Proposição 2.1.4. *Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$. Se $a|(b + c)$, então $a|b \Longleftrightarrow a|c$.*

Demonstração: Como $a|(b+c)$, então existe $k \in \mathbb{Z}$ tal que $(b+c) = ak$. Vamos supor que $a|b$, então, existe $w \in \mathbb{Z}$ tal que $b = aw$. Logo, $b+c = aw+c = ak$, donde segue-se que $c = ak - aw = a(k-w)$, que nos diz que $a|c$. Agora, se $a|c$, então, existe $h \in \mathbb{Z}$ tal que $c = ah$. Logo, $b+c = b+ah = ak$, donde segue-se que $b = ak - ah = a(k-h)$, que nos diz que $a|b$. Portanto, $a|b \iff a|c$. $\square$

Proposição 2.1.5. *Sejam $a, b \in \mathbb{Z}^*$. Se $a|b$ e $b|a$, então $a = \pm b$.*

Demonstração: Como $a|b$ e $b|a$, existem $k, w \in \mathbb{Z}$ tais que $b = ak$ e $a = bw$. Assim, temos $a = (ak) \cdot w$, ou ainda, $a = a \cdot (kw)$, o que implica $kw = 1$, o que nos diz que $w|1$, ou seja $w = \pm 1$. Portanto, $a = \pm b$. $\square$

Proposição 2.1.6. *Sejam $a, b \in \mathbb{Z}^*$. Se $a|b$, então $|a| \leq |b|$.*

Demonstração: Como $a|b$, existe $k \in \mathbb{Z}^*$ tal que $b = a \cdot k$, donde $|b| = |a| \cdot |k|$. Como, $|k| \geq 1$, segue que $|b| \geq |a|$. $\square$

Proposição 2.1.7. *Sejam $a, b, n \in \mathbb{N}$ com $a + b \neq 0$. Então $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração: Demonstra-se usando indução sobre n. Para $n = 0$ a afirmação é verdadeira, pois $a + b$ divide $a^1 + b^1 = a + b$. Vamos supor que $(a+b)|(a^{2n+1} + b^{2n+1})$. Reescrevendo $a^{2(n+1)+1} + b^{2(n+1)+1}$, obtemos:

$$a^{2(n+1)+1}+b^{2(n+1)+1} = a^2a^{2n+1}-b^2a^{2n+1}+b^2a^{2n+1}+b^2b^{2n+1} = (a^2-b^2)a^{2n+1}+b^2(a^{2n+1}+b^{2n+1}).$$

Como, $(a+b)|(a^2-b^2)$ e, por hipótese, $(a+b)|(a^{2n+1}+b^{2n+1})$, segue da Proposição 2.1.2 que $(a+b)|(a^{2(n+1)+1}+b^{2(n+1)+1})$ o que estabelece o resultado para todo $n \in \mathbb{N}$. $\square$

Proposição 2.1.8. *Sejam $a, b, n \in \mathbb{N}$ com $a \geq b > 0$. Então $a + b$ divide $a^{2n} - b^{2n}$.*

Demonstração: Novamente usaremos indução sobre n. Para $n = 0$ a afirmação é verdadeira, pois $a+b$ divide $a^0 - b^0 = 0$. Suponhamos que $(a+b)|(a^{2n} - b^{2n})$. Reescrevendo $a^{2(n+1)} - b^{2(n+1)}$, obtemos:

$$a^{2(n+1)} - b^{2(n+1)} = a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} = (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n}).$$

Como, $(a+b)|(a^2-b^2)$ e, por hipótese, $(a+b)|(a^{2n}-b^{2n})$, segue da Proposição 2.1.2 que $(a+b)|(a^{2(n+1)}+b^{2(n+1)})$ o que completa a demonstração. $\square$

Proposição 2.1.9. *Sejam $a, b, n \in \mathbb{N}$ com $a > b > 0$. Então $a - b$ divide $a^n - b^n$.*

Demonstração: Provaremos o resultado usando indução sobre n. Para $n = 0$ a afirmação é verdadeira, pois $a - b$ divide $a^0 - b^0 = 0$. Suponhamos, agora, que $(a - b)|(a^n - b^n)$. Reescrevendo $a^{n+1} - b^{n+1}$, obtemos:

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n).$$

Como, $(a - b)|(a - b)$ e, por hipótese, $(a - b)|(a^n - b^n)$, segue da Proposição 2.1.2 que $(a - b)|(a^{n+1} + b^{n+1})$ o que completa a demonstração. □

2.2 Divisão Euclidiana

Teorema 2.2.1 (Divisão Euclidiana)**.** *Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r, \quad r < a$$

Demonstração: Vamos supor que $b > a$, e consideremos, enquanto se fizer sentido, os números que formam o conjunto

$$S = \{b,\ b - a,\ b - 2a,\ , \cdots, b - na, \cdots\}$$

Pelo Princípio da Boa Ordem, o conjunto S tem um menor elemento, digamos $r = b - q \cdot a$. Vamos provar que r satisfaz as condições enunciadas no Teorema, ou seja, $r < a$. Se $a|b$, então $r = 0$ e nada mais temos a demonstrar. Se, por outro lado, $a \nmid b$, provaremos que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos $c = b - q \cdot a - a = b - (q + 1) \cdot a$, com $c < r$, o que é uma contradição com o fato de r ser o menor elemento de S. Portanto, $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Resta provar a unicidade. Vamos tomar dois elementos distintos em S. Note que a diferença entre o maior e o menor desses dois números é um múltiplo de a e, assim, essa diferença é no mínimo igual a a. Logo se $r_1 = b - a \cdot q_1$ e $r_2 = b - a \cdot q_2$, com $r_1 < r_2 < a$, teríamos $r_2 - r_1 \geq a$. Isso nos daria, $r_2 \geq r_1 + a \geq a$, absurdo, portanto $r_2 = r_1$.

Como $r_2 = r_1$, segue-se que $b - a \cdot q_1 = b - a \cdot q_2$, o que implica que $a \cdot q_1 = a \cdot q_2$ e, portanto $q_1 = q_2$.

□

Os números q e r são chamados, respectivamente, de *quociente* e *resto* da divisão de b por a.

O resto da divisão é zero se, e somente se, $a|b$.

Note que a demonstração do Teorema fornece um algorítmo para obtenção de q e de r. Veja o exemplo 2.2.1.

Exemplo 2.2.1. *Vamos encontrar o quociente e o resto da divisão de* 40 *por* 7.

Solução: Considere as diferenças sucessivas

$$40-7=33>7,\ 40-2\cdot 7=26>7,\ 40-3\cdot 7=19>7,\ 40-4\cdot 7=12>7,\ 40-5\cdot 7=5<7.$$

que nos dá $q=5$ e $r=5$.

Corolário 2.2.1. *Dados dois números naturais a e b com $1<a\leq b$, existe um número natural n tal que*

$$na\leq b<(n+1)a.$$

Demonstração: Pela Divisão Euclidiana, existem $q,r\in\mathbb{N}$ com $r<a$ determinados de forma única, tais que $b=a\cdot q+r$, o que implica, $aq\leq b$. Por outro lado, $b=a\cdot q+r<a\cdot q+a=a\cdot(q+1)$. Portanto, $aq\leq b<a\cdot(q+1)$. Basta tomar $n=q$ para completar a demonstração do Corolário. $\square$

2.3 Máximo Divisor Comum

Definição 2. *O máximo divisor comum de dois inteiros a e b (a ou b diferente de zero) é o maior inteiro que divide a e b. Indica-se por (a,b) o máximo divisor comum de a e b.*

Teorema 2.3.1. *Seja d o máximo divisor comum de a e b. Então existem n_1 e m_1 inteiros tais que $d=n_1a+m_1b$.*

Demonstração: Seja B o conjunto de todas as combinações lineares $na+mb$, com n e m inteiros. Obviamente, B contém números negativos, positivos e também o zero. Vamos escolher n_1 e m_1 tais que $c=n_1a+m_1b$ seja o menor inteiro positivo pertencente ao conjunto B. Primeiramente, vamos provar que $c|a$ e $c|b$. Suponhamos que $c\nmid a$, neste caso, pelo Teorema 2.2.1, existem q e r tais que $a=qc+r$ com $0<r<c$. Portanto, $r=a-qc=a-q(n_1a+m_1b)=(1-qn_1)a+(-qm_1)b$. Isto mostra que $r\in B$, o que é uma contradição, uma vez que $0<r<c$ e, por hipótese, c era o menor elemento positivo de B. Logo $c|a$ e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem inteiros w_1 e w_2 tais que $a=w_1d$ e $b=w_2d$ e, portanto, $c=n_1a+m_1b=n_1w_1d+m_1w_2d=d(n_1w_1+m_1w_2)$ o que implica $d|c$. Por serem d e c ambos positivos, segue da proposição 2.1.6, que $d\leq c$. Como $d<c$ não é possível, uma vez que ele é o máximo divisor comum, concluímos que $d=c$, isto é, $d=n_1a+m_1b$. $\square$

Observe que, se $a, b \in \mathbb{Z}$, tem-se obviamente que $(a, b) = (b, a)$, $(0, a) = |a|$, $(1, a) = 1$ e que $(a, a) = |a|$. Além disso, para todo $b \in \mathbb{Z}$, temos

$$a|b \Longleftrightarrow (a, b) = |a| \,.$$

De fato, se $a|b$, temos que $|a|$ é um divisor comum de a e b, e se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = (a, b)$.

Agora, se $(a, b) = |a|$, segue-se que $|a|$ divide b, isto é, $a|b$.

Observe que dados a e b inteiros, se existir o (a, b) de a e b, então

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

Assim, podemos supor sempre a e b não negativos no cálculo do mdc entre a e b.

Diante disso, podemos agora provar a existência do máximo divisor comum de dois números inteiros. Basta mostrarmos que o resultado é válido para dois números não negativos, fato demonstrado por Euclides.

Lema 2.3.2 (Lema de Euclides)**.** *Sejam $a, b, n \in \mathbb{N}$ com $a < na < b$. Se existe $(a, b - na)$, então existe (a, b) e*

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

Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que $d|b$, pois $b = b - na + na$. Logo d é um divisor comum de a e b. Vamos supor que c seja um divisor comum de a e b, logo c é um divisor comum de a e $b - na$ e, portanto $c|d$. Isso prova que $d = (a, b)$. □

Proposição 2.3.3. *Para todo inteiro positivo t e $a, b \in \mathbb{Z}$, tem-se que $(ta, tb) = t(a, b)$.*

Demonstração: Pelo Teorema 2.3.1, existem $k, w \in \mathbb{Z}$ tais que $(ta, tb) = kta + wtb$. Segue que $kta + wtb = t(ka + wb) = t(a, b)$. □

Proposição 2.3.4. *Se $c > 0$ e a e b são divisíveis por c, então*

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

Demonstração: Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são números inteiros. Substituindo a por $\frac{a}{c}$ e b por $\frac{b}{c}$ e tomando $t = c$ na Proposição 2.3.3 chegamos ao resultado desejado. □

Corolário 2.3.5. *Se $(a, b) = d$, então*

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

Demonstração: Tomando $c = d$ na Proposição 2.3.4, segue o resultado. $\square$

Proposição 2.3.6. *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Como $(a, b) = 1$ pelo Teorema 2.3.1, existem inteiros w e k tais que $wa + kb = 1$. Multiplicando os dois membros dessa última equação por c temos que $w(ac) + k(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$, então, pela Proposição 2.1.2, $a|c$. $\square$

2.4 Algorítmo de Euclides

No Livro VII de Os Elementos, Proposição 2, Euclides apresenta a prova construtiva da existência do Máximo Divisor Comum. O método apresentado é denominado *Algorítmo de Euclides*.

Dados $a, b \in \mathbb{N}$, supondo $a < b$, se $a = b$, ou ainda $a|b$, temos que $(a, b) = a$.

Vamos então, supor que $1 < a < b$ e que $a \nmid b$. Logo, pela Divisão Euclidiana podemos escrever

$$b = aq_1 + r_1, \text{ com } r_1 < a.$$

Temos duas possibilidades:

a) $r_1|a$, e, neste caso, $r_1 = (a, r_1) = (a, b - q_1 a) = (a, b)$ o que finaliza o algorítmo, ou

b) $r_1 \nmid a$, podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1 q_2 + r_2, \text{ com } r_2 < r_1.$$

Novamente temos duas possibilidades:

a$_1$) r$_2|r_1$, e, neste caso, $r_2 = (r_1, r_2) = (r_1, a - q_2 r_1) = (r_1, a) = (b - q_1 a, a) = (b, a) = (a, b)$ o que finaliza o algorítmo, ou

b$_1$) r$_2 \nmid r_1$, efetuamos a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } r_3 < r_2.$$

Esse procedimento não ocorre infinitamente, uma vez que obteríamos uma sequência de números naturais $a > r_1 > r_2 > r_3 > \cdots$ que não teria um menor elemento, contrariando o Princípio da Boa Ordem. Assim, para algum n, temos que $r_n = r_{n+1}$, o que implica $(a, b) = r_n$.

O Algorítmo de Euclides pode ser realizado na prática como se segue.

Inicialmente, dividimos b por a, obtendo q_1 e r_1 e colocamos esses números no diagrama a seguir da seguinte forma:

	q_1	
b	a	
r_1		

Em seguida, efetuamos a divisão de a por r_1, obtendo q_2 e r_2. Colocando esses novos números no diagrama, ficamos com

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Seguindo o procedimento, enquanto for possível, teremos

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

Exemplo 2.4.1. *Determinemos o mdc de 500 e 345.*

	1	2	4	2	3
500	345	155	35	15	5
155	35	15	5		

Observando o algorítmo podemos escrever, $5 = 35 - 2 \cdot 15$, $15 = 155 - 4 \cdot 35$, $35 = 345 - 2 \cdot 155$ e $155 = 500 - 1 \cdot 345$.

Segue que

$5 = 35 - 2 \cdot 15 = 35 - 2 \cdot (155 - 4 \cdot 35) = 9 \cdot 35 - 2 \cdot 155 = 9 \cdot (345 - 2 \cdot 155) - 2 \cdot 155 = 9 \cdot 345 - 20 \cdot 155 = 9 \cdot 345 - 20 \cdot (500 - 1 \cdot 345) = 9 \cdot 345 - 20 \cdot (500 - 1 \cdot 345) = 29 \cdot 345 - 20 \cdot 500.$

Logo, $(500, 345) = 5 = 29 \cdot 345 - 20 \cdot 500$.

3 EQUAÇÕES DIOFANTINAS

Neste capítulo apresentamos as Equações Diofantinas e alguns procedimentos para se obter suas soluções.

3.1 Equação Diofantina

Definição 1. *Uma equação Diofantina é uma equação do tipo*

$$f(x_1, x_2, \cdots, x_n) = 0, \tag{3.1}$$

onde f é uma função n-variável com $n \geq 2$ e coeficientes inteiros. As soluções de 3.1 são as n-uplas $(a_1, a_2, \cdots, a_n)$ em que $a_i \in \mathbb{Z}$, $1 \leq i \leq n$.

Este tipo de equação foi abordado pelo grego Diofanto na obra *Aritmética*, por isso, recebe o nome de Equação Diofantina.

Ao observarmos uma equação diofantina é natural surgirem três questionamentos básicos:

Questionamento 1. *A equação tem solução?*

Questionamento 2. *Se tem solução, o número de soluções é finito ou infinito?*

Questionamento 3. *Se tem solução e o número de soluções é finito, quais são estas soluções?*

Como as equações têm 2 ou mais variáveis, pode haver uma infinidade de soluções inteiras. Por exemplo, a equação diofantina $3x - 2y = 1$ tem como solução os números $x = 1 + 2k$ e $y = 1 + 3k$ para k inteiro.

3.2 Métodos Elementares para resolução de Equações Diofantinas

3.2.1 O Método da Fatoração

Dada a equação $f(x_1, x_2, \cdots, x_n) = 0$, nós podemos escrevê-la na forma equivalente

$$f_1(x_1, x_2, \cdots, x_n) \cdot f_2(x_1, x_2, \cdots, x_n) \cdot \cdots \cdot f_k(x_1, x_2, \cdots, x_n) = a \tag{3.2}$$

onde $f_1, f_2, \cdots, f_k$ têm coeficientes inteiros e $a \in \mathbb{Z}$. Fatorando a em números primos, obtemos um número finito de decomposições em k fatores inteiros $a_1, a_2, \cdots, a_k$. Cada uma dessas decomposições gera um sistema de equações

$$\begin{cases} f_1(x_1, x_2, \cdots, x_n) = a_1 \\ f_2(x_1, x_2, \cdots, x_n) = a_2 \\ \vdots \\ f_k(x_1, x_2, \cdots, x_n) = a_k \end{cases}$$

Vejamos algumas equações diofantinas para exemplificar o método da fatoração.

Exemplo 3.2.1.1. *Determine as soluções inteiras da equação*

$$6x^2 - 2y^2 + xy - 5 = 0.$$

Solução: Reescrevendo $6x^2 - 2y^2 + xy - 5 = 0$ como $6x^2 + 4xy - 2y^2 - 3xy = 5$, ou ainda, $2x(3x + 2y) - y(3x + 2y) = 5$. Daí obtemos, $(3x + 2y)(2x - y) = 5$ o que nos leva aos sistemas:

$$\begin{cases} 3x + 2y = 1 \\ 2x - y = 5 \end{cases}, \quad \begin{cases} 3x + 2y = 5 \\ 2x - y = 1 \end{cases}, \quad \begin{cases} 3x + 2y = -1 \\ 2x - y = -5 \end{cases}, \quad \begin{cases} 3x + 2y = -5 \\ 2x - y = -1 \end{cases}$$

Resolvendo os sistemas, obtém-se $(1, 1)$ e $(-1, -1)$ como soluções inteiras da equação $6x^2 - 2y^2 + xy - 5 = 0$.

Exemplo 3.2.1.2. *Determine as soluções inteiras e positivas da equação*

$$xy = x + y + 3.$$

Solução: Reescrevendo a equação $xy = x + y + 3$ como $xy - x - y + 1 = 4$, ou ainda, $x(y - 1) - 1(y - 1) = 4$. Daí obtemos, $(x - 1)(y - 1) = 4$ o que nos conduz aos sistemas:

$$\begin{cases} x - 1 = 1 \\ y - 1 = 4 \end{cases}, \quad \begin{cases} x - 1 = 4 \\ y - 1 = 1 \end{cases}, \quad \begin{cases} x - 1 = 2 \\ y - 1 = 2 \end{cases}$$

Resolvendo os sistemas, obtemos as seguintes soluções: $(2, 5), (5, 2), (3, 3)$.

Portanto, a equação $xy = x + y + 3$ tem três soluções inteiras e positivas: $(2, 5)$, $(5, 2)$ e $(3, 3)$.

Exemplo 3.2.1.3. *(Olimpíada Indiana de Matemática) Determine todas as soluções inteiras não-negativas da equação*

$$(xy - 7)^2 = x^2 + y^2.$$

Solução: Reescrevendo a equação $(xy-7)^2 = x^2+y^2$ como $x^2y^2-14xy+49 = x^2+y^2$, ou ainda, $x^2y^2 - 12xy + 36 + 13 = x^2 + 2xy + y^2$. Segue que, $(xy - 6)^2 - (x + y)^2 = -13$.

Portanto, $[xy-6-(x+y)][xy-6+x+y] = (xy-6)^2-(x+y)^2 = -13$, que nos conduz aos sistemas:

$$\begin{cases} xy-6-(x+y)=1 \\ xy-6+x+y=-13 \end{cases}, \quad \begin{cases} xy-6-(x+y)=-1 \\ xy-6+x+y=13 \end{cases}$$

$$\begin{cases} xy-6-(x+y)=13 \\ xy-6+x+y=-1 \end{cases}, \quad \begin{cases} xy-6-(x+y)=-13 \\ xy-6+x+y=1 \end{cases}$$

que são semelhantes aos sistemas

$$\begin{cases} x+y=-7 \\ xy=0 \end{cases}, \quad \begin{cases} x+y=7 \\ xy=12 \end{cases}$$

$$\begin{cases} x+y=-7 \\ xy=12 \end{cases}, \quad \begin{cases} x+y=7 \\ xy=0 \end{cases}$$

Resolvendo os sistemas, obtem-se $(-7,0)$, $(0,-7)$, $(3,4)$, $(4,3)$, $(-3,-4)$, $(-4,-3)$, $(0,7)$ e $(7,0)$ como soluções.

Logo, as soluções inteiras e não negativas da equação $(xy-7)^2 = x^2+y^2$ são $(3,4)$, $(4,3)$, $(0,7)$ e $(7,0)$.

Exemplo 3.2.1.4. *Determine todas as soluções inteiras positivas da equação*

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{6}.$$

Solução: Reescrevendo a equação $\frac{1}{x}+\frac{1}{y}=\frac{1}{6}$ como $6(x+y)-xy=0$, ou ainda, $6x+6y-xy=0$. Segue que, $x(6-y)-6(6-y)=-36$. Portanto, a equação é equivalente a $(x-6)(y-6)=36$.

Observe que $\frac{1}{x}<\frac{1}{6}$, então, $x>6$ e, portanto, $x-6>0$.

Assim a equação $(x-6)(y-6)=36$ nos conduz aos sistemas:

$$\begin{cases} x-6=1 \\ y-6=36 \end{cases}, \quad \begin{cases} x-6=2 \\ y-6=18 \end{cases}, \quad \begin{cases} x-6=3 \\ y-6=12 \end{cases}, \quad \begin{cases} x-6=4 \\ y-6=9 \end{cases}, \quad \begin{cases} x-6=6 \\ y-6=6 \end{cases}$$

$$\begin{cases} x-6=9 \\ y-6=4 \end{cases}, \quad \begin{cases} x-6=12 \\ y-6=3 \end{cases}, \quad \begin{cases} x-6=18 \\ y-6=2 \end{cases}, \quad \begin{cases} x-6=36 \\ y-6=1 \end{cases}$$

Resolvendo os sistemas, obtemos as seguintes soluções: $(7,42)$, $(8,24)$, $(9,18)$, $(10,15)$, $(12,12)$, $(15,10)$, $(18,9)$, $(24,8)$ e $(42,7)$ que são as soluções inteiras positivas da equação $\frac{1}{x}+\frac{1}{y}=\frac{1}{6}$.

Exemplo 3.2.1.5. *(Olimpíada Polonesa de Matemática) Determine todas as soluções inteiras equação*

$$x^2(y-1)+y^2(x-1)=1.$$

Solução: Fazendo $x = u + 1$ e $y = v + 1$ reescreve-se a equação dada como $(u+1)^2v+(v+1)^2u = 1$, ou ainda, $u^2v + 2uv + v + uv^2 + 2uv + u = 1$, o que nos dá, $uv(u+v)+4uv+(u+v) = 1$. Daí, temos $uv(u+v+4)+(u+v+4) = 5$, que é equivalente à equação $(uv + 1)(u + v + 4) = 5$.

A equação $(uv + 1)(u + v + 4) = 5$ nos conduz aos sistemas:

$$\begin{cases} uv+1=1 \\ u+v+4=5 \end{cases}, \quad \begin{cases} uv+1=-1 \\ u+v+4=-5 \end{cases},$$

$$\begin{cases} uv+1=5 \\ u+v+4=1 \end{cases}, \quad \begin{cases} uv+1=-5 \\ u+v+4=-1 \end{cases}$$

Estes sistemas são equivalentes à

$$\begin{cases} uv=0 \\ u+v=1 \end{cases}, \quad \begin{cases} uv=-2 \\ u+v=-9 \end{cases},$$

$$\begin{cases} uv=4 \\ u+v=-3 \end{cases}, \quad \begin{cases} uv=-6 \\ u+v=-5 \end{cases}$$

Resolvendo os sistemas, observa-se que somente o primeiro e o último apresentam soluções inteiras que são: $(0, 1)$, $(1, 0)$, $(-6, 1)$, $(1, -6)$. Como $(x, y) = (u + 1, v + 1)$, as soluções inteiras da equação $x^2(y - 1) + y^2(x - 1) = 1$ são dadas pelos pares ordenados $(1, 2)$, $(2, 1)$, $(-5, 2)$, $(2, -5)$.

Exemplo 3.2.1.6. *Encontre todos os triângulos retângulos de lados com medidas inteiras tais que suas áreas e perímetros sejam iguais.*

Solução: Seja x e y o comprimento dos catetos e z o comprimento da hipotenusa. Então, pelo Teorema de Pitágoras, $z = \sqrt{x^2 + y^2}$. Como a área e o perímetro são iguais, temos,

$$\frac{xy}{2} = x + y + \sqrt{x^2+y^2}.$$

Multiplicando por 2, isolando o radical e elevando ao quadrado, obtemos:

$$[xy - 2(x + y)]^2 = 4(x^2 + y^2)$$

ou

$$x^2y^2 - 4xy(x+y) + 4(x^2+y^2+2xy) = 4(x^2+y^2)$$

Portanto, temos

$$x^2y^2 - 4xy(x+y) + 8xy = 0$$

que é equivalente à

$$xy - 4x - 4y + 8 = 0$$

Fatorando o lado esquerdo da equação $xy - 4x - 4y + 8 = 0$, obtemos

$$(x-4)(y-4) = 8.$$

Como $x > 0$ e $y > 0$, a equação $(x-4)(y-4) = 8$ nos conduz aos sistemas:

$$\begin{cases} x-4=1 \\ y-4=8 \end{cases}, \quad \begin{cases} x-4=2 \\ y-4=4 \end{cases}, \quad \begin{cases} x-4=4 \\ y-4=2 \end{cases}, \quad \begin{cases} x-4=8 \\ y-4=1 \end{cases}$$

Resolvendo os sistemas, observa-se que as soluções inteiras são: $(5,12)$, $(6,8)$, $(8,6)$, $(12,5)$. Asssim, são apenas dois triângulos retângulos, um com lados medindo 6, 8 e 10 e, o outro, com lados medindo 5, 12 e 13.

3.2.2 Usando Inequações para Resolver Equações Diofantinas

Este método consiste em restringir os intervalos em que as variáveis se encontram usando desigualdades adequadas. Geralmente, esse processo leva a um número finito de possibilidades para todas as variáveis ou para algumas delas.

Vejamos alguns exemplos de aplicação deste método.

Exemplo 3.2.2.1. *Encontre os pares de inteiros (x, y) tal que*

$$x^3 + y^3 = (x+y)^2.$$

Solução: Observe que, devido à simetria da equação, os pares da forma $(t, -t)$, $t \in \mathbb{Z}$, são soluções. Se $x + y \neq 0$, a equação torna-se

$$x^2 - xy + y^2 = x + y,$$

ou, multiplicando por 2 e reordenando os termos

$$(x^2 - 2xy + y^2) + (x^2 - 2x + 1) + (y^2 - 2y + 1) = 2,$$

que é equivalente a

$$(x-y)^2+(x-1)^2+(y-1)^2=2.$$

Segue que, $(x-1)^2 \leq 1$ e $(y-1)^2 \leq 1$. Isto restringe os valores das varáveis x e y no intervalo $[0,2]$.

Se $x=0$, temos $y^2-y=0$, que nos dá o par $(0,1)$; se $x=1$, temos $y^2-2y=0$ o que nos dá os pares $(1,0)$ e $(1,2)$ e se $x=2$, temos $y^2-3y+2=0$ o que nos dá os pares $(2,2)$ e $(2,1)$.

Assim obtemos as soluções $(0,1)$, $(1,0)$, $(1,2)$, $(2,2)$, $(2,1)$ e $(t,-t)$, $t \in \mathbb{Z}$.

Exemplo 3.2.2.2. *(Olimpíada Romena de Matemática) Resolva a seguinte equação nos inteiros positivos x, y e z*

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}.$$

Solução: Devido à simetria da equação, pode-se assumir que $2 \leq x \leq y \leq z$.

Isto implica que

$$\frac{3}{x} \geq \frac{3}{5} \Longrightarrow x \in \{2,3,4,5\}.$$

Se $x=2$, temos

$$\frac{1}{y}+\frac{1}{z}=\frac{1}{10}.$$

Isto acarreta que

$$\frac{2}{y} \geq \frac{1}{10} \Longrightarrow y \in \{11,12,\cdots,20\}.$$

Segue que

$$z=\frac{10y}{y-10}.$$

Neste caso, temos as soluções $(2,11,110)$, $(2,12,60)$, $(2,14,35)$, $(2,15,30)$, $(2,20,20)$.

Se $x=3$, tem-se

$$\frac{1}{y}+\frac{1}{z}=\frac{4}{15}.$$

Isto implica que

$$\frac{2}{y} \geq \frac{4}{15} \Longrightarrow y \in \{3,4,5,6,7\}.$$

Segue que

$$z=\frac{15y}{4y-15}.$$

Neste caso, as soluções são: $(3,4,60)$, $(3,5,15)$, $(3,6,10)$.

Se $x = 4$, temos
$$\frac{1}{y} + \frac{1}{z} = \frac{7}{20}.$$
Isso acarreta que
$$\frac{2}{y} \geq \frac{7}{20} \Longrightarrow y \in \{4, 5\}.$$
Substituindo esses valores, encontra-se a solução $(4, 4, 10)$.

Se $x = 5$, temos
$$\frac{1}{x} + \frac{1}{y} = \frac{2}{5}.$$
Isto implica que
$$\frac{2}{y} \geq \frac{2}{5} \Longrightarrow y \in \{5\}.$$
Segue que
$$z = \frac{5y}{2y - 5}.$$
Neste caso, temos a solução $(5, 5, 5)$.

Portanto, as soluções inteiras da equação dada são $(2, 11, 110)$, $(2, 12, 60)$, $(2, 14, 35)$, $(2, 15, 30)$, $(2, 20, 20)$, $(3, 4, 60)$, $(3, 5, 15)$, $(3, 6, 10)$, $(4, 4, 10)$ e $(5, 5, 5)$.

Exemplo 3.2.2.3. *Determine as soluções da equação*
$$3(xy + xz + yz) = 4xyz.$$

Solução: Podemos reescever a equação como
$$\frac{xy + xz + yz}{xyz} = \frac{4}{3},$$
que é equivalente à equação
$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{4}{3}.$$
Devido à simetria desta equação, podemos assumir que $x \leq y \leq z$. Isto implica que
$$\frac{3}{x} \geq \frac{4}{3} \Longrightarrow x \leq \frac{9}{4} \Longrightarrow x \in \{1, 2\}.$$
Se $x = 1$, temos
$$\frac{1}{y} + \frac{1}{z} = \frac{1}{3} \Longrightarrow \frac{2}{y} \geq \frac{1}{3} \Longrightarrow y \leq 6 \Longrightarrow y \in \{1, 2, 3, 4, 5, 6\}$$
Substituindo os valores obtemos as soluções $(1, 4, 12)$ e $(1, 6, 6)$.

Se $x = 2$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{5}{6} \Longrightarrow \frac{2}{y} \geq \frac{5}{6} \Longrightarrow y \leq \frac{12}{5} \Longrightarrow y \in \{2\}.$$

Fazendo a substituição obtemos a solução $(2, 2, 3)$.

Logo as soluções procuradas são $(1, 4, 12)$, $(1, 6, 6)$, $(2, 2, 3)$ e todas as permutações dessas soluções.

Exemplo 3.2.2.4. *(Olimpíada Romena de Matemática) Determine todos os ternos de inteiros positivos (x, y, z) que são soluções da equação*

$$(x + y)^2 + 3x + y + 1 = z^2.$$

Solução: Observe que

$$(x+y)^2 < (x+y)^2+3x+y+1 = z^2 < (x+y)^2+4x+4y+4 = (x+y)^2+4(x+y)+4 = (x+y+2)^2.$$

Assim, $(x + y)^2 + 3x + y + 1 = (x + y + 1)^2$, ou ainda, $(x + y)^2 + 3x + y + 1 = (x + y)^2 + 2x + 2y + 1$. Concluímos que $x = y$.

Substituindo na equação $x = y = k$, $k \in \mathbb{Z}_+$, obtemos $z = 2k + 1$.

Logo, as soluções procuradas são $(k, k, 2k + 1)$, $k \in \mathbb{Z}_+$.

Exemplo 3.2.2.5. *(Olimpíada Romena de Matemática) Determine todos os pares de inteiros (x, y) que são soluções da equação $(x + 1)^4 - (x - 1)^4 = y^3$.*

Solução: temos que

$$(x + 1)^4 - (x - 1)^4 =)[(x + 1)^2 + (x - 1)^2][(x + 1)^2 - (x - 1)^2] = (2x^2 + 2)(4x) = 8x^3 + 8x.$$

Seja (x, y) solução com $x \geq 1$.

Assim $8x^3 < 8x^3 + 8x < 8x^3 + 4x^2 + 4x + 1$, ou seja, $(2x)^3 < y^3 < (2x + 1)^3$, que é uma contradição.

Logo, $x < 1$.

Observe que se (x, y) é uma solução, $(-x, -y)$ também será. Assim, $-x$ deve ser não positivo. Portanto, $x = 0$. Substituindo na equação, obtemos $y = 0$, ou seja a equação tem uma única solução $(0, 0)$.

Exemplo 3.2.2.6. *Determine todos os inteiros positivos x, y, z, t tais que*

$$\begin{cases} x^n + y = z^n \\ x + y^n = t^n \end{cases}$$

para algum inteiro $n \geq 2$.

Solução: Da primeira equação obtemos, $x^n = z^n - y \leq z^n$, então $x < z$ ou $(x+1) \leq z$. Dessa mesma equação, obtemos $y = z^n - x^n \geq (x+1)^n - x^n = \binom{n}{1}x^{n-1} + \binom{n}{2}x^{n-2} + \binom{n}{3}x^{n-3} + \cdots + \binom{n}{n} > x$, isto é, $y > x$. Usando a segunda equação, obtemos $y^n = t^n - x \leq t^n$, então $y < t$ ou $(y+1) \leq t$. Dessa mesma equação, também obtemos $x = t^n - y^n \geq (y+1)^n - y^n = \binom{n}{1}y^{n-1} + \binom{n}{2}y^{n-2} + \binom{n}{3}y^{n-3} + \cdots + \binom{n}{n} > y$, isto é, $x > y$ que é uma contradição.

Logo, a equação dada não tem solução.

3.2.3 Equações Diofantinas Lineares

A resolução de vários problemas em Teoria dos Números que exigem soluções inteiras recai, em várias situações, em equações do tipo $ax + by = c$, com $a, b, c \in \mathbb{Z}$.

Essas equações são chamadas *Equações Diofantinas Lineares.*

Nem sempre essas equações apresentam soluções, vejamos por exemplo a equação:

$$2x + 4y = 3$$

Observe que não há nenhuma solução inteira para a equação, pois, o primeiro membro da equação é par e, nunca será igual ao segundo membro que é um número ímpar.

É natural perguntar-se quais são as condições necessárias e suficientes para que a equação diofantina linear tenha solução e como fazer para encontrá-las. As respostas são dadas pelo teorema a seguir.

Teorema 3.2.1. *Sejam $a, b, c, k \in \mathbb{Z}$ e $d = (a, b)$. Se $d \nmid c$, então a equação $ax + by = c$ não tem solução inteira. Se $d|c$ a equação possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por:*

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

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

Demonstração: Se $d \nmid c$, então a equação não possui solução pois, como $d|a$ e $d|b$, d deveria dividir c, uma vez que c é uma combinação linear de a e b. Suponhamos, portanto, que $d|c$. Pelo Teorema 2.3.1, existem inteiros n_0 e m_0, tais que $an_0 + bm_0 = d$. Como $d|c$, existe um inteiro k tal que $c = kd$. Multiplicando $an_0 + bm_0 = d$ por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par ordenado (x_0, y_0) com $x_0 = n_0k$ e $y_o = m_0k$ é uma solução de $ax + by = c$.

Vamos agora verificar que os pares ordenados da forma $x = x_0 + \left(\frac{b}{d}\right)k$ e $y = y_0 - \left(\frac{a}{d}\right)k$ são soluções de $ax + by = c$.

De fato,
$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)k\right) + b\left(y_0 - \left(\frac{a}{d}\right)k\right) = ax_0 + \frac{ab}{d} + by_0 - \frac{ab}{d} = ax_0 + by_o = c.$

Assim, mostramos que conhecida uma solução particular dada pelo par ordenado (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Resta mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + \left(\frac{b}{d}\right)k$ e $y = y_0 - \left(\frac{a}{d}\right)k$. Vamos supor que o par ordenado (x, y) seja uma solução, isto é, $ax + by = c$. Mas como $ax_0 + by_o = c$, obtemos, subtraindo membro a membro, que

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

o que acarreta $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$, segue do Corolário 2.3.4,

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

Portanto, dividindo os membros de $a(x - x_0) = b(y_0 - y)$ por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{3.3}$$

Logo, pela Proposição 2.3.5, $\left(\frac{b}{d}\right)|(x - x_0)$. Portanto existe um inteiro k tal que $x - x_0 = k\left(\frac{b}{d}\right)$. Substituindo esse valor na equação 3.3 temos $y = y_0 - \left(\frac{a}{d}\right)k$ o que completa a demonstração. □

Exemplo 3.2.1. *Anita 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 ela comprou.*

Solução: Sejam x o número de canetas e y o número de borrachas com $x, y \in \mathbb{N}$. Obtemos a equação $1,7x + 0,9y = 37,4$. Multiplicando essa equação por 10, ela se torna $17x + 9y = 374$.

Como $1 = (17, 9)|374$ a equação tem solução.

Usando o Algorítmo de Euclides, vamos encontrar uma solução para a equação $17x + 9y = 374$.

	1	1	8
17	9	8	1
8	1		

Observando o algorítmo podemos escrever, $1 = 9 - 1 \cdot 8$ e $8 = 17 - 1 \cdot 9$.

Segue que $1 = 9 - 1 \cdot 8 = 9 - 1 \cdot (17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9$. Multiplicando por 374, teremos

$$374 = -374 \cdot 17 + 748 \cdot 9.$$

Isso nos dá a solução particular $x_0 = -374$ e $y_0 = 748$. A solução geral é, então, dada por $(x, y) = (-374 + 9t, 748 - 1t)$. Como $x > 0$ e $y > 0$, temos $41 < t < 44$, ou seja, $t = 42$ ou $t = 43$.

Se $t = 43$, teremos, $x = 13$ e $y = 17$ e, se $t = 42$, então, $x = 4$ e $y = 34$. Como x deve ser ímpar, segue $x = 13$ e $y = 17$, isto é, foram compradas 13 canetas e 17 borrachas.

Exemplo 3.2.2. *Determinar o menor inteiro positivo que dividido por* 8 *e por* 15 *deixa os restos* 6 *e* 13, *respectivamente.*

Solução: Seja n o número inteiro positivo. Pelo algoritmo da divisão, existem x e y positivos tais que $n = 8x + 6$ e $n = 15y + 13$. Assim,

$$8x + 6 = 15y + 13 \Longrightarrow 8x - 15y = 7$$

Como $1 = (8, 15)|7$ a equação tem solução.

Usando o Algorítmo de Euclides, vamos encontrar uma solução para a equação $8x - 15y = 7$.

	1	1	7
15	8	7	1
7	1		

Observando o algorítmo podemos escrever, $1 = 8 - 1 \cdot 7$ e $7 = 15 - 1 \cdot 8$.

Segue que $1 = 8 - 1 \cdot 7 = 8 - 1 \cdot (15 - 1 \cdot 8) = 2 \cdot 8 - 1 \cdot 15$. Multiplicando por 7, teremos

$$7 = 14 \cdot 8 - 7 \cdot 15.$$

Isso nos dá a solução particular $x_0 = 14$ e $y_0 = -7$. A solução geral é, então, dada por $(x, y) = (14 - 15t, 7 - 8t)$. Como $x > 0$ e $y > 0$, temos $14 - 15t > 0$ e $7 - 8t > 0$, ou seja, $t < \frac{14}{15}$. O menor valor de n será obtido ao tomar o menor valor de x e y que satisfaça a equação $8x - 15y = 7$ e, isso acontece quando $t = 0$. Isso nos dá $(x, y) = (14, 7)$ e, portanto, $n = 118$.

Exemplo 3.2.3. *Exprimir* 100 *como soma de dois inteiros positivos de modo que o primeiro seja divisível por* 7 *e o segundo seja divisível por* 11.

Solução: Sejam $7x$ e $11y$ esses dois números. Assim, temos $7x + 11y = 100$.

Como $1 = (7, 11)|100$ a equação tem solução.

Usando o Algorítmo de Euclides, vamos encontrar uma solução para a equação $7x + 11y = 100$.

	1	1	1	3
11	7	4	3	1
4	3	1		

Observando o algorítmo podemos escrever, $1 = 4 - 1 \cdot 3$, $3 = 7 - 1 \cdot 4$ e $4 = 11 - 1 \cdot 7$

Segue que $1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 17 = 2 \cdot (11 - 1 \cdot 7) - 1 \cdot 7 = 2 \cdot 11 - 3 \cdot 7$. Multiplicando por 100, teremos

$$100 = -300 \cdot 7 + 200 \cdot 11.$$

Isso nos dá a solução particular $x_0 = -300$ e $y_0 = 200$. A solução geral é, então, dada por $(x, y) = (-300 + 11t, 200 - 7t)$. Como $x > 0$ e $y > 0$, temos $-300 + 11t > 0$ e $200 - 7t > 0$, ou seja, $27 < t < 29$. Logo, $n = 28$, o que nos dá $(x, y) = (8, 4)$. Assim, os números são 56 e 44.

4 TRANSPOSIÇÃO DIDÁTICA

Capítulo destinado às atividades de ensino.

4.1 Sequência didática para o uso da fatoração na resolução de Equações Diofantinas

Atividade 4.1.1. *Avaliação Diagnóstica - Duração: 1 a 3 aulas de 50 minutos.*

Primeiramente, deve-se fazer um diagnóstico de como estão os estudantes em relação ao conteúdo de fatoração. Assim, deve-se elaborar uma sondagem com os diversos casos de fatoração estudados no Ensino Fundamental e no Ensino Médio. Diante dos resultados obtidos, verifica-se se há a necessidade de uma revisão.

Essa avalição diagnóstica deverá conter questões envolvendo: fator comum em evidência, fatoração por agrupamento, fatoração da diferença de dois quadrados, fatoração da soma e da diferença de cubos, fatoração do trinômio quadrado perfeito, entre outros casos.

Atividade 4.1.2. *Resolvendo uma Equação Diofantina - Duração: 1 a 3 aulas de 50 minutos.*

Nessa segunda atividade, resolve-se a equação

$$(5x + 3y)(2x + y) = 7.$$

Observe que ela já está na forma fatorada e servirá para apresentar a técnica aos estudantes. Se houver dúvidas quanto à resolução e ao uso da técnica, consultar os exemplos da subseção O Método da Fatoração, do capítulo 3.

Atividade 4.1.3. *Fatorando e resolvendo uma Equação Diofantina - Duração: 3 a 6 aulas de 50 minutos.*

Nessa atividade, o professor deverá apresentar os exemplos que estão na subseção *O Método da Fatoração* no capítulo 3.

Após a resolução de todos esses exemplos, o professor poderá apresentar outros para fixação da aprendizagem do tema.

Atividade 4.1.4. *Avaliação da Aprendizagem - Duração: 2 aulas de 50 minutos.*

Essa atividade, a ser elaborada pelo professor, deverá conter cinco Equações Diofantinas que possam ser resolvidas utilizando-se a fatoração. O objetivo é verificar a aprendizagem e, a partir, da análise dos resultados verificar a necessidade de uma retomada do tema em foco. Para isso, consulte os livros citados nas referências bibliográficas.

4.2 Sequência didática para o uso das desigualdades na resolução de Equações Diofantinas

Atividade 4.2.1. *Revisão - Duração: 2 aulas de 50 minutos.*

Para introduzir o uso das desigualdades na Resolução de Equações Diofantinas, é necessário revisar os conteúdos: inequações do primeiro grau e a relação de desigualdades entre números racionais e, outros que o professor considerar necessário durante as aulas.

Atividade 4.2.2. *Resolvendo uma Equação Diofantina - Duração: 1 a 3 aulas de 50 minutos.*

Nessa segunda atividade, deverá ser resolvido o problema: Encontre os pares de inteiros (x, y) tal que $x^3 + y^3 = (x + y)^2$. Observe que ele é um dos exemplos resolvidos na subseção *Usando Inequações para Resolver Equações Diofantinas* no capítulo 3. A resolução completa desse problema mostrará a importância do uso das desigualdades na resolução de Equações Diofantinas.

Durante a resolução, comente todas as desigualdades utilizadas esclarecendo todas as dúvidas que os estudantes apresentarem.

Atividade 4.2.3. *Resolvendo outras Equações Diofantinas - Duração: 4 a 6 aulas de 50 minutos.*

Nessa atividade, o professor deverá apresentar os outros exemplos que estão na subseção Usando Inequações para Resolver Equações Diofantinas do capítulo 3.

Após a resolução de todos esses exemplos, o professor deverá apresentar outros exemplos para fixação da aprendizagem do tema. Para isso, o professor deverá consultar os livros citados nas referências bibliográficas.

Atividade 4.2.4. *Avaliação da Aprendizagem - Duração: 2 aulas de 50 minutos.*

Essa atividade, a ser elaborada pelo professor, deverá conter cinco Equações Diofantinas que possam ser resolvidas utilizando-se desigualdades.

O objetivo é verificar a aprendizagem e, a partir, da análise dos resultados verificar a necessidade de uma retomada do tema em foco.

4.3 Sequência didática para resolução de Equações Diofantinas Lineares

Atividade 4.3.1. *Motivação - Duração: 3 aulas de 50 minutos.*

Os estudantes são divididos em grupos e devem resolver a seguinte situação-problema:

Anita 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 ela comprou.

Atividade 4.3.2. *Apresentação das soluções e formas de resolução realizadas pelos grupos - Duração: 1 a 3 aulas de 50 minutos.*

Nessa segunda atividade, cada grupo apresenta os resultados e as forma de resolução utilizada para se obter a solução do problema.

Caso, nenhum grupo consiga apresentar uma resolução, o professor deve orientá-los, ajudando-os a obter a equação

$$17x + 9y = 374$$

Atividade 4.3.3. *Resolvendo a Equações Diofantina* $17x + 9y = 374$ *- Duração: 2 aulas de 50 minutos.*

Nessa atividade, o professor induz o uso de tabelas para obtenção de possíveis respostas inteiras. O método da Tentativa e Erro deve ser estimulado.

As soluções devem ser apresentadas e discutidas por todos. Verifica-se, então, se algum desses resultados satisfaz o problema inicial.

Atividade 4.3.4. *Uso do Algorítmo de Euclides - Duração: 4 aulas de 50 minutos.*

Essa atividade, a ser ministrada pelo professor, introduz o conceito de Equações Diofantinas Lineares, bem como, o uso do Algorítmo de Euclides em sua resolução. O professor resolve a equação motivadora $17x + 9y = 374$ e, também, instiga os alunos com perguntas, tais como: Quando uma Equação Diofantina Linear tem solução? ou A solução é única? ou Se existir solução como ela é?.

Nesse momento, o professor deve fazer uma introdução à Teoria dos Números.

Atividade 4.3.5. *Introdução à Teoria dos Números - Duração: 10 aulas de 50 minutos.*

Essa atividade deve ter como foco os conceitos de Divisibilidade, de M.D.C. e da Divisão Euclidiana, bem como, o uso do Algorítmo de Euclides. Pode-se escolher como material didático o capítulo 2. Deve-se dar importância ao Teorema que responde às perguntas da atividade anterior.

O uso de exemplos é essencial nessa atividade. Para isso, o professor deverá consultar os livros citados nas referências bibliográficas.

Atividade 4.3.6. *Avaliação da Aprendizagem - Duração: 2 aulas de 50 minutos.*

Essa atividade, a ser elaborada pelo professor, deverá conter Equações Diofantinas Lineares e tópicos de Teoria dos Números. O resultado dessa avaliação servirá de parâmetro para análise da aprendizagem dos estudantes.

Considerações Finais

O presente trabalho deve ser entendido em sua totalidade, pois o capítulo que trata das atividade didáticas está entrelaçado aos outros capítulos. Assim, todos os capítulos compõem a Transposição Didática proposta para o assunto Equações Diofantinas.

Nesse sentido, torna-se imprescindível a abordagem histórica, bem como o estudo, mesmo que apenas introdutório, dos tópicos de Teoria dos Números abordados no trabalho.

O material pode ser desenvolvido a partir do nono ano do Ensino Fundamental. Deve-se dar ênfase às aplicações das equações diofantinas lineares com duas variáveis no Ensino Fundamental e as aplicações das equações diofantinas lineares com três variáveis e a resolução por meio de fatoração e desigualdades no Ensino Médio.

Nas escolas públicas, cabe ao professor explorá-lo da forma que lhe pareça mais adequado, de modo a levar os estudantes à investigação e à pesquisa por meio de situações-problema instigadoras e curiosas. Pode ser, também, usado como material para uma preparação para as Olímpiadas de Matemática em relação às Equações Diofantinas.

Para esse desenvolvimento, sugere-se alguns livros citados nas Referências Bibliografia que subsidiarão o trabalho do professor, tais como HEFEZ [2011], HEFEZ [2009] e DOMINGUES [1991], que podem contribuir com este tema tão rico em aplicações envolvendo os números inteiros.

Referências

[1] HEFEZ, Abramo. Elementos de Aritmética. 2.ed. Rio de janeiro: SBM, 2011. Coleção Textos Universitários.

[2] HEFEZ. Iniciação à Aritmética. Rio de Janeiro: SBM/IMPA/MEC, 2009.

[3] ALENCAR FILHO, Edgard de. Teoria elementar dos números. São Paulo: Nobel, 2000.

[4] SANTOS, José Plínio Oliveira. Introdução à Teoria dos Números. 3.ed. Rio de Janeiro: IMPA, 2011.

[5] COUTINHO, S. C. Números Inteiros e Criptografia RSA. 3.ed. Rio de Janeiro: IMPA/SBM, 1997.

[6] EVES, Howard. Introdução à História da Matemática. Campinas,SP: Editora Unicamp, 2004.

[7] NETO, Antônio Caminha Muniz. Tópicos de Matemática Elementar Volume 5: Teoria dos Números. Rio de Janeiro: SBM, 2012. Coleção do professor de matemática.

[8] LINS, R. C.; GIMENEZ, J. Perspectivas em Aritmética e Álgebra para o Século XXI. 5.ed. Campinas, SP: Papirus, 2005. 176p.

[9] ROQUE, Tatiana. História da matemática Uma visão crítica, desfazendo mitos e lendas. 1.ed. São Paulo, SP: Zahar, 2012. 512p.

[10] DOMINGUES, Hygino Hugueros. Fundmentos de Aritmética. São Paulo: Atual, 1991.

[11] ANDREESCU, Titu; ANDRICA, Dorin; CUCUREZANU, Ion. An Introduction to Diophantine Equations. New Iork: Birkhauser, 2000.

[12] SINGH, Simon. O Último Teorema de Fermat. 11. ed. Rio de Janeiro, 2005.