UNIVERSIDADE FEDERAL DE RORAIMA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

ALTINO DA SILVA NETO

CONVITE ÀS EQUAÇÕES DIOFANTINAS: uma abordagem para a educação básica

Boa Vista - RR

2016

ALTINO DA SILVA NETO

CONVITE ÀS EQUAÇÕES DIOFANTINAS: uma abordagem para a educação básica

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática PROFMAT da Sociedade Brasileira de Matemática - SBM e Universidade Federal de Roraima - UFRR, como parte dos requisitos para a obtenção do título de MESTRE em Matemática.

Orientador: Prof. Dr. Alberto Martin Martínez Castañeda

Boa Vista - RR

2016

Dados Internacionais de Catalogação na publicação (CIP)
Biblioteca Central da Universidade Federal de Roraima

S586c Silva Neto, Altino da.
Convite às equações diofantinas: uma abordagem para a educação básica / Altino da Silva Neto. – Boa Vista, 2016.
152 f. : il.

Orientador: Prof. Dr. Alberto Martin Martinez Castañeda.

Dissertação (mestrado) – Universidade Federal de Roraima, Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional.

1 – Teoria dos números. 2 – Equações diofantinas. 3 – Equações diofantinas lineares. 4 – Equações diofantinas não lineares. I – Título. II – Castañeda, Alberto Martin Martinez (orientador).

CDU – 511.5

ALTINO DA SILVA NETO

CONVITE ÀS EQUAÇÕES DIOFANTINAS: uma abordagem para a educação básica

Dissertação de mestrado apresentada ao Programa de Pós-graduação em Matemática PROFMAT da Sociedade Brasileira de Matemática - SBM e Universidade Federal de Roraima - UFRR, como parte dos requisitos para a obtenção do título de MESTRE em Matemática.

Trabalho aprovado. Boa Vista - RR, 24 de agosto de 2016.

Prof. Dr. Alberto Martin Martínez Castañeda
Orientador/UFRR

Prof. Dr. Tomás Daniel Menéndez Rodríguez
UNIR

Prof. Dr. Joselito de Oliveira
UFRR

Boa Vista - RR
2016

Dedico este trabalho ao meu pai, o senhor Edivalne Alves da Silva (Capixaba), que acreditou em mim até mesmo naqueles momentos que nem eu mesmo acreditava. Obrigado pai. Sinto saudades dos seus abraços...

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me carregar em Seus braços, principalmente naqueles momentos de maior dificuldade.

A todos os professores do Profmat, pela paciência e empenho em dar o melhor de si para que pudéssemos alçar voos cada vez mais altos. Foram muitos sábados de dedicação.

Ao Prof. Dr. Alberto Martin Martínez Castañeda, que me recebeu de braços abertos. Lembro-me do dia que questionei se ele poderia ser o meu orientador. Naquela ocasião, após ter recebido um não, ele me recebeu com a seguinte frase: "Será uma honra ser o seu orientador". Senti-me o máximo. Sem a sua dedicação e incontestável/unânime competência, não teria saído nem da página um. Obrigado, professor.

À minha bela flor, a linda Vânia Celeste Gonçalves de Castro, companheira de todas as horas, a minha amada-amante, aquela que é a responsável pelas minhas maiores conquistas. Inclusive esta. Obrigado, minha bela flor.

Aos meus filhos, razão do meu viver, os meus maiores tesouros, Tales Pitico, Tiago Gostoso, Gabriel Gatinho, Alice Tchu-tchu-tchu e Dimítrio Hulk. Não poderia deixar de lado o príncipe da casa, o Ruffus Pico-pico.

Aos amigos de jornada, de altos e baixos, tropeços e vitórias. Em especial ao Gilson Nunes, com quem tive um contato maior. Juntos, resolvemos muitos problemas interessantes. Exemplo de persitência. Grande amigo. É uma pena que tenha subido aos céus antes de concluir a dissertação. Deus tinha propósitos muito maiores. Colocarei o seu nome na minha/nossa dissertação. Valeu, amigão.

RESUMO

Nesta dissertação, apresentamos os resultados de uma ampla pesquisa bibliográfica sobre as equações diofantinas e seus métodos de solução mais utilizados. A mais simples desta classe de equações é a da forma $ax + by = c$, com a, b e c números inteiros e $ab \neq 0$, chamada equação diofantina linear nas duas incógnitas x e y. No trabalho, expomos diversos métodos de resolução destas equações, em duas e três incógnitas. Para tanto, utilizamos conceitos de divisibilidade, divisão euclidiana, máximo divisor comum, números primos, dentre outros, que formam parte do currículo do Ensino Fundamental. No Brasil, as equações diofantinas não são comumente exploradas na Educação Básica, embora sejam perfeitamente compreensíveis nesse nível, como se mostra no texto do professor A. Guelfond, consultado na redação do trabalho. Na dissertação, incluímos, também, um capítulo sobre as contribuições de Diofanto para a Aritmética, que pode ser uma fonte de motivação para o estudo das equações diofantinas; e outro capítulo, ampliando as perspectivas sobre equações diofantinas não lineares. Esperamos que o trabalho seja uma fonte bibliográfica facilmente acessível aos professores da Educação Básica, e estimule seu interesse e criatividade para a introdução elementar desses conteúdos na prática docente e na preparação dos alunos para as Olimpíadas de Matemática.

Palavras-chave: Teoria dos números. Equações diofantinas. Equações diofantinas lineares. Equações diofantinas não lineares.

ABSTRACT

In this dissertation, the results of a wide bibliographic research about Diophantine equations and their most used solution methods are exposed. The simplest equation of these class is the one in the form $ax + by = c$, with a, b and c integers numbers and $ab \neq 0$, called Diophantine linear equation in the unknowns x and y. Divers solutions methods for these equations, in two or three unknowns are discussed. Therefore, concepts like divisibility, Euclidean division, grated common divisor, prime numbers, among others, that are included in the Elementary School's curriculum. In Brazil, Diophantine equations are not commonly exploited in Basic Education, even though they are perfectly understandable at this educational level, like Professor A. Guelfond shows in his book consulted in the redaction of the dissertation. There are also a chapter about Diophantus's contributions to Arithmetic, which can be a source of motivation to study the Diophantine equations; and another chapter, extending perspectives, about nonlinear Diophantine equations. We hope that the dissertation becomes a suitable easy accessible bibliographic font for Basic Education teachers and stimulates their interest and creativity for an elemental introducing of these contents in their teaching and in the student's training for Math Olympiads.

Key-words: Number theory. Diophantine equations. Linear diophantine equations. Nonlinear diophantine equations.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Conta a história que existia uma princesa que tinha muitos pretendentes. Cada um deles lhe enviava uma infinidade de coisas para poder chamar sua atenção. Levaram-lhe coisas de grande valor, tanto material quanto sentimental; porém, nenhum ganhou sua atenção. Até que chegou um dos aspirantes que tinha passado dias observando tudo que os demais haviam levado sem obter resposta da princesa, e antes de mostrar o que havia levado, colocou-lhe um par de óculos, deixando-a assombrada. E com essa ideia extremamente simples, conquistou o coração da princesa.

O que este último pretendente fez foi mudar a visão que todos tinham do problema. E certamente encontrou a solução.

Os problemas, em muitas ocasiões, tornam-se complicados porque só vemos uma única forma de resolvê-los. Por isso, é muito importante mudar o ponto de vista para resolvê-los, e assim, ter a possibilidade de encontrar novas e melhores soluções (VERA, 2014).

“Ao procurarmos a solução, podemos variar continuamente o nosso ponto de vista, a nossa maneira de encarar o problema. Temos de mudar de posição de quando em quando” (POLYA, 1995, p. 3) .

Dados os inteiros a, b e c, com $ab \neq 0$, chamamos de *equação diofantina linear* nas incógnitas x e y uma equação da forma $ax + by = c$. *Solução inteira* ou apenas *solução* é todo par de inteiros (x_0, y_0) tais que $ax_0 + by_0 = c$.

Na Teoria dos Números, encontramos o importante teorema que diz que a equação diofantina linear $ax + by = c$ admite infinitas soluções dadas por $x = x_0 + (b/d)t$ e $y = y_0 - (a/d)t$, desde que d divida c, onde d é máximo divisor comum de a e b e (x_0, y_0) é uma solução particular, com $t \in \mathbb{Z}$. Uma das nossas maiores inquietações foi saber se existem outras formas de resolver uma equação diofantina da forma $ax + by = c$, além daquela descrita no teorema citado anteriormente. Para nossa grata surpresa, em nossas pesquisas encontramos outros métodos de resolução, tanto em casos gerais quanto em casos específicos que, em certas circunstâncias, ajudar-nos-ão a otimizar nosso tempo na resolução de problemas.

Devido à pouca, ou nenhuma abordagem do tema “equações diofantinas não lineares" nos livros de graduação e da Educação Básica, sentimo-nos motivados em pesquisar esse assunto. Nesta linha, iremos discorrer, dentre outros, sobre as triplas pitagóricas, ideias geométricas e as equações de Pell.

Feitas essas considerações iniciais, frisamos que temos como objetivo geral estudar as equações diofantinas lineares (principalmente as de duas e três incógnitas) e as equações diofantinas não lineares, com enfoque nas de grau 2. Temos como objetivos específicos:

a) Estudar a história de Diofanto;

b) Revisar tópicos da Teoria dos Números que estejam relacionados com as equações diofantinas, visando subsidiar nossos estudos;

c) Estudar formas alternativas de resolver a equação diofantina linear $ax + by = c$ nas incógnitas x e y, onde a, b e c são inteiros dados, sendo $ab \neq 0$;

d) Estudar algumas equações diofantinas não lineares, mormente as de grau 2, apresentando diversos resultados clássicos.

Como forma de melhor organizar as ideias, dividimos o nosso trabalho em quatro capítulos, a saber:

1) História de Diofanto;

2) Fundamentos;

3) Equações Diofantinas Lineares e

4) Equações Diofantinas não Lineares.

No capítulo 1 (História de Diofanto) discutiremos sobre a vida de Diofanto, suas contribuições, seus métodos, problemas e equações diofantinas. Esse capítulo é destinado a professores e alunos da Educação Básica que estejam interessados na vida e nas obras de Diofanto de Alexandria, de uma forma mais panorâmica, que poderá ser utilizado como motivação ao estudo das equações diofantinas.

No capítulo 2 (Fundamentos) estudaremos alguns tópicos da Teoria dos Números relacionados com nossos estudos sobre as Equações Diofantinas. Dentre eles, destacamos: Os Princípios da Boa Ordenação e da Indução Matemática, a Divisão Euclidiana, o Algoritmo de Euclides, o Teorema Fundamental da Aritmética, as Congruências e as Classes Residuais, dentre outros. Esse capítulo é destinado a professores da Educação Básica que estejam interessados em rever alguns tópicos de Teoria dos Números e, também, a alunos do Ensino Fundamental e Ensino Médio, auxiliados pelos professores. Principalmente aqueles alunos que estão em treinamento para as Olimpíadas de Matemática.

No capítulo 3 (Equações Diofantinas Lineares) estudaremos o clássico teorema que versa sobre a resolução de equações diofantinas lineares nas incógnitas x e y, além dos métodos de Euler e dos “múltiplos". Usando congruências e noções de classes residuais, resolveremos algumas equações diofantinas lineares. Também veremos alguns casos práticos, a saber: Critério do Algarismo Final, Critério da Multiplicidade e Critério do Agrupamento que, em certas condições específicas, podem reduzir os passos na resolução de problemas. Destacamos que grande parte dos métodos utilizados para resolver equações diofantinas lineares nas incógnitas x e y também foram utilizados na resolução de equações diofantinas do tipo $ax + by + cz = c$, nas incógnitas x, y e z. Esse capítulo é, *a priori*, destinado a alunos do Ensino Fundamental, auxiliados pelos

professores. O estudo desse capítulo irá auxiliar na resolução de diversos problemas interessantes, além de ajudar o desenvolvimento do raciocínio lógico dos alunos por meio da união da resolução de cálculos com a interpretação de problemas. Para um bom entendimento deste capítulo, outros conceitos devem ser trabalhados como pré-requisitos, como, por exemplo, a divisão euclidiana, o algoritmo de Euclides e o máximo divisor comum (mdc) entre dois ou mais números inteiros, que são vistos no ensino fundamental.

No capítulo 4 (Equações Diofantinas não Lineares) abordaremos as triplas pitagóricas, os triângulos pitagóricos e o método geométrico, o descenso infinito de Fermat (ou descida de Fermat) e as equações de Pell. Também veremos os métodos da fatoração e o método aritmético modular. Utilizaremos, ainda, inequações para resolver equações diofantinas. Esse capítulo, o mais elegante, é destinado a alunos do Ensino Médio, auxiliados pelos professores. Ele pode ser fortemente utilizado por estudantes que estejam em treinamento para as Olimpíadas de Matemática.

Por fim, destacamos que aplicamos como metodologia de trabalho a pesquisa bibliográfica, onde consultamos, inicialmente, a bibliografia listada neste trabalho, seminários e entrevistas com o orientador. O resultado deste estudo foi escrito na forma de dissertação, utilizando o editor de texto **texmaker** do pacote **Latex**, e apresentado a uma banca avaliadora. O trabalho será publicado, após a aprovação da banca, no sítio do Departamento de Matemática desta Universidade. Os arquivos finais da dissertação serão enviados para publicação eletrônica no Sistema de Controle Acadêmico (SAC) do PROFMAT. Pretende-se, ainda, produzir um artigo e submetê-lo à revista eletrônica do Centro de Ciências e Tecnologia (CCT) da UFRR. Realizamos, ainda, inúmeras pesquisas na rede mundial de computadores, mais particularmente no Banco Indutor de Trabalhos[1].

[1] Acesse <http://bit.profmat-sbm.org.br/xmlui/>

1 HISTÓRIA DE DIOFANTO

Neste capítulo, discutiremos sobre a vida de Diofanto, suas contribuições, seus métodos, problemas e equações diofantinas.

1.1 Diofanto de Alexandria

Diofanto de Alexandria, que viveu por volta do século III, foi um grande expoente da matemática grega. Segundo Garbi (2009a), por volta de 250 d.C. um grande talento matemático floresceu na Grécia, sendo conhecido por Diofanto de Alexandria. Sua grande contribuição ocorreu nos campos da Álgebra e da Teoria dos Números. Contudo, pouco se sabe com exatidão sobre Diofanto, visto não ser exato o período em que viveu; mas, sabe-se que escreveu três tratados: *Arithmética*, em 13 livros, dos quais remanesceram 6, sobre Números Poligonais, do qual restaram fragmentos e Porismas, que foi perdido.

Faz observar Garbi (2009a) que o tratado *Arithmética* de Diofanto é uma obra de suma importância para o tratamento do tema conhecido, hoje, como Teoria dos Números, e deixa claro que seu autor era um gênio do mais alto quilate. Informa, ainda, que Euclides e outros já tinham realizado várias descobertas importantes nessa área; porém, Diofanto produziu avanços significativos ao exibir em seu livro vários exemplos das melhores qualidades de um teórico dos números.

Segundo Eves (2004), a obra *Arithmética* contou com inúmeros comentadores, mas foi Regiomontanus, em 1463, o primeiro estudioso a apresentar uma tradução do original grego descoberto em Pádua. Uma tradução de 1575 por Xilander recebeu diversos comentários elogiosos, sendo usada pelo francês Bachet de Méziriac que, em 1621, publicou a primeira edição do texto em grego, seguida de uma tradução latina acompanhada de notas. Em 1670, surge uma segunda edição, que é historicamente importante devido ao fato de conter notas marginais de Fermat que tanto incentivaram as pesquisas em Teorias dos Números.

Para Bashmakova (2015), a *Arithmética* é, sem dúvida, o resultado de numerosas investigações de Diofanto, devido à riqueza e singularidade de seus métodos e resultados. A *Arithmética* de Diofanto é um livro de problemas (189 no total), onde cada um deles vem acompanhado de sua solução (às vezes com mais de uma variante) e explicações necessárias. Por esse motivo, à primeira vista, parece não se tratar de uma obra teórica. Mas, se analisado atentamente, ver-se-á que os problemas foram escolhidos cuidadosamente, e servem de ilustração a métodos rigorosamente elaborados. Como era de costume na Antiguidade, os métodos não eram formulados de forma geral, mas se repetiam na solução dos problemas de um mesmo tipo.

De acordo com Eves (2004), a obra *Arithmética* é uma abordagem analítica da teoria algébrica dos números, que coloca Diofanto como um expoente no seu campo de atuação. A parte restante do trabalho é dirigida para a resolução de 130 problemas, numa variedade digna de consideração, que conduzem a equações do primeiro e do segundo graus. Somente uma cúbica muito particular é solucionada. O primeiro livro dedica-se a equações determinadas em uma incógnita e os demais se ocupam de equações indeterminadas de segundo grau, e, em alguns casos, de grau maior, em duas ou três incógnitas. É patente a ausência de métodos gerais e a aplicação repetida de simulação inventiva para as necessidades de cada problema. Diofanto só aceitava soluções entre os números racionais positivos e, em muitos casos, bastava-lhe apenas uma resposta do problema.

Faz observar Garbi (2009a) que, na *Arithmética*, Diofanto resolve 130 problemas de naturezas variadas, com o uso de equações do primeiro, segundo e até terceiro graus. Algumas das equações são do tipo indeterminado, com duas ou mais incógnitas que devem, além de atender à relação expressa pela equação, pertencer ao conjunto dos inteiros. Como, por exemplo, a equação $2x + 3y = 13$ é satisfeita pelo par inteiro $x = 2$, $y = 3$; porém, existiriam outros pares inteiros capazes de satisfazê-la? A resposta é sim, e esse foi um dos temas investigados e analisados por Diofanto, razão pela qual, aqueles e outros tipos de equações indeterminadas são hoje chamadas de Equações Diofantinas.

Ainda, segundo Eves (2004), existem enunciados de teoremas que adentram à Aritmética. Assim é que se encontram, sem prova, mas com uma referência a Porismas, que a diferença entre dois cubos racionais representa também a soma de dois cubos racionais. Essa é uma questão que posteriormente iria chamar a atenção de Viète, Bachet e Fermat. Existem muitas propostas em relação à representação de números como soma de dois, três ou quatro quadrados. Aliás, esse é um campo de investigação que iria ser completado por Fermat, Euler e Lagrange.

1.2 Contribuições de Diofanto

[...] Na época de Diofanto, o conceito de Álgebra não havia ainda sido explicitado. Assim, as questões aritméticas, ou as que hoje são chamadas de algébricas, eram trabalhadas através de raciocínios manifestos apenas por meio de palavras e não de símbolos. O exemplo, na sequência, ilustra melhor o que foi dito. Haja vista o clássico problema: “Em um terreno há cabras e galinhas, perfazendo um total de 32 cabeças e 88 pés. Quantos animais de cada tipo há em tal área?” Na atualidade, chamar-se-iam de x e y, respectivamente, os números de cabras e galinhas; adotar-se-ia um sistema de duas equações do primeiro grau com duas incógnitas e encontrar-se-iam as respostas. Como o sistema de símbolos não estava ainda disponível, o problema era solucionado

do seguinte modo: “Se todos os animais no terreno fossem galinhas, existiria um total de 2 vezes 32 pernas, isto é, 64 pernas. Como o total de pernas é 88, a diferença 88 menos 64, isto é, 24 pernas, devem vir das cabras. Como cada cabra participa com duas pernas para tal diferença, há 24 dividido por 2, isto é, 12 cabras no terreno. Como existem 32 animais, o número de galinhas é 32 menos 12, isto é, 20”. Como se observa, o problema foi solucionado sem o uso de símbolos, de uma forma que, na atualidade, tem-se por hábito chamar de “Álgebra Retórica” (GARBI, 2009b).

Segundo Roque (2012), a contribuição mais conhecida de Diofanto é a introdução de uma forma de representar o valor desconhecido em um problema, nomeando-o de *arithmos*, de onde vem o nome aritmética. O livro *Arithmética* apresenta uma coleção de problemas que integrava a tradição matemática da época. No livro I, ele inseriu símbolos, aos quais chama “designações abreviadas”, para designar 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:

ς (última letra da palavra arithmos, a quantidade desconhecida)
Δ^Y (primeira letra de dynamis, o quadrado da quantidade desconhecida)
K^Y (primeira letra de kybos, o cubo)
$\Delta^Y\Delta$ (o quadrado-quadrado) [quarta potência]
ΔK^Y (o quadrado-cubo) [quinta potência]
$K^Y K$ (o cubo-cubo) [sexta potência]

Para Garbi (2009b), Diofanto inseriu vários símbolos no estudo do que hoje se conhece como Álgebra: a incógnita era designada pela letra sigma minúscula (ς) última da palavra $\alpha\rho\iota\theta\mu o\varsigma$ equivalente a *aritmos* (número, em Grego); seu quadrado por Δ^Y, abreviação de $\Delta\upsilon\nu\alpha\mu\iota\varsigma$ equivalente a *dynamis* (potência); seu cubo de K^Y abreviação de $K\upsilon\beta o\varsigma$ que equivale a *kybos* (cubo); sua quarta potência por $\Delta^Y\Delta$ abreviação de *dynamodynamis* (potênciapotência); etc.; a igualdade por $\iota\sigma$, abreviação de $\iota\sigma o\varsigma$ (isos – igual) e a subtração por $\curlywedge$. Não havia um símbolo para a soma, que era expressa pela simples justaposição das parcelas, e os termos independentes da incógnita eram expressas pelo símbolo μ^0 monadei (unidade).

Faz observar Roque (2012) que o fato de existirem símbolos para as potências superiores ao cubo já denota a separação entre a aritmética de Diofanto e a geometria, pois, na geometria da época, uma potência maior que três para um número não tinha relação com nenhuma grandeza. À guisa de exemplo de como esses símbolos eram utilizados, descreve-se na sequência a solução do problema 27 do livro 1: “Encontrar dois números cuja a soma e produto sejam números dados”.

Vale ressaltar que Diofanto considera que a soma é 20 e o produto é 96. Este tipo de procedimento foi comum até que o simbolismo algébrico tivesse sido desenvolvido: alcançar resultados gerais com um caso específico, bastante representativo da

situação geral.

Suponha-se que a diferença entre dois números seja *arithmoi*. Começa-se por dividir a soma desses números (que é 20) em dois (obtendo 10). Em seguida, considera-se um *arithmos* somado e subtraído, na devida ordem, a cada uma das metades. Como a metade da soma é 10, tomando a metade subtraída de 1 *arithmos* mais a metade acrescentada de 1 *arithmos* obtém-se 20, que é a soma desejada. Para que o produto seja 96, multiplicam-se essas mesmas quantidades, atingindo 100 subtraído do quadrado do *arithmos* (um *dynamis*). Chega-se, assim, à conclusão de que o *dynamis* deve ser 4; portanto, o valor do *arithmos* é 2. Os valores procurados serão, por conseguinte, 10 mais 2 e 10 menos 2, ou seja, 12 e 8.

Explicação do procedimento utilizando tanto as abreviações de Diofanto quanto os símbolos atuais para as operações: deseja-se encontrar dois números com soma 20 e produto 96. Se estes números fossem iguais, cada um deles seria 10. Admitindo-se que a diferença entre eles seja 2ς, ou seja, os dois números procurados são obtidos retirando ς de um destes 10 e somando ς ao outro. Como a soma não se altera depois dessas operações, tem-se $10 - \varsigma + 10 + \varsigma = 20$. Porém, sabe-se também que o produto destes números é 96; portanto, pode-se escrever $(10 - \varsigma)(10 + \varsigma) = 96$. Conclui-se daí que o valor de ς deve ser 2. Assim, os números procurados são, respectivamente, 8 e 12.

Observem que uma primeira novidade é o fato de não se utilizar de nenhuma construção geométrica para a resolução do problema. Uma segunda novidade é que, na solução desse problema, atua-se com quantidades desconhecidas do mesmo modo que se opera com as conhecidas. Isto é, quantidades conhecidas e desconhecidas têm o mesmo estatuto. Portanto, supõe-se, de algum modo, que todas sejam conhecidas. Somente desse modo será possível inserir um símbolo para uma quantidade desconhecida. Essa é uma das características do pensamento algébrico (ROQUE, 2012).

Roque (2012) acreditava que para Diofanto o *arithmos* representa uma "quantidade indeterminada de unidades", distinto dos números, que são compostos de certa quantidade bem definidas de unidades. Contudo, ambos são submetidos ao mesmo tipo de tratamento. De igual modo, segundo Eecke (1926 apud ROQUE, 2012), as partes dos números são nomeadas de maneira adequada a estes números. Como o terço equivale a três, o quarto equivale a quatro, denominar-se-á também as partes dos números fixados acima, os *arithmes*, de maneira correspondente a estes números. Por exemplo, para o *arithme*, dir-se-á o inverso do *arithme*; para sua potência, dir-se-á o inverso do quadrado.

A natureza dos novos objetos, e as operações que se podem fazer com eles, está apoiada sobre a estrutura dos números determinados, que representam os números com exatidão. Com o intuito de resolver problemas, os vários tipos de números podem ser reunidos em grupos de mesma espécie, que equivalem aos nossos monômios ou

em expressões resultantes das operações entre espécies (ROQUE, 2012).

As soluções são apresentadas de modo discursivo, conforme o exemplo dado anteriormente. Porém, essa descrição é resumida pela utilização de símbolos (para números, frações, potências de números, incógnitas e monômios) que formam um princípio de linguagem algébrica. Essa forma de representação, que não é ainda totalmente simbólica, é conhecida como "álgebra sincopada". Os símbolos são empregados para resumir o texto que descreve a solução de um problema (ROQUE, 2012).

Vale ressaltar que os coeficientes numéricos da incógnita e de suas potências eram escritos depois delas. Por exemplo, $5x^2$ seria $x^2 5$. Como o sistema indo-arábico de numeração não havia sido criado, Diofanto grafava os números através de letras do alfabeto grego, o conhecido Sistema Jônico de Numeração. Sendo o início da simbolização da Álgebra, porém, como ainda eram empregadas abreviações de palavras juntamente com alguns símbolos, o sistema desenvolvido por Diofanto foi chamado de "Álgebra Sincopada" (GARBI, 2009b).

A principal diferença entre a sincopação de Diofanto e a notação algébrica moderna está na ausência de símbolos que especifiquem as operações e relações, bem como a notação exponencial. Nos problemas diofantinos, observou-se a utilização de generalizações de métodos, ainda que nem sempre se procurassem todas as soluções possíveis. Nas situações-problema, Diofanto adotava diversos números desconhecidos e, quando possível, em termos de um apenas (LIMA, 2011).

Faz observar Roque (2012) que diversos historiadores, como Heath, por exemplo, criam que é possível descobrir, em meio à variedade de exemplos, vários métodos comuns que podem servir a um enunciado geral. Em muitos casos, encontrar-se-iam mesmo regras gerais, como para a solução de equações determinadas, as chamadas "puras", que dispõem apenas de uma potência de quantidade ignorada de um grau qualquer.

Para Garbi (2009b), dentre as muitas contribuições de Diofanto à Matemática, duas delas merecem um comentário especial. Comece-se por algo que é sabido de todos, mas que poucos conseguem justificar: as regras dos sinais na multiplicação de números relativos. Nos primeiros contatos com a Aritmética, aprende-se que, na multiplicação, os sinais comportam-se da seguinte maneira:

$$+ \times + = +$$
$$+ \times - = -$$
$$- \times + = -$$
$$- \times - = +$$

Segundo Garbi (2009b), Diofanto, talvez, tenha sido o primeiro matemático a expor estes fatos de maneira clara, mostrando sua validade com base na chamada propriedade distributiva do produto no tocante à soma e à subtração. É essa propriedade, por exemplo, que justifica escrever-se:

a(b + c)=ab + ac

Ou

a(b – c)=ab – ac

Ou

a – b(c + d)=a – bc – bd

De onde decorrem as generalizações:

$+ \times + = +$

$+ \times - = -$

$- \times + = -$

No entanto, as coisas exigem um pouco mais de raciocínio quando se trata de mostrar que a multiplicação de dois números negativos dá um número positivo. Existem, pelo menos, duas formas de se chegar a esta conclusão. Começa-se por uma bastante intuitiva. Suponha a operação:

a – b=c

O que ocorre com o resultado desta subtração se for aumentado o subtraendo b de um valor, isto é, igual a d; ou seja, qual será o valor de a – (b + d)? É evidente que, se o subtraendo for aumentado de d, o resultado será c diminuído de d. Pelo mesmo raciocínio, se o subtraendo for diminuído de d, o resultado será aumentado de d, o que permite escrever:

Se a – b = c

Então a – (b – d) = c + d

Ou a – b – (– d) = c + d

Como a – b = c, tem-se

c – (–d) = c + d

e, subtraindo c dos dois lados, tem-se

– (–d) = +d

E está demonstrado que (–) x (–) = +.

A prova de Diofanto, entretanto, foi geométrica. Considere-se a figura sequencial, em que os números a, b, c e d são representados por segmentos de reta.

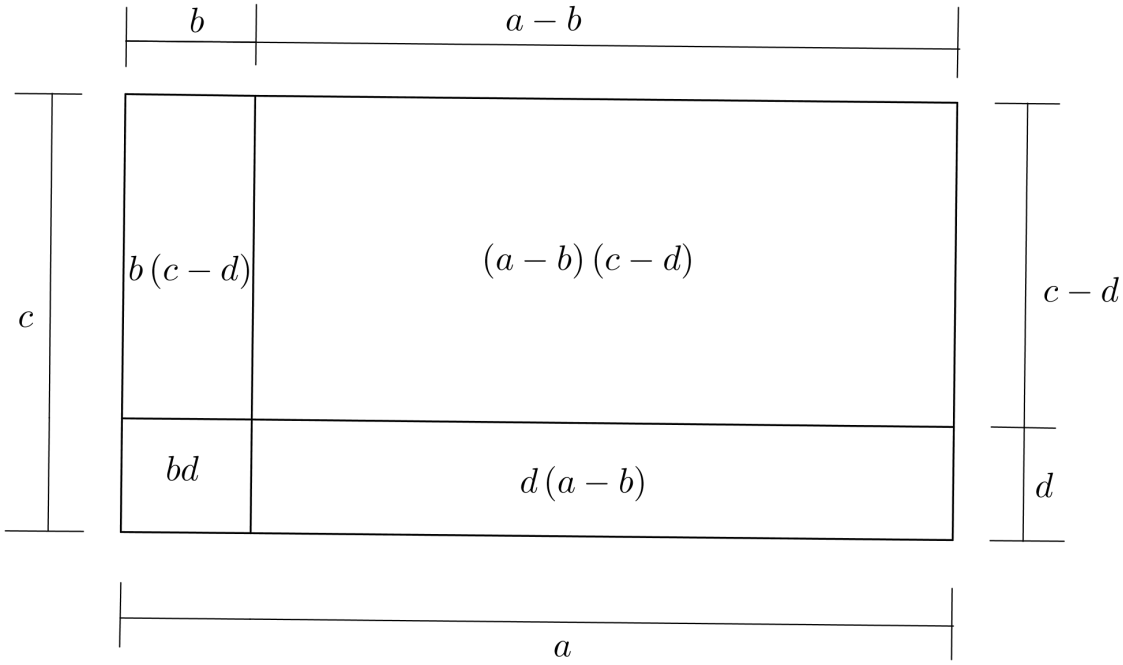

Figura 1 – Representação dos números **a**, **b**, **c** e **d** por segmentos de reta.
Fonte: Garbi (2009b), com adaptações.

Na figura 1, tem-se:

(a – b)(c – d) + b(c – d) + bd + d(a – b) = ac

(A área do retângulo maior é igual à soma das áreas dos quatro retângulos nele contidos).

O desenvolvimento dessa expressão, aceitando-se a validade da propriedade distributiva do produto no tocante à soma e à subtração, é:

(a – b)(c – d) + bc – bd + bd + ad – bd = ac ou

(a – b)(c – d) + bc + ad – bd = ac

Subtraindo bc e ad e adicionando bd a ambos os membros da igualdade (noção comum de Euclides), obtém-se:

(a – b)(c – d) = ac – ad – bc + bd

Isto demonstra que, no desenvolvimento de (a – b)(c – d), o produto (–b)(–d) é igual a +bd; de novo, a lei menos vezes menos dá mais. Vale ressaltar que diversos livros de Matemática registram que as regras dos sinais são convenções. Contudo, esse registro é um tanto simplista, visto que não se trata de convenções arbitrárias, mas de algo que tem de ser realizado se se quiser que a propriedade distributiva do produto equivalha generalizadamente no tocante à soma e à subtração (GARBI, 2009b).

1.3 Sobre os Métodos de Diofanto

É sabido que Diofanto dominava o método geral para determinar os pontos racionais de curvas de segundo grau. De acordo com Poincaré, este método pode ser aplicado a todas as curvas de gênero 0 [1] que tenham um ponto racional [2]. Diofanto também descobriu métodos gerais para localizar pontos racionais em curvas de terceiro grau. Deve-se observar que estes métodos foram muito diferentes daqueles aplicados para as curvas de segundo grau. O trabalho de Poincaré mostra que esses métodos de Diofanto podem ser utilizados para encontrar os pontos racionais de quaisquer curvas de gênero 1. Atualmente, estes são os únicos métodos conhecidos para encontrar pontos racionais de curvas algébricas (BASHMAKOVA, 2015).

Segundo Bashmakova (2015), a maioria de historiadores da ciência, ao contrário dos matemáticos, não deram o merecido valor ao trabalho de Diofanto. Muitos, inclusive, consideraram que Diofanto se limitava na busca de uma única solução e utilizava para isto procedimentos artificiais, diferentes para cada problema. Aliás, essa foi a opinião de Hermann Hankel, que afirmou que era difícil para um matemático moderno solucionar o problema 101 incluso depois de ter estudado 100 soluções de Diofanto. Assim, Diofanto mais segava que entusiasmava.

De acordo com Bashmakova (2015), é possível que as palavras de Hermann Hankel tenham sido escritas antes da obra de Henri Poincaré, na qual se esclareceu grande parte dos problemas relacionados às Equações Diofantinas. No entanto, escrevem Oskar Becker e Joseph E. Hofmann em seu livro História da Matemática, publicado em 1951, que Diofanto não oferece nenhum método geral, visto que adotava para cada problema um procedimento inesperado semelhante aos usados pelos matemáticos orientais.

Waerden (1954 apud BASHMAKOVA, 2015), faz comentários semelhantes em seu livro de álgebra ao assinalar que, via de regra, Diofanto se contentava com uma solução apenas sem esclarecer se essa é inteira ou fracionada. Assim, seu método muda de um caso a outro. No tocante às equações indeterminadas de segundo grau, Bartel Van der Waerden acrescenta que Diofanto consegue, de uma maneira surpreendentemente enganosa, que essa equação quadrática não tenha um final com $\boldsymbol{x^2}$ ou constante; e consegue uma solução racional para x. Contudo, isso diz respeito a um método comum ou corrente.

Uma avaliação mais precisa dos resultados de Diofanto se encontra na obra de

---

[1] Este é um conceito encontrado no estudo da Geometria Diofantina (ramo da Matemática relacionado com equações indeterminadas). Mas, em síntese, as retas e as curvas de segundo grau têm gênero 0 e as curvas de terceiro grau, satisfeitas certas condições, podem ser de gênero 0 ou 1. Fonte: Bashmakova (2015).

[2] Este é um outro conceito encontrado no estudo da Geometria Diofantina. O polinômio $f(x, y) = 0$ define no plano $\mathbb{R}^2$ uma curva algébrica e as soluções racionais de $f(x, y) = 0$ são denominadas **pontos racionais** da curva. Fonte: Bashmakova (2015).

H. G. Zeuthen, onde está registrado que, em geral, Diofanto trata de encontrar apenas um método e não um método geral, que contenha todas as soluções particulares. Contudo, não se deve dar muita importância a este fato, se se deseja compreender os resultados obtidos por Diofanto, uma vez que seus resultados particulares ocorrem somente porque ele atribui imediatamente quantidades auxiliares específicas usadas para resolver o problema (BASHMAKOVA, 2015).

Pode-se concluir que diversos gênios da matemática, como Fermat, Viète e outros, reconheceram e conhecem a importância de Diofanto para o ensino da Matemática, especialmente em se tratando da Álgebra.

1.4 Problemas Diofantinos

Boyer (2010) afirma que Diofanto buscava resolver problemas envolvendo diversos números desconhecidos, exprimindo de forma engenhosa todas as quantidades desconhecidas, quando possível, em termos de uma apenas. Dois problemas da *Arithmética* serão usados para ilustrar o método diofantino. Ao encontrar dois números, cuja soma seja 20 e a soma dos quadrados 208, os números são definidos por x e y, mas como 10 + x e 10 – x (para efeito de notação), então, (10 + x)^2 + (10 - x)^2 = 208; logo, $x = 2$. Então, os números buscados são 8 e 12. Diofanto discutiu também o problema semelhante em que a adição dos dois números e a soma dos cubos são dadas como sendo 10 e 370, na devida ordem.

Nesses problemas, Diofanto está trabalhando com uma equação determinada. Contudo, ele utilizou particularmente o mesmo método na análise indeterminada. Um problema solicita que se encontre dois números tais que cada um adicionado com o quadrado do outro dê um quadrado perfeito. Esse é um exemplo característico de análise diofantina, onde somente números racionais são aceitos como resposta. Ao resolver o problema, Diofanto não denominou os números de x e y, mas de x e $2x + 1$. Neste caso, o segundo, quando adicionado ao quadrado do primeiro, dará um quadrado perfeito independente do valor de x definido. Agora, impõe-se que $(2x + 1)^2 + x$ represente um quadrado perfeito. Neste ponto, Diofanto não alude à existência da infinidade de respostas. Ele se satisfaz em escolher um caso específico de quadrado perfeito; aqui, o número $(2x - 2)^2$, tal que quando igualado a $(2x + 1)^2 + x$ tenha como resultado uma equação linear em x. Neste caso, o resultado é $x = 3/13$, de maneira que o outro número, $2x + 1$, seja 19/13. Poder-se-ia, é claro, utilizar $(2x - 3)^2$ ou $(2x - 4)^2$, ou expressões análogas, em vez de $(2x - 2)^2$, e atingir a outros pares de números, tendo a propriedade desejada. Neste ponto, vê-se um esquema próximo de ser um “método” na obra de Diofanto: quando duas condições devem ser cumpridas por dois números, eles são definidos de maneira a atender a uma das duas condições; e, assim, ataca-se o problema de satisfazer à segunda. Isto é, em vez de trabalhar

equações simultâneas sobre duas incógnitas, Diofanto atua com condições sucessivas, de modo que surja um só número desconhecido no trabalho (BOYER, 2010).

Dentre os problemas indeterminados postos na obra *Arithmética*, existem alguns relativos a equações, como $x^2 = 1 + 30y^2$ e $x^2 = 1 + 26y^2$, que são exemplos da denominada "equação de Pell" $x^2 = 1 + py^2$; de novo, considera-se, nesse caso, que uma só solução é suficiente. De certo modo, é injustificado criticar Diofanto por se contentar com uma única resposta, uma vez que ele estava resolvendo problemas, não equações. Em certo sentido, a *Arithmética* se configura um compêndio de problemas de aplicação de álgebra, não um texto de álgebra. Sendo assim, Diofanto se aproxima dos algebristas babilônios; e sua obra é tida como "o mais belo florescimento da álgebra babilônica" (SWIFT, 1956 apud BOYER, 2010). De certa forma, tal caracterização é injustificada, pois os números usados por Diofanto são inteiramente abstratos e não dizem respeito a medidas de grãos ou dimensões de campos ou unidades monetárias, como no caso da álgebra egípcia e mesopotâmica. Ademais, Diofanto se interessava apenas por soluções racionais exatas; já os babilônios possuíam gostos computacionais e admitiam aproximações de soluções irracionais das equações. Por esse motivo, equações cúbicas, com raridade, surgem na obra de Diofanto, ao passo que entre os babilônios havia sido dada atenção à redução de cúbicas à forma padrão $n^3 + n^2 = a$, com o intuito de resolver, aproximadamente, utilizando interpolação em uma tabela de valores de $n^3 + n^2$ (BOYER, 2010).

Faz observar Boyer (2010) que não se pode estimar quantos problemas na *Arithmética* eram originais, ou se Diofanto havia tomado emprestado de outras obras. Em muitos dos problemas ou métodos é possível seguir o caminho até às origens babilônicas, posto que enigmas e exercícios são comuns reaparecerem geração após geração. Nos dias atuais, a *Arithmética* de Diofanto configura-se notavelmente original; contudo, é possível que essa impressão tenha como consequência a perda de coleções de problemas rivais. A visão moderna da matemática grega é consequência de um número relativamente pequeno de obras preservadas, e as impressões e conclusões obtidas deles são precárias.

Para Boyer (2010), indicações de que Diofanto tenha sido uma figura menos isolada do que se imagina está presente numa coleção de problemas possivelmente do início do segundo século de nossa era (portanto, presumivelmente anterior à *Arithmética*) em que surgem vários símbolos diofantinos. Contudo, Diofanto teve uma influência bem maior sobre a teoria moderna dos números do que qualquer outro algebrista grego não geométrico. De forma particular, Fermat descobriu seu célebre "grande" ou "último" teorema quando buscou generalizar um problema que tinha lido na *Arithmética* de Diofanto (II.8): dividir um determinado quadrado em dois quadrados.

1.5 Equações Diofantinas

Uma equação polinomial com qualquer número de incógnitas e coeficientes inteiros para a qual se busca soluções inteiras é conhecida como equação diofantina. Esse tipo de equação pode ter uma ou mais soluções, mas pode, também, não ter solução (OLIVEIRA, 2006).

Conforme Pommer e Pommer (2012), atualmente, na grande maioria dos livros-textos, as soluções são buscadas unicamente na forma de números inteiros, em virtude da possibilidade de se determinar uma solução equivalente, uma vez que, se "[...] uma dada equação tem soluções racionais, uma equação correspondente com soluções inteiras pode ser achada multiplicando a primeira equação por uma constante inteira" (ZERHUSEN; RAKES; MEECE, 1999, p. 2).

Zerhusen, Rakes e Meece (1999) afirmam que diversos problemas trabalhados no livro *Arithmética* de Diofanto são associados às chamadas equações diofantinas. Contudo, a referida obra não dispõe de problemas envolvendo as equações indeterminadas de primeiro grau, pois Diofanto não lhes atribuía importância. Afirmam que vários historiadores acreditam que o não desenvolvimento de um método algébrico geral por Diofanto deu-se devido às limitações do estilo sincopado de sua notação.

Contudo, o mesmo texto opõe-se ao discurso de Isabella Bashmakova, no livro Diophantus and Diophantine Equation, ao levar em consideração que muitas das técnicas utilizadas eram mais gerais que os críticos supunham. Porém, não são aceitas como tais em função das limitações em sua notação. Por exemplo, Diofanto não insere variáveis adicionais em um problema, visto que prefere inserir um inteiro de forma arbitrária. Ao se ler um problema posto no Livro *Arithmética*, tomo 2, pode ser observado que Diofanto tem consciência que qualquer inteiro servirá (ZERHUSEN; RAKES; MEECE, 1999, p. 3).

Faz observar Ribeiro (2014) que a resolução de inúmeros problemas em Teoria dos Números que requer soluções inteiras recai, em diversas situações, em equações do tipo: ax + by $=$ c, com a, b, c $\in \mathbb{Z}$. Essas equações são conhecidas como equações diofantinas lineares. Em muitos casos, essas equações não apresentam soluções, haja vista a equação: 2x + 4y $=$ 3. Observa-se que não existe solução inteira para a equação, visto que o primeiro membro da equação é par e jamais será igual ao segundo membro que é um número ímpar. É comum perguntar quais são as condições imprescindíveis e suficientes para que a equação diofantina linear apresente solução, e como fazer para encontrá-la. Nesses casos, é preciso recorrer a teoremas.

Para Savóis e Freitas (2015), equação diofantina linear em duas variáveis é um tipo de equação que, afora os conceitos especiais na sua resolução, como, por exemplo, a visão de solução geral da equação que é definida por meio da introdução de um parâmetro (conceito utilizado no estudo das equações paramétricas, em geo-

metria analítica), auxilia a resolver diversos problemas interessantes, além de ajudar o desenvolvimento do raciocínio lógico dos alunos por meio da união da resolução de cálculos com a interpretação de problemas. Contudo, para o ensino dessas equações, outros conceitos devem ser trabalhados como pré-requisitos, como, por exemplo, a divisão euclidiana, o algoritmo de Euclides e o máximo divisor comum (mdc) entre dois ou mais números inteiros.

2 FUNDAMENTOS

Neste capítulo, estudaremos alguns tópicos da Teoria dos Números relacionados com nossos estudos sobre as Equações Diofantinas. Dentre eles, destacamos: Os Princípios da Boa Ordenação e da Indução Matemática, a Divisão Euclidiana, o Algoritmo de Euclides, o Teorema Fundamental da Aritmética, as Congruências e as Classes Residuais, dentre outros.

2.1 Introdução

O conjunto dos números inteiros, usualmente denotado por $\mathbb{Z}$, pode ser construído formalmente a partir do conjunto $\mathbb{N}$ dos naturais. $\mathbb{N}$ é formalizado axiomaticamente segundo os conhecidos axiomas de Peano. Então, determina-se uma relação de equivalência conveniente no produto cartesiano $\mathbb{N} \times \mathbb{N}$. $\mathbb{Z}$ é definido como o conjunto das classes de equivalência em $\mathbb{N} \times \mathbb{N}$. As operações de adição e multiplicação de números inteiros se definem convenientemente no conjunto quociente. A partir daí se provam todas as propriedades conhecidas dos inteiros e o conjunto $\mathbb{N}$ resulta ser “algebricamente idêntico" a uma parte de $\mathbb{Z}$, especificamente a $\mathbb{Z}_+$. Este método de construção de $\mathbb{Z}$ está exposto em Ferreira (2013). Contudo, inspirados nas ideias de Hefez (2013), adotaremos uma apresentação axiomática-informal de $\mathbb{Z}$. De fato, assumiremos a existência de $\mathbb{Z}$ e enunciaremos como axiomas as propriedades **P1** a **P8**, que serão vistas na subseção 2.2.

Iniciemos, então, a nossa jornada com o *conjunto dos números inteiros*:

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

juntamente com as operações de adição $(a, b) \mapsto a + b$ e de multiplicação $(a, b) \mapsto a.b$ (denotamos $a.b$ também por $a \times b$, ou ainda ab) (HEFEZ, 2013, p. 2).

Neste conjunto $\mathbb{Z}$, Alencar Filho (1987, p. 1) destaca os subconjuntos:

1. Conjunto $\mathbb{Z}^*$ dos inteiros não nulos $(\neq 0)$:
   $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \neq 0\} = \{\pm 1, \pm 2, \pm 3, ...\}$

2. Conjunto $\mathbb{Z}_-$ dos inteiros não positivos (≤ 0) :
   $\mathbb{Z}_- = \{x \in \mathbb{Z} \mid x \leq 0\} = \{0, -1, -2, -3, ...\}$

3. Conjunto $\mathbb{Z}_+$ dos inteiros não negativos (≥ 0) :
   $\mathbb{Z}_+ = \{x \in \mathbb{Z} \mid x \geq 0\} = \{0, 1, 2, 3, ...\}$

4. Conjunto $\mathbb{Z}_-^*$ dos inteiros negativos (< 0) :
   $\mathbb{Z}_-^* = \{x \in \mathbb{Z} \mid x < 0\} = \{-1, -2, -3, ...\}$

5. Conjunto $\mathbb{Z}_+^*$ dos inteiros positivos (> 0) :
   $\mathbb{Z}_+^* = \{x \in \mathbb{Z} \mid x > 0\} = \{1, 2, 3, ...\}$

Note-se que o único elemento comum aos conjuntos $\mathbb{Z}_-$ e $\mathbb{Z}_+$ é o inteiro 0 (zero), e que os conjuntos $\mathbb{Z}_-^*$ e $\mathbb{Z}_+^*$ não possuem elemento comum, isto é, são disjuntos:

$$Z_- \cap \mathbb{Z}_+ = \{0\} \text{ e } \mathbb{Z}_-^* \cap \mathbb{Z}_+^* = \varnothing.$$

Portanto, o inteiro 0 (zero) não é negativo nem positivo, ou seja, o inteiro 0 (zero) é **neutro**.

Os inteiros positivos 1, 2, 3, ... são também denominados **inteiros naturais**, e, por isso, o conjunto dos inteiros positivos é habitualmente designado pela letra $\mathbb{N}$: $\mathbb{N} = \mathbb{Z}_+^*$ (ALENCAR FILHO, 1987, p. 2).

2.2 A Adição e a Multiplicação em $\mathbb{Z}$

Faz saber Hefez (2013, p. 3-4) que as operações de adição e de multiplicação em $\mathbb{Z}$ possuem as seguintes propriedades fundamentais, a partir das quais pode-se provar todas as propriedades algébricas de $\mathbb{Z}$:

P1 A adição e a multiplicação são *bem definidas*:
Para todos a, b, a', $b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$; então, $a + b = a' + b'$ e $a.b = a'.b'$.

P2 A adição e a multiplicação são *comutativas*:
Para todos a, $b \in \mathbb{Z}$, $a + b = b + a$ e $a.b = b.a$.

P3 A adição e a multiplicação são *associativas*:
Para todos a, b, $c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a.b).c = a.(b.c)$.

P4 A adição e a multiplicação possuem *elementos neutros*:
Para todo $a \in \mathbb{Z}$, $a + 0 = a$ e $a.1 = a$.

P5 A adição possui *elementos simétricos*:
Para todo $a \in \mathbb{Z}$, existe $b(= -a)$ tal que $a + b = 0$.

P6 A multiplicação é *distributiva* com relação à adição:
Para todos a, b, $c \in \mathbb{Z}$, tem-se $a.(b + c) = a.b + a.c$.

A propriedade **P1** é que permite somar um dado número a ambos os lados de uma igualdade, ou multiplicar ambos os lados por um mesmo número.

Note que o conjunto dos números inteiros é particionado em três subconjuntos:

$$\mathbb{Z} = \mathbb{Z}_+^* \cup \{0\} \cup \mathbb{Z}_-^*,$$

onde $\mathbb{Z}_-^*$ é o conjunto dos simétricos dos elementos de $\mathbb{Z}_+^*$. Vejamos uma consequência desses axiomas.

Proposição 2.2.1. $a.0 = 0$ *para todo* $a \in \mathbb{Z}$.

(Fonte: Hefez (2013, p. 4-5))

Demonstração. Temos das propriedades **P4** e **P6** que

$$a.0 = a(0 + 0) = a.0 + a.0.$$

Somando-se $-(a.0)$ aos membros extremos da igualdade, pelas Propriedades **P5**, **P3**, **P2** e **P4**, obtemos:

$$\begin{aligned} 0 &= -(a.0) + a.0 = -(a.0) + (a.0 + a.0) \\ &= (-(a.0) + a.0) + a.0 = 0 + a.0 \\ &= a.0 \end{aligned}$$

□

Proposição 2.2.2. *A adição é compatível e cancelativa com respeito à igualdade:* $\forall a, b, c \in \mathbb{Z}, a = b \iff a + c = b + c$.

(Fonte: Hefez (2013, p. 5))

Demonstração. A implicação $a = b \implies a + c = b + c$ é consequência do fato de a adição ser bem definida (Propriedade **P1**).

Suponha agora que $a + c = b + c$. Somando $(-c)$ a ambos os lados, obtemos o desejado. □

A operação de adição permite-nos definir uma nova operação chamada de *subtração*, como a seguir.

Dados dois números inteiros a e b, define-se o número b *menos* a, denotado por $b - a$, como sendo

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

Dizemos que $b - a$ é o resultado da *subtração* de a de b.

2.3 Ordenação dos inteiros

Admitiremos que em $\mathbb{Z}$ também valem as seguintes propriedades:

P7 *Fechamento* de $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todo $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $ab \in \mathbb{N}$.

P8 *Tricotomia*: Dados $a, b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

$$i)\, a = b; \qquad ii)\, b - a \in \mathbb{N}; \qquad iii)\, -(b - a) = a - b \in \mathbb{N}.$$

Diremos que a é *menor do que* b, simbolizado por $a < b$, toda vez que a propriedade ii anterior for verificada.

Com essa definição, temos que a propriedade iii anterior equivale a afirmar que $b < a$. Assim, a tricotomia nos diz que, dados $a, b \in \mathbb{Z}$, uma, e somente uma, das seguintes condições é verificada:

$$i)\, a = b; \qquad ii)\, a < b; \qquad iii)\, b < a.$$

Utilizaremos a notação $b > a$, que se lê b *é maior do que* a, para representar $a < b$.

Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z}; x > 0\} = \mathbb{N} \quad \text{e} \quad \{x \in \mathbb{Z}; x < 0\} = -\mathbb{N}.$$

Daí decorre que $a > 0$ se, e somente se, $-a < 0$ (HEFEZ, 2013, p. 7).

Proposição 2.3.1. *A relação "menor do que" é transitiva:*
$\forall a, b, c \in \mathbb{Z}, a < b \quad e \quad b < c \Longrightarrow a < c.$

(Fonte: Hefez (2013, p. 7-8))

Demonstração. Supondo $a < b$ e $b < c$, temos que $b - a \in \mathbb{N}$ e $c - b \in \mathbb{N}$. Como $\mathbb{N}$ é aditivamente fechado, temos que

$$c - a = (b - a) + (c - b) \in \mathbb{N},$$

logo, $a < c$. □

Proposição 2.3.2. *A adição é compatível e cancelativa com respeito à relação "menor do que":*
$\forall a, b, c \in \mathbb{Z}, a < b \iff a + c < b + c.$

(Fonte: Hefez (2013, p. 8))

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto,

$$(b + c) - (a + c) = b - a \in \mathbb{N},$$

o que implica que $a + c < b + c$.

Reciprocamente, suponha que $a + c < b + c$. Pela primeira parte da proposição, podemos somar $(-c)$ a ambos os lados da desigualdade, o que nos conduz ao resultado que desejamos provar. □

Proposição 2.3.3. *A multiplicação por elementos de* $\mathbb{N}$ *é compatível e cancelativa com respeito à relação "menor do que":*
$\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N}, a < b \iff ac < bc.$

(Fonte:Hefez (2013, p. 8-9))

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, pelo fato de $\mathbb{N}$ ser multiplicativamente fechado, temos,

$$(bc) - (ac) = (b - a)c \in \mathbb{N},$$

logo $ac < bc$.

Reciprocamente, suponha que $ac < bc$, com $c \in \mathbb{N}$. Pela tricotomia, temos três casos a analisar:
$(i) a = b$. Isso acarretaria $ac = bc$, o que é falso. $(ii) b < a$. Isso acarretaria, pela primeira parte da demonstração, que $bc < ac$, o que também é falso. $(iii) a < b$. Esta é a única possibilidade válida. □

Proposição 2.3.4. *A multiplicação é compatível e cancelativa com respeito à igualdade:*
$\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{Z}^*, a = b \iff ac = bc.$

(Fonte: Hefez (2013, p. 9))

Demonstração. A implicação $a = b \implies ac = bc$ vale também quando $c = 0$ e decorre imediatamente do fato de a multiplicação ser bem definida (Propriedade **P1**).

Suponha agora que $ac = bc$. Temos duas possibilidades:
$i)$ Caso $c > 0$. Se $a < b$, pela **Proposição 2.3.3**, temos que $ac < bc$, o que é um absurdo. Se $b < a$, pelo argumento acima, $bc < ac$, o que é um absurdo. Portanto, a única opção válida é $a = b$.
$ii)$ Caso $-c > 0$. A argumentação segue a mesma linha usada acima para o caso $c > 0$, levando em conta que $d < e$ se, e somente se, $-d > -e$. □

Segue-se daí que $\mathbb{Z}$ é um *domínio de integridade*, isto é, se a e b são inteiros tais que $ab = 0$, então $a = 0$ ou $b = 0$. De fato, se $a \neq 0$, então $ab = 0 = a0$. Pelo cancelamento de $a \neq 0$ segue-se que $b = 0$.

Essa propriedade admite a seguinte formulação contrapositiva:

Para todos $a, b \in \mathbb{Z}^*$ tem-se que $ab \neq 0$.

Note que a relação "$<$" não é uma relação de ordem, pois não é reflexiva. Podemos, no entanto, por meio dela, obter uma relação de ordem, como descrevemos a seguir.

Diremos que a é menor ou igual do que b, ou que b é maior ou igual do que a, escrevendo $a \leq b$ ou $b \geq a$, se $a < b$ ou $a = b$.

Note que $a \leq b$ se, e somente se, $b - a \in \mathbb{N} \cup \{0\}$. Com isso, é fácil verificar que essa nova relação é efetivamente uma relação de ordem, pois possui as seguintes propriedades:

1. É reflexiva: $\forall a \in \mathbb{Z},\ a \leq a$;
2. É antissimétrica: $\forall a, b \in \mathbb{Z},\ a \leq b$ e $b \leq a \Longrightarrow a = b$;
3. É transitiva: $\forall a, b, c \in \mathbb{Z},\ a \leq b$ e $b \leq c \Longrightarrow a \leq c$ (HEFEZ, 2013, p. 9-10).

2.4 Valor Absoluto

Chama-se *valor absoluto* (ou *módulo*) de um inteiro a o inteiro que se indica por $|a|$, e tal que

$$|x| = \begin{cases} a & se \quad a \geq 0 \\ -a & se \quad a < 0 \end{cases}$$

Assim, por exemplo:

$$|3| = 3 \quad \text{e} \quad |-5| = -(-5) = 5.$$

Consoante a definição anterior, para todo inteiro a, temos:

$$|a| \geq 0 \quad , \quad |a|^2 = a^2 = |-a|^2$$
$$|-a| = |a| \quad , \quad |a| \geq a.$$

O *valor absoluto* $|a|$ de um inteiro a pode ser definido pelas igualdades:

$$|a| = \sqrt{a^2} \quad , \quad |a| = \text{máx}(-a, a),$$

onde$\sqrt{a^2}$ denota a raiz quadrada não negativa de a^2 e máx$(-a, a)$ indica o maior do dois inteiros $-a$ e a.
Assim, por exemplo:
$|-6| = \sqrt{(-6)^2} = \sqrt{36} = 6$
$|-7|$ =máx$(-(-7), -7)$ =máx $(7, -7) = 7$ (ALENCAR FILHO, 1987, p. 39).

2.4.1 Propriedades do Valor Absoluto

Proposição 2.4.1. *Quaisquer que sejam os inteiros a e b:*
(i) $|ab| = |a| \,.\, |b|$*;*
(ii) $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$, *se* $b \neq 0$.

(Fonte: Alencar Filho (1987, p. 40))

Demonstração. (i) $|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}.\sqrt{b^2} = |a| \,.\, |b|$.
(ii) $\left|\frac{a}{b}\right| = \sqrt{\left(\frac{a}{b}\right)^2} = \sqrt{\frac{a^2}{b^2}} = \frac{\sqrt{a^2}}{\sqrt{b^2}} = \frac{|a|}{|b|}, b \neq 0.$ □

Proposição 2.4.2 (Desigualdade triangular)**.** *Quaisquer que sejam os inteiros a e b:*
$|a + b| \leq |a| + |b| \,.$

(Fonte: Alencar Filho (1987, p. 40))

Demonstração. $|a + b|^2 = (a + b)^2 = a^2 + b^2 + 2ab = |a|^2 + |b|^2 + 2ab$.
Como $ab \leq |ab| = |a| \,.\, |b|$, temos $2ab \leq 2\,|a| \,.\, |b|$, o que implica:
$|a + b|^2 \leq |a|^2 + |b|^2 + 2\,|a| \,.\, |b| = (|a| + |b|)^2$.
Por ser $|a + b| \geq 0$ e $|a| + |b| \geq 0$, temos:
$|a + b| \leq |a| + |b| \,.$ □

Proposição 2.4.3. *Quaisquer que sejam os inteiros a e b:*
(i) $|a - b| \leq |a| + |b|$*;*
(ii) $|a \pm b| \geq |a| - |b| \,.$

(Fonte: Alencar Filho (1987, p. 40-41))

Demonstração. (i) $|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$.
(ii) $|a| = |(a + b) + (-b)| \leq |a + b| + |-b| = |a + b| + |b|$.
Portanto:
$|a| - |b| \leq |a + b| \,.$ isto é: $|a + b| \geq |a| - |b|$ e
$|a - b| = |a + (-b)| \geq |a| - |-b| = |a| - |b| \,.$ □

Proposição 2.4.4. *Quaisquer que sejam os inteiros a e b:*
$|a - b| \geq ||a| - |b|| \,.$

(Fonte: Alencar Filho (1987, p. 41))

Demonstração. $|a-b|^2 = (a-b)^2 = a^2 + b^2 - 2ab = |b|^2 + |b|^2 - 2ab$.
Como $ab \leq |ab| = |a|\,|b|$, temos $2ab \leq 2\,|a|\,|b|$, o que implica
$|a-b|^2 \geq |a|^2 + |b|^2 - 2\,|a|\,|b| = (|a| - |b|)^2$, ou seja:
$|a-b|^2 \geq ||a| - |b||^2$.
Por ser $|a-b| \geq 0$ e $||a| - |b|| \geq 0$, temos:
$|a-b| \geq ||a| - |b||$. □

Proposição 2.4.5. *Quaisquer que sejam os inteiros x, a e c:*
(i) $\quad |x| < |a| \iff -a < x < a$;
(ii) $\quad |x-a| < c \iff a - c < x < a + c$.

(Fonte: Alencar Filho (1987, p. 42))

Demonstração. (i) $\quad |x|$= máx$(x, -x) < a \iff x < a$ e $-x < a$
$\iff x < a$ e $-a < x \iff -a < x < a$.
(ii) $\quad |x-a|$=máx$[(x-a), -(x-a)] < c$
$\iff (x-a) < c$ e $-(x-a) < c$
$\iff x < a + c$ e $a - c < x$
$\iff a - c < x < a + c$. □

2.5 Indução Matemática

2.5.1 Elemento Mínimo de um Conjunto de Inteiros

Seja **A** um conjunto de inteiros. Chama-se *elemento mínimo* de **A** um inteiro $a \in$ **A** tal que $a \leq x$ para todo $x \in$ **A** (ALENCAR FILHO, 1987, p. 79). Diremos que um subconjunto **A** de $\mathbb{Z}$ é *limitado inferiormente*, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in$ **A** (HEFEZ, 2013, p. 12).

Representa-se pela notação “mínA", que se lê: “mínimo de A" (ALENCAR FILHO, 1987, p. 79).

Proposição 2.5.1. *Se a é elemento mínimo de **A**, então este elemento é único.*

(Fonte: Alencar Filho (1987, p. 79))

Demonstração. Com efeito, se existisse um outro elemento mínimo b de **A**, teríamos:
(i) $\quad a \leq b$, porque $a =$mínA;
(ii) $\quad b \leq a$, porque $b =$mínA.
Logo, pela propriedade antissimétrica da relação de ordem em $\mathbb{Z}$, temos $a = b$. □

O elemento mínimo de **A**, se existe, denomina-se também *primeiro elemento* de **A** ou *menor elemento* de **A** (ALENCAR FILHO, 1987, p. 79).

Exemplo 2.5.1. *O conjunto* $A = \{x \in \mathbb{Z} | \, x > 12\}$ *tem o elemento mínimo, que é* 13 $(\textit{mín}A = 13)$*, porque* $13 \in A$ *e* $13 \leq x$ *para todo* $x \in A$.

(Fonte: Alencar Filho (1987, p. 79))

Exemplo 2.5.2. *O conjunto* $A = \{x \in \mathbb{N} | \, 3$ *divide* $x^2\}$ *tem o elemento mínimo, que é* 3 $(\textit{mín}A = 3)$*, porque* $3 \in A$ *(*3 *divide* $3^2 = 9$*) e* $3 \leq x$ *para todo* $x \in A$ $(1 \notin A$ *e* $2 \notin A)$.

(Fonte: Alencar Filho (1987, p. 79))

Exemplo 2.5.3. $\mathbb{Z}$ *e* $-\mathbb{N}$ *não são limitados inferiormente, nem possuem um menor elemento. Por outro lado,* $\mathbb{N}$ *é limitado inferiormente e possui 1 como menor elemento.*

(Fonte: Hefez (2013, p. 12))

2.5.2 Princípio da Boa Ordenação

Este importante princípio tem o seguinte enunciado: Todo conjunto não vazio **A** de inteiros não negativos possui o elemento mínimo. Em outros termos, todo subconjunto não vazio **A** do conjunto $\mathbb{Z}_+$ dos inteiros não negativos possui o elemento mínimo (ALENCAR FILHO, 1987, p. 80).

Ou ainda: Se **A** é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então **A** possui um menor elemento (HEFEZ, 2013, p. 12).

Exemplo 2.5.4. *O conjunto* $A = \{1, 3, 5, 7, ...\}$ *dos inteiros positivos ímpares é um subconjunto não vazio de* $\mathbb{Z}_+$*. Logo, pelo Princípio da Boa Ordenação,* ***A*** *possui o elemento mínimo, que é 1 (mín***A***=* 1*).*

(Fonte: Alencar Filho (1987, p. 80))

Exemplo 2.5.5. *O conjunto* $P = \{2, 3, 5, 7, 11, 13, ...\}$ *dos primos é um subconjunto não vazio de* $\mathbb{Z}_+$*. Logo, pelo Princípio da Boa Ordenação,* ***P*** *possui o elemento mínimo, que é* 2 *(mín***P***=* 2*).*

(Fonte: Alencar Filho (1987, p. 80))

Proposição 2.5.2. *Não existe inteiro* k *tal que* $0 < k < 1$.

(Fonte: Alencar Filho (1987, p. 80))

Demonstração. De fato, suponhamos, por absurdo, que existe $k \in \mathbb{Z}$ tal que $0 < k < 1$. Então, o conjunto:
$S = \{k \in \mathbb{Z} | \, 0 < k < 1\}$
não é vazio e, obviamente, é um subconjunto de $\mathbb{Z}_+$. Logo, pelo *Princípio da Boa Ordenação*, existe o elemento mínimo x_0 de S (mínS $= x_0$), e temos $0 < x_0 < 1$, o que implica:
$0 < x_0^2 < x_0 < 1$,

e isto contradiz a minimalidade de $x_0 \in S$. Logo, não existe inteiro algum compreendido entre 0 e 1; isto é, 1 é o menor inteiro positivo, ou seja, 1 é o elemento mínimo do conjunto $\mathbb{N}$ dos inteiros positivos. □

Corolário 2.5.1. *Dado um número inteiro n qualquer, não existe nenhum número inteiro m tal que $n < m < n + 1$.*

(Fonte: Hefez (2013, p. 13))

Demonstração. Suponhamos, por absurdo, que exista um número inteiro m satisfazendo as desigualdades $n < m < n + 1$; logo, $0 < m - n < 1$, o que contradiz a **Proposição 2.5.2**. □

Corolário 2.5.2. *Se a e b são inteiros positivos tais que o produto $ab = 1$, então $a = 1$ e $b = 1$.*

(Fonte: Alencar Filho (1987, p. 81))

Demonstração. Com efeito, pela **Proposição 2.5.2**, temos $1 \leq a$ e $1 \leq b$. Multiplicando ambos os membros da relação $1 \leq a$ por b, temos $b \leq ab$ ou (como $ab = 1$) $b \leq 1$. Então, $1 \leq b$ e $b \leq 1$, o que implica $b = 1$, valor que substituído na igualdade $ab = 1$ dá-nos $a.1 = 1$ ou $a = 1$. □

Corolário 2.5.3. *Se a e $b \in \mathbb{Z}$, com $b \neq 0$, então $|ab| \geq |a|$.*

(Fonte: Hefez (2013, p. 13))

Demonstração. De fato, como $b \neq 0$, pela **Proposição 2.5.2**, temos que $|b| \geq 1$. Logo,

$$|ab| = |a|\,|b| \geq |a|\,.$$

□

Corolário 2.5.4 (Propriedade Arquimediana)**.** *Sejam a e $b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$ (HEFEZ, 2013, p. 14). Ou então: Se a e b são dois inteiros positivos quaisquer, então existe um inteiro positivo n tal que $nb \geq a$ (ALENCAR FILHO, 1987, p. 81).*

Demonstração. (1ª) Como $|b| \neq 0$, da **Proposição 2.5.2** temos que $|b| \geq 1$, logo,

$$(|a| + 1)\,|b| \geq |a| + 1 > |a| \geq a.$$

O resultado segue se na desigualdade acima tomarmos $n = |a| + 1$, se $b > 0$ e $n = -(|a| + 1)$, se $b < 0$. □

Demonstração. (2ª) Suponhamos, por absurdo, que a e b são inteiros positivos para os quais $nb < a$, qualquer que seja o inteiro positivo n. Então, todos os elementos do conjunto:

$$S = \{a - nb | \, n \in \mathbb{N}\}$$

são inteiros positivos e, pelo *Princípio da Boa Ordenação*, S possui o elemento mínimo, digamos mín$S = a - kb$. Mas $a - (k + 1)b$ pertence a S, porque S contém todos os inteiros positivos desta forma. E como $a-(k+1)b = (a-kb)-b < a-kb$, segue-se que $a - kb$ não é o elemento mínimo de S, o que é uma contradição. Logo, a Propriedade Arquimediana é verdadeira. □

Para Hefez (2013, p. 14), um subconjunto T de $\mathbb{Z}$ será dito *limitado superiormente* se for vazio ou se existir um número $d \in \mathbb{Z}$ tal que

$$\forall x \in T, \quad x \leq d.$$

Nesse caso, diremos que d é uma *cota superior* para T.

Diremos que um elemento $b \in \mathbb{Z}$ é o *maior elemento* de T, se b é uma cota superior de T com $b \in T$.

Convencionamos também que o conjunto vazio é limitado superiormente, tendo qualquer número como cota superior.

É imediato verificar que o maior elemento de um conjunto, se existir, é único. Nesse caso, ele será denotado por max$T$.

O *Princípio da Boa Ordenação* possui a seguinte formulação:

Proposição 2.5.3. *Se T é um subconjunto de $\mathbb{Z}$ não vazio e limitado superiormente, então T possui um maior elemento.*

(Fonte: Hefez (2013, p. 14))

Demonstração. Suponha que d seja uma cota superior para T. Logo, $x \leq d$ para todo $x \in T$. Considere o conjunto

$$S = \{y \in \mathbb{Z} | \, y = d - x, \, x \in T\}.$$

O conjunto S é não vazio, e como $y = d - x \geq 0$, para todo $x \in T$, ele é limitado inferiormente. Logo, pelo *Princípio da Boa Ordenação*, ele tem um menor elemento $d - b$, com $b \in T$. Vamos mostrar que $b =$max$T$. De fato, se $x \in T$, temos que $d - x \in S$ e, portanto, $d - x \geq d - b$, o que implica que $x \leq b$. □

Uma das mais importantes consequências do *Princípio da Boa Ordenação* é o *Princípio da Indução Matemática*, que na axiomática de Peano consta como Axioma 4, e que apresentaremos a seguir:

Teorema 2.5.1 (Princípio da Indução Matemática)**.** *Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que*
(i) $a \in S$*;*
(ii) *Se S é fechado com respeito à operação de "somar 1" a seus elementos, ou seja,* $\forall n, n \in S \Longrightarrow n+1 \in S$.
Então, $\{x \in \mathbb{Z} | \, x \geq a\} \subset S$.
(Fonte: Hefez (2013, p. 15))

Demonstração. Ponhamos $S' = \{x \in \mathbb{Z} | \, x \geq a\}$ e suponhamos por absurdo que $S' \not\subset S$; logo, $S' - S \neq \varnothing$. Como esse conjunto é limitado inferiormente (por a), existe um menor elemento c em $S' - S$. Pelo fato de $c \in S'$ e $c \notin S$, temos que $c > a$. Portanto, $c - 1 \in S'$ e $c - 1 \in S$. Pela hipótese sobre S, temos que $c = (c-1)+1 \in S$, como $c \in S'$, obtemos uma contradição com o fato de $c \in S' - S$. □

Para Hefez (2013, p. 15), uma *sentença aberta* em n é uma frase de conteúdo matemático onde figura a letra n como palavra e que se torna uma sentença verdadeira ou falsa quando n é substituído por um número inteiro bem determinado.

Segue-se, do Princípio de Indução Matemática, o seguinte importante instrumento para provar teoremas:

Teorema 2.5.2. *Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em n. Suponha que*
(i) $p(a)$ *é verdadeiro, e que*
(ii) $\forall n \geq a, p(n) \Longrightarrow p(n+1)$ *é verdadeiro.*
Então, $p(n)$ é verdadeiro para todo $n \geq a$.
(Fonte: Hefez (2013, p. 15-16))

Demonstração. Seja $V = \{n \in \mathbb{Z} | \, p(n)$ é verdadeira$\}$, ou seja, V é o subconjunto dos elementos de $\mathbb{Z}$ para os quais $p(n)$ é verdadeiro.

Como por (i) $a \in V$ e por (ii)

$$\forall n, \quad n \in V \Longrightarrow n+1 \in V,$$

segue-se do *Princípio da Indução Matemática* que $\{x \in \mathbb{Z} | \, x \geq a\} \subset V$. □

Exemplo 2.5.6. *Demonstrar a proposição:*
$P(n) : \dfrac{1}{1.2} + \dfrac{1}{2.3} + \dfrac{1}{3.4} + ... + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}, \forall \in \mathbb{N}$.
(Fonte: Alencar Filho (1987, p. 84-85))

Demonstração.
(i) P(1) é verdadeira, visto que $\dfrac{1}{1.2} = \dfrac{1}{1+1}$.
(ii) Por hipótese, a proposição:

$$P(k): \frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+...+\frac{1}{k(k+1)}=\frac{k}{k+1},\ k\in\mathbb{N}$$

é verdadeira.

Adicionando $\frac{1}{(k+1)(k+2)}$ a ambos os membros desta igualdade, obtemos:

$$\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+...+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=$$

$$=\frac{k}{k+1}+\frac{1}{(k+1)(k+2)}=\frac{k^2+2k+1}{(k+1)(k+2)}=\frac{k+1}{k+2},$$

e isto significa que a proposição $P(k+1)$ é verdadeira. Logo, pelo *Princípio da Indução Matemática*, a proposição $P(n)$ é verdadeira para todo inteiro positivo n. □

Exemplo 2.5.7. *Demonstrar a proposição:*
$P(n): 2^n > n, \forall n \in \mathbb{N}$.

(Fonte: Alencar Filho (1987, p. 86))

Demonstração.
(i) $P(1)$ é verdadeira: $2^1 = 2 > 1$.
(ii) Por hipótese, a proposição:
$P(k): 2^k > k, \forall k \in \mathbb{N}$
é verdadeira. Portanto:
$2.2^k > 2k$ (multiplicando ambos os membros por 2) ou $2^{k+1} > k + k \geq k + 1$ (observe que $k \geq 1$) o que implica $2^{k+1} > k + 1$, isto é, a proposição $P(k+1)$ é verdadeira. Logo, pelo *Teorema da Indução Matemática*, a proposição $P(n)$ é verdadeira para todo inteiro positvo n. □

Exemplo 2.5.8. *Usando o Teorema da Indução Matemática, demonstrar a Propriedade Arquimediana: Se a e b são dois inteiros positivos, então existe um inteiro positivo n tal que $na \geq b$.*

(Fonte: Alencar Filho (1987, p. 88))

Demonstração.
(i) A proposição é verdadeira para $b = 1$: $2a > 1$.
(ii) Suponhamos, agora, que a proposição é verdadeira para $b = k$, $k \in \mathbb{N}$; isto é, que existe um inteiro positivo m_k tal que se tem $am_k \geq k$. Então:

$$a(m_k + 1) = am_k + a \geq k + a \geq k + 1,$$

de modo que a proposição é verdadeira para $b = k + 1$. Logo, pelo *Teorema da Indução Matemática*, a proposição é verdadeira para cada inteiro positivo b.

Observação 2.5.1. *Faz observar Alencar Filho (1987, p. 86-87) que na demonstração de uma proposição $P(n)$ pelo Teorema da Indução Matemática é obrigatório demonstrar sempre as partes (i) e (ii), isto é, demonstrar que $P(1)$ é verdadeira, e que $P(k)$ suposta verdadeira implica $P(k+1)$ também verdadeira, porque a veracidade de apenas uma dessas duas partes não basta para garantir a veracidade de $P(n)$ para todo inteiro positivo n. Assim, por exemplo, na proposição:*
$P(n) : n^3 + 11n = 6n^2 + 6, \forall n \in \mathbb{N},$
temos que
$P(1)$ *é verdadeira:* $1^3 + 11.1 = 6.1^2 + 6$,
$P(2)$ *é verdadeira:* $2^3 + 11.2 = 6.2^2 + 6$,
$P(3)$ *é verdadeira:* $3^3 + 11.3 = 6.3^2 + 6$.
No entanto, a proposição $P(n)$ é falsa, visto que $n^3 + 11n \neq 6n^2 + 6$ para todo inteiro $n \geq 4$.
Analisemos, agora, a proposição:
$P(n) : n + (n + 1) = 2n, \forall n \in \mathbb{N}.$
Supondo verdadeira a proposição:
$P(k) : k + (k + 1) = 2k, k \in \mathbb{N},$
temos:
$$(k+1) + (k+2) = \underbrace{k + (k+1)}_{=2k(hipótese)} + 2 = 2k + 2 = 2(k+1),$$
isto é, a proposição $P(k+1)$ também é verdadeira. No entanto, a proposição $P(n)$ é falsa, visto que
$P(1) : 1 + (1 + 1) \neq 2.1$
$P(2) : 2 + (2 + 1) \neq 2.2$
$P(3) : 3 + (3 + 1) \neq 2.3$
$\vdots$
$P(n) : n + (n + 1) \neq 2.n$ *para todo inteiro positivo n.*

O *Princípio da Indução Matemática* admite a variante chamada de *Princípio da Indução Completa*, ou *Segunda Forma do Princípio de Indução*, que é muito útil e que damos a seguir.

Teorema 2.5.3. *Seja $p(n)$ uma sentença aberta tal que*
(i) $p(a)$ *é verdadeiro, e que*
(ii) $\forall n, p(a)$ *e* $p(a+1)$ *e ... e* $p(n) \Longrightarrow p(n+1)$ *é verdadeiro.*
Então, $p(n)$ é verdadeiro para todo $n \geq a$.

(Fonte: Hefez (2013, p. 19))

Demonstração. Considere o conjunto
$V = \{n \in a + \mathbb{N};\ p(n)\}$.
Queremos provar que o conjunto $W = (a + \mathbb{N}) - V$ é vazio. Suponha, por absurdo, que vale o contrário. Logo, pelo *Princípio da Boa Ordenação*, W teria um menor elemento k, e, como sabemos de (i) que $a \notin W$, segue-se que existe n tal que $k = a + n > a$. Portanto, $a, a+1, ..., k-1 \notin W$; logo, $a, a+1, ..., k-1 \in V$. Por (ii) conclui-se que $k = k - 1 + 1 \in V$, o que contradiz o fato de $k \in W$. □

2.6 Divisão nos Inteiros

2.6.1 Divisibilidade

Alencar Filho (1987, p. 109) apresenta a seguinte definição de divisibilidade em $\mathbb{Z}$: Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a divide b se, e somente se, existe um inteiro q tal que $b = aq$.

Se a divide b, também se diz que a é um divisor de b; que a é um fator de b; que b é divisível por a ou que b é múltiplo de a.

Com a notação "$a|b$" indica-se que $a \neq 0$ divide b e, portanto, a notação "$a \nmid b$" significa que $a \neq 0$ não divide b.

A relação "a divide b $(a|b)$" denomina-se *relação de divisibilidade em* $\mathbb{Z}$.

Assim, por exemplo:

$2|6$, porque $6 = 2.3$;

$-5|30$, porque $30 = (-5).(-6)$;

$7|-21$, porque $-21 = 7.(-3)$;

$3 \nmid 10$, porque não existe $q \in \mathbb{Z}$ tal que 10=3q.

Observação 2.6.1. *Note-se que, se a é um inteiro, então:*
$a|0$, $a \neq 0$, *porque* $0 = a.0$;
$1|a$ *e* $-1|a$, *porque* $a = 1.a$ *e* $a = (-1)(-a)$;
$a|a$ *e* $-a|a$, $a \neq 0$, *porque* $a = a.1$ *e* $a = (-a)(-1)$.

Proposição 2.6.1. *Se $a|b$, então:*
$-a|b, \quad a|-b, \quad -a|-b, \quad |a| \mid |b|$.

(Fonte: Alencar Filho (1987, p. 109))

Demonstração. Com efeito, se $a|b$, então $b = aq$, e como $a \neq 0$, segue-se que $-a \neq 0$

e também $|a| \neq 0$. Portanto:

$$\begin{aligned} b &= (-a)(-q); \\ -b &= a(-q); \\ -b &= (-a)q; \\ |a| &= |a|\,|q|\,. \end{aligned}$$

□

Proposição 2.6.2. *Sejam a e b dois inteiros.*

(i) *Se $a|1$, então $a = 1$ ou $a = -1$;*

(ii) *Se $a|b$ e se $b|a$, então $a = b$ ou $a = -b$;*

(iii) *Se $a|b$, com $b \neq 0$, então $|a| \leq |b|$.*

(Fonte: Alencar Filho (1987, p. 110-111))

Demonstração.

(i) Sabemos que 1 e -1 são divisores de 1. Suponhamos que $a|1$. Então existe $q \in \mathbb{Z}$ tal que $1 = aq$ e, portanto:

$|a|\,.\,|q| = |aq| = 1$,

de modo que $|a| \neq 0$ e $|q| \neq 0$, isto é $|a| \geq 1$ e $|q| \geq 1$. Mas, se $|a| > 1$, então

$|a|\,.\,|q| > |q|$ e $|a|\,.\,|q| > |1|$,

o que é impossível. Logo, $|a| = 1$; isto é, $a = 1$ ou $a = -1$.

(ii) Se $a|b$ e se $b|a$, então:

$b = aq$ e $a = bq_1$, com $q, q_1 \in \mathbb{Z}$,

o que implica:

$a = aqq_1$ e $qq_1 = 1$,

e esta última igualdade ocorre quando $q = q_1 = 1$ ou $q = q_1 = -1$, o que implica:

$a = b$ ou $a = -b$.

(iii) Se $a|b$ com $b \neq 0$, então $b = aq$, com $q \neq 0$. Portanto:

$|q| \geq 1$ e $|b| = |a|\,.\,|q| \geq |a|\,.$ □

Faz observar Hefez (2013, p. 49) que, em particular, se $a \in \mathbb{Z}$ e $a|1$, então $0 < |a| \leq 1$, logo $|a| = 1$ e, portanto, $a = \pm 1$. Ou seja, a partir do resultado do item (iii) da **Proposição 2.6.2** damos outra demonstração para o item (i) da mesma proposição.

Note que, se $a \neq \pm b$, então $|a| < |b|$, visto que $|a| = |b|$ se, e somente se, $a = \pm b$ (ALENCAR FILHO, 1987, p. 111).

Como para $b \neq 0$, temos que todo divisor a de b é tal que $|a| \leq |b|$; segue-se que, nesse caso, que b tem um número finito de divisores que estão no intervalo $-|b| \leq a \leq |b|$ (HEFEZ, 2013, p. 49).

Proposição 2.6.3. *Sejam a, b e c inteiros;*

(i) *Se $a|b$ e se $c \neq 0$, então $ac|bc$;*

(ii) *Se $ac|bc$, então $a|b$;*

(iii) *Se $a|b$ e se $c|d$, então $ac|bd$;*

(iv) *Se $a|b$ e se $b|c$, então $a|c$;*

(v) *Se $a|(b \pm c)$, então $a|b \iff a|c$;*

(vi) *Se $a|b$ e se $a|c$, então $a|(bx + cy)$, $\quad x, y \in \mathbb{Z}$.*

(Fonte: Alencar Filho (1987, p. 111-112))

Demonstração.

(i) Como $a \neq 0$, temos $ac \neq 0$. Por outro lado, se $a|b$, então $b = aq$, com $q \in \mathbb{Z}$. Portanto:

$$bc = (ac)q \quad \text{e} \quad ac|bc.$$

(ii) Como $ac \neq 0$, segue-se que $a \neq 0$ e $c \neq 0$. Por outro lado, se $ac|bc$, então $bc = acq$, com $q \in \mathbb{Z}$. Portanto:

$$b = aq \quad \text{e} \quad a|b.$$

(iii) Se $a|b$ e se $c|d$, então $b = aq$ e $d = cq_1$, com $q, q_1 \in \mathbb{Z}$. Portanto:

$$bd = (ac)(qq_1) \quad \text{e} \quad ac|bd.$$

(iv) Se $a|b$ e se $b|c$, então $b = aq$ e $c = bq_1$, com $q, q_1 \in \mathbb{Z}$. Portanto:

$$c = a(qq_1) \quad \text{e} \quad a|c.$$

(v) Suponhamos que $a|(b + c)$. Logo, existe $q \in \mathbb{Z}$ tal que $b + c = aq$.

Agora, se $a|b$, temos que existe $q_1 \in \mathbb{Z}$ tal que $b = aq_1$. Juntando as duas igualdades anteriores, temos

$$aq_1 + c = aq,$$

donde segue-se que $c = (q - q_1)a$, logo $a|c$.

A prova da implicação contrária é inteiramente análoga.

Por outro lado, se $a|(b-c)$ e se $a|b$, pelo caso anterior, temos $a|-c$, o que implica $a|c$.

(vi) Se $a|b$ e se $a|c$, então $b = aq$ e $c = aq_1$, com $q, q_1 \in \mathbb{Z}$. Portanto, quaisquer que sejam os inteiros x e y, temos:

$$bx + cy = aqx + aq_1y = a(qx + q_1y)$$

e

$$a|(bx + cy).$$

□

Faz observar Alencar Filho (1987, p. 112) que, em particular, se $a|b$ e se $a|c$, então: $a|(b + c)$ e $a|(b - c)$.

O item (vi) da propriedade anterior admite uma óbvia generalização:

$$\text{Se } a|b_k,\ k = 1, 2, 3, ..., n, \text{ então } a|(b_1x_1 + b_2x_2 + ... + b_nx_n)$$

quaisquer que sejam os inteiros $x_1, x_2, ..., x_n$ (ALENCAR FILHO, 1987, p. 112).

Faz observar Hefez (2013, p. 49), que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, pois:

(i) é reflexiva: $\forall a \in \mathbb{N},\ a|a$.

(ii) é transitiva: se $a|b$ e $b|c$, então $a|c$.

(iii) é antissimétrica: se $a|b$ e $b|a$, então $a = b$.

Entretanto, a relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois, apesar de ainda ser reflexiva e transitiva, ela não é antissimétrica. Da fato, $-2|2$ e $2|-2$, mas $2 \neq -2$.

As proposições a seguir são de grande utilidade.

Proposição 2.6.4. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$.*

(Fonte: Hefez (2013, p. 49))

Demonstração. Vamos provar isso usando o *Princípio da Indução Matemática*.

A afirmação é verdadeira para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.

Suponhamos, agora, que $(a - b)|(a^n - b^n)$. Escrevamos

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

Como $(a - b)|(a - b)$ e, por hipótese, $(a - b)|(a^n - b^n)$, decorre da igualdade acima e do item (vi) da **Proposição 2.6.3** que $(a - b)|(a^{n+1} - b^{n+1})$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. □

Proposição 2.6.5. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

(Fonte: Hefez (2013, p. 50))

Demonstração. Vamos provar isso usando o *Princípio da Indução Matemática*.

A afirmação é verdadeira para $n = 0$, pois $a + b$ divide $a^1 + b^1 = a + b$.

Suponhamos, agora, que $(a + b)|(a^{2n+1} + b^{2n+1})$. Escrevamos

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

Como $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$ e, por hipótese, $(a + b)|(a^{2n+1} + b^{2n+1})$, decorre das igualdades acima e do item (vi) da **Proposição 2.6.3** que $(a+b)|(a^{2(n+1)+1}+ b^{2(n+1)+1})$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. □

Proposição 2.6.6. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.*

(Fonte: Hefez (2013, p. 50))

Demonstração. Vamos provar isso usando o *Princípio da Indução Matemática*.

A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$.

Suponhamos, agora, que $(a + b)|(a^{2n} - b^{2n})$. Escrevamos

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

Como $a+b$ divide $a^2-b^2 = (a+b)(a-b)$ e, por hipótese, $(a+b)|(a^{2n}-b^{2n})$, decorre das igualdades acima e do item (vi) da **Proposição 2.6.3** que $(a + b)|(a^{2(n+1)} - b^{2(n+1)})$, estabelecendo, assim, o resultado para todo $n \in \mathbb{N}$. □

Exemplo 2.6.1. *Mostrar que, se a soma de dois inteiros quaisquer é divisível por 2, então a sua diferença também é divisível por 2.*

(Fonte: Alencar Filho (1987, p. 115))

Demonstração. Sejam a e b dois inteiros cuja soma $a + b$ é divisível por 2, ou seja, $2|(a + b)$. Como $2|2b$, segue que $2|\,[(a + b) - 2b]$ (**Proposição 2.6.3**, (vi)), isto é, $2|(a - b)$. □

Exemplo 2.6.2. *Mostrar que, se $a|(4n + 3)$ e se $a|(2n + 1)$, então $a = \pm 1$.*

(Fonte: Alencar Filho (1987, p. 115-116))

Demonstração. Com efeito: $a|\,[(4n + 3) + (-2)(2n + 1)]$ (**Proposição 2.6.3**, (vi)) ou seja, $a|1$ o que implica $a = \pm 1$ (**Proposição 2.6.2**, (i)). □

Exemplo 2.6.3. *Mostrar que, se $n^2 + 1$ é divisível por $n + 1$, então $n = 1$.*

(Fonte: Alencar Filho (1987, p. 116))

Demonstração. Como:

$$n - 1 = n(n + 1) - (n^2 + 1).$$

Se $(n + 1)|(n^2 + 1)$, decorre da igualdade acima e do item (vi) da **Proposição 2.6.3** que $(n + 1)|(n - 1)$, o que somente é possível se $n - 1 = 0$, isto é, se $n = 1$. □

Exemplo 2.6.4. *Mostrar que a expressão $10^n(9n - 1) + 1$ é divisível por 9, qualquer que seja o inteiro positivo n.*

(Fonte: Alencar Filho (1987, p. 116))

Demonstração. Com efeito:

$$\begin{aligned} 10^n(9n-1)+1 &= 9n.10^n-(10^n-1) \\ &= 9n.10^n-\underbrace{9...9}_{n\,vezes} \\ &= 9n.10^n-9\,\underbrace{1...1}_{n\,vezes} \\ &= 9(n.10^n-\underbrace{1...1}_{n\,vezes}), \end{aligned}$$

ou seja, $9|10^n(9n-1)+1$, qualquer que seja o inteiro positivo n. □

Exemplo 2.6.5. *Mostrar que, se $c=ab$, com $a\neq\pm1$, então $|b|<|c|$.*

(Fonte: Alencar Filho (1987, p. 117-118))

Demonstração. Com efeito, se $c=ab$, então $b|c$. Logo, pelo item (iii) da **Proposição 2.6.2**:$|b|\leq|c|$. Mas, $|c|=|a|\,|b|$, de modo que, se $|b|=|c|$, então $|a|=1$; isto é, $a=\pm1$. E como $a\neq\pm1$, segue-se que $|b|<|c|$. □

Exemplo 2.6.6. *Sejam a e b dois inteiros positivos. Mostrar que a relação "$a^a|b^b$"não implica necessariamente $a|b$.*

(Fonte: Alencar Filho (1987, p. 118))

Demonstração. Com efeito:

$4^4|10^{10}$, mas $4\nmid10$;
$9^9|21^{21}$, mas $9\nmid21$.

□

Exemplo 2.6.7. *Sendo n um inteiro positivo, mostrar que $665|(9^{3n}-8^{2n})$.*

(Fonte: Alencar Filho (1987, p. 118))

Demonstração. Como:

$$9^{3n}-8^{2n}=3^{6n}-2^{6n}=(3^6)^n-(2^6)^n$$

e

$$3^6-2^6=665.$$

Tomando $a=3^6$ e $b=2^6$, temos, pela **Proposição 2.6.4**, que

$$665=(3^6-2^6)|\left[(3^6)^n-(2^6)^n\right]=(9^{3n}-8^{2n})$$

. □

Observação 2.6.2. *Faz observar Hefez (2013, p. 21) que uma Progressão Aritmética (PA) é uma sequência de números reais* (a_n) *tal que* a_1 *é dado e, para todo* $n \in \mathbb{N}$ *tem-se que*

$$a_{n+1} = a_n + r,$$

onde r *é um número real fixo chamado razão. Nestas condições, temos:*

a) $a_n = a_1 + (n-1)r$.

b) Se $S_n = a_1 + ... + a_n$, *então:*

$$S_n = \frac{(a_1 + a_n)n}{2}.$$

Observação 2.6.3. *Faz observar Hefez (2013, p. 21) que Progressão Geométrica (PG) é uma sequência de números reais* (a_n) *tal que* a_1 *é dado e, para todo* $n \in \mathbb{N}$ *tem-se que*

$$a_{n+1} = a_n q,$$

onde q *é um número real fixo, diferente de* 0 *e de* 1, *chamado razão. Nestas condições, temos:*

a) $a_n = a_1 q^{n-1}$.

b) Se $S_n = a_1 + ... + a_n$, *então:*

$$S_n = a_1 \frac{q^n - 1}{q - 1} \quad \textit{ou} \quad S_n = \frac{a_n q - a_1}{q - 1}.$$

Exemplo 2.6.8. *Mostrar que a soma de* $2n+1$ *inteiros consecutivos é divisível por* $2n+1$.

(Fonte: Alencar Filho (1987, p. 116-117))

Demonstração. Denotando por k o inteiro médio, a soma dos $2n + 1$ inteiros consecutivos está abaixo representada:

$$(k-n) + (k-n+1) + ... + (k-1) + k + (k+1) + ... + (k+n-1) + (k+n).$$

Observando que a expressão acima é a soma dos $2n + 1$ termos consecutivos de uma PA de primeiro termo $(k - n)$, último termo $(k + n)$ e razão 1, temos:

$$(k-n) + (k-n+1) + ... + (k-1) + k + (k+1) + ... + (k+n-1) + (k+n) =$$

$$= \frac{[(k-n) + (k+n)]\,(2n+1)}{2} = (2n+1)k$$

o que implica

$$(2n+1)|\,[(k-n)+(k-n+1)+...+(k-1)+k+(k+1)+...+(k+n-1)+(k+n)]$$

ou seja, a soma de $2n+1$ inteiros consecutivos é divisível por $2n+1$. □

Exemplo 2.6.9. *Calcular a soma:*

$$S_n = 1 + 11 + 111 + ... + 111...1$$

sendo a última parcela formada de n algarismos 1.

(Fonte: Alencar Filho (1987, p. 120))

Resolução.

$$\begin{aligned} 9S_n &= 9 + 99 + 999 + ... + 999...9 \\ &= (10-1) + (10^2-1) + (10^3-1) + ... + (10^n-1) \\ &= (10 + 10^2 + 10^3 + ... + 10^n) - n \end{aligned}$$

Na última igualdade, a soma dentro dos parênteses é a soma dos n termos de uma PG finita, cujo primeiro termo e a razão são iguais a 10. Assim:

$$\begin{aligned} (10 + 10^2 + 10^3 + ... + 10^n) &= \frac{10(10^n-1)}{10-1} \\ &= \frac{1}{9}(10^{n+1} - 10) \end{aligned}$$

Portanto:

$$9S_n = \frac{1}{9}(10^{n+1} - 10) - n$$

e

$$S_n = \frac{1}{81}(10^{n+1} - 9n - 10).$$

Exemplo 2.6.10. *Calcular a soma:*

$$S = 1 + 2.2 + 3.2^2 + 4.2^3 + 5.2^4 + ... + 100.2^{99}.$$

(Fonte: Alencar Filho (1987, p. 121))

Resolução.

A soma dada S pode escrever-se na forma a seguir indicada:

$$\begin{array}{rcccccccccccccc} S &=& 1 &+& 2 &+& 2^2 &+& 2^3 &+& ... &+& 2^{98} &+& 2^{99} &+ \\ & & &+& 2 &+& 2^2 &+& 2^3 &+& ... &+& 2^{98} &+& 2^{99} &+ \\ & & & & &+& 2^2 &+& 2^3 &+& ... &+& 2^{98} &+& 2^{99} &+ \\ & & & & & & & & 2^3 &+& ... &+& 2^{98} &+& 2^{99} &+ \\ & & & & & & & & & & \vdots & & & & \\ & & & & & & & & & & & & 2^{98} &+& 2^{99} &+ \\ & & & & & & & & & & & & & & 2^{99} & \end{array}$$

onde cada linha é a soma dos termos de uma PG de razão 2. Portanto:

$$S = 1(2^{100} - 1) + 2(2^{99} - 1) + 2^2(2^{98} - 1) + 2^3(2^{97} - 1) + ... + 2^{98}(2^2 - 1) + 2^{99}(2 - 1)$$

ou seja:

$$\begin{aligned} S &= (2^{100} - 1) + (2^{100} - 2) + (2^{100} - 2^2) + (2^{100} - 2^3) + ... + (2^{100} - 2^{98}) + (2^{100} - 2^{99}) \\ &= 100.2^{100} - (1 + 2 + 2^2 + 2^3 + ... + 2^{98} + 2^{99}) \\ &= 100.2^{100} - 1(2^{100} - 1) \\ &= 99.2^{100} + 1. \end{aligned}$$

Exemplo 2.6.11. *Determinar a soma dos n primeiros termos da sequência:*

$$1, (1 + 2), (1 + 2 + 2^2), ..., (1 + 2 + 2^2 + ... + 2^{n-1}).$$

(Fonte: Alencar Filho (1987, p. 123))

Resolução.
O enésimo termo $(1 + 2 + 2^2 + ... + 2^{n-1})$ da sequência dada é a soma dos termos de uma PG de razão 2 e o valor deste termo é $2^n - 1$. Logo, a soma dos n primeiros termos da sequência dada é:

$$\begin{aligned} S &= (2^1 - 1) + (2^2 - 1) + (2^3 - 1) + ... + (2^n - 1) \\ &= (2^1 + 2^2 + 2^3 + ... + 2^n) - (\underbrace{1 + 1 + 1 + ... + 1}_{n\,vezes}) \\ &= (2^{n+1} - 2) - n \\ &= 2^{n+1} - n - 2. \end{aligned}$$

2.6.1.1 Divisão Euclidiana

Teorema 2.6.1. *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que*

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

(Fonte: Hefez (2013, p. 53))

Demonstração. Considere o conjunto

$$S = \{x = a - by;\ y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela *Propriedade Arquimediana*, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$; logo, $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0; logo, pelo *Princípio da Boa Ordenação*, temos que S possui um menor elemento r.

Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos, por absurdo, que $r \geq b$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$; logo, $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.
Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b|\,|q - q'| = |r' - r| < |b|\,,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$. □

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de a por b.

Da divisão euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a.

Exemplo 2.6.12. *Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:*
(i) *o resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q$; ou*
(ii) *o resto da divisão de n por 2 é 1, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q + 1$.*
(Fonte: Hefez (2013, p. 56))

Portanto, os números inteiros dividem-se em duas classes, a dos números da forma $2q$ para algum $q \in \mathbb{Z}$, chamados *números pares*, e a da forma $2q + 1$, chamados de *números ímpares* (HEFEZ, 2013, p. 56). Assim, os inteiros pares são:

$$0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \pm 14, \pm 16, \pm 18, \pm 20, \pm 22, ...$$

e os inteiros ímpares são

$$\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17, \pm 19, \pm 21, \pm 23, ...$$

Faz observar Alencar Filho (1987, p. 130) que

$$a^2 = (2q)^2 = 4k = 2(2k) \quad \text{ou} \quad a^2 = (2q+1)^2 = 4(q^2+q) + 1 = 4h + 1 = 2(2h) + 1$$

de modo que na divisão do quadrado a^2 de um inteiro qualquer a por 4 o resto é 0 ou 1. Ou ainda: o quadrado de um inteiro par é par e o quadrado de um inteiro ímpar é ímpar.

Faz saber Alencar Filho (1987, p. 130) que dois inteiros que são ambos pares ou ambos ímpares dizem-se de *mesma paridade*, e que dois inteiros tais que um é par e o outro é ímpar dizem-se *paridade diferente*. Assim, por exemplo, 3 e 7, e -4 e 6 são de mesma paridade, enquanto que 5 e 8 são de paridade diferente.

A soma e a diferença de dois inteiros de mesma paridade é um inteiro par, porque

$$2m \pm 2n = 2(m \pm n)$$

e

$$(2m+1) \pm (2n+1) = 2(m+n+1) \text{ ou } 2(m-n).$$

A soma e a diferença de dois inteiros de paridade diferente é um inteiro ímpar, porque

$$(2m+1) \pm 2n = 2(m \pm n) + 1.$$

Exemplo 2.6.13. *De modo mais geral, fixado um número natural $m \geq 2$, pode-se sempre escrever um número qualquer n, de modo único, na forma $n = mk + r$, onde $k, r \in \mathbb{Z}$ e $0 \leq r < m$.*

(Fonte: Hefez (2013, p. 56))

Por exemplo, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $3k$, $3k+1$, ou $3k+2$.

Outro exemplo: todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $4k$, $4k+1$, $4k+2$, ou $4k+3$.

Exemplo 2.6.14. *Mostre que o quadrado de qualquer inteiro ímpar é da forma $8k+1$.*

(Fonte: Alencar Filho (1987, p. 131))

Demonstração. Pelo exemplo anterior, o inteiro a pode ser escrito em uma, e somente uma, das seguintes formas:

$$4q,\ 4q+1,\ 4q+2, \text{ ou } 4q+3.$$

Nesta classificação, o inteiro a é ímpar se $a = 4q+1$ ou $4q+3$ e, nestes dois casos, temos:

$$\begin{aligned} a^2 &= (4q+1)^2 = 8(2q^2+q)+1 = 8k+1 \\ a^2 &= (4q+3)^2 = 8(2q^2+3q+1)+1 = 8k+1 \end{aligned}$$

□

Exemplo 2.6.15. *Mostre que, se a e b são inteiros ímpares, então $8|(a^2-b^2)$.*

(Fonte: Alencar Filho (1987, p. 132-133))

Demonstração. Pelo exemplo anterior:

$$a^2 = 8k + 1 \text{ e } b^2 = 8h + 1.$$

Portanto:

$$a^2 - b^2 = 8(k - h) \quad \text{e} \quad 8|(a^2 - b^2).$$

□

Exemplo 2.6.16. *Mostre que, se n é um inteiro ímpar não divisível por 3, então $(n^2 + 5)$ é divisível por 6.*

(Fonte: Alencar Filho (1987, p. 134))

Demonstração. Com efeito, se n não é divisível por 3, então, os possíveis restos na divisão de n por 3 são 1 e 2. Logo, pelo algoritmo da divisão:

$$n = 3q + 1 \text{ ou } n = 3q + 2 = 3(q + 1) - 1,$$

ou seja:

$$n = 3h \pm 1.$$

Por outro lado, se n é ímpar, então h é par, isto é, $h = 2k$, e temos:

$$n = 6k \pm 1.$$

Portanto:

$$n^2 + 5 = (6k \pm 1)^2 + 5 = 6(6k^2 \pm 2k + 1),$$

isto é, $(n^2 + 5)$ é divisível por 6. □

Exemplo 2.6.17. *Sendo a e b inteiros consecutivos cujo produto é c, mostre que o inteiro $n = a^2 + b^2 + c^2$ é o quadrado de um inteiro ímpar.*

(Fonte: Alencar Filho (1987, p. 136))

Demonstração. Temos $b = a + 1$ e $c = ab = a(a + 1)$, o que implica:

$$n = a^2 + (a + 1)^2 + a^2(a + 1)^2 = (a^2 + a + 1)^2$$

onde $a^2 + a + 1 = a(a + 1) + 1$ é um inteiro ímpar, visto que o produto $a(a + 1)$ é um inteiro par. □

Exemplo 2.6.18. *Mostre que, se um inteiro par é a soma de dois quadrados, então a metade desse inteiro também é a soma de dois quadrados.*

(Fonte: Alencar Filho (1987, p. 138))

Demonstração. Se o inteiro par $2n = a^2 + b^2$, então os inteiros a e b são de mesma paridade.

Por outro lado, temos:

$$n = \frac{a^2 + b^2}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$$

onde $\frac{a+b}{2}$ e $\frac{a-b}{2}$ são inteiros, porque a e b são de mesma paridade. Logo, n é a soma de dois quadrados. □

2.7 MDC de Dois Inteiros

Alencar Filho (1987, p. 184) apresenta a seguinte definição para máximo divisor comum de dois inteiros a e b: Sejam a e b dois inteiros não conjuntamente nulos. Chama-se máximo divisor comum de a e b o inteiro d $(d > 0)$ que satisfaz as condições:

(i) $d|a$ e $d|b$;

(ii) se $c|a$ e se $c|b$, então $c \leq d$.

Note que, pela condição (i), d é um divisor comum de a e b, e pela condição (ii) d é o maior dentre todos os divisores comuns de a e b.

O *máximo divisor comum* de a e b indica-se pela notação $mdc(a, b)$ (alguns autores usam a notação (a, b)).

A definição do $mdc(a, b)$ é simétrica em relação aos inteiros a e b, de modo que $mdc(a, b) = mdc(b, a)$. Em particular:

1. o $mdc(0, 0)$ não existe, porque todo inteiro divide 0 (alguns autores, a exemplo de Hefez (2013), consideram que $mdc(0, 0) = 0$);
2. o $mdc(a, 1) = mdc(a, -1) = 1$;
3. se $a \neq 0$, então o $mdc(a, 0) = |a| = mdc(a, a)$;
4. o $mdc(a, 0) = 1$ se, e somente se, $a = \pm 1$;
5. se $a|b$, então o $mdc(a, b) = |a|$.

Alencar Filho (1987, p. 185) também define combinação linear dos inteiros a e b: Sejam a e b dois inteiros. Chama-se **combinação linear** de a e b todo inteiro n da forma

$$n = ax + by,$$

onde x e y são inteiros quaisquer.

Assim, por exemplo, temos:

$$25 = 15.3 + 20.(-1)$$

e, portanto, o inteiro 25 é uma combinação linear dos inteiros 15 e 20.

Teorema 2.7.1. *Se a e b são dois inteiros não conjuntamente nulos, então existem inteiros x e y tais que o*

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

isto é, o $mdc(a, b)$ é uma combinação linear de a e b.

(Fonte: Alencar Filho (1987, p. 185-186))

Demonstração. Seja S o conjunto de todos os inteiros positivos da forma $au + bv$, onde u e v são inteiros, isto é, simbolicamente:

$$S = \{au + bv | au + bv > 0 \text{ e } u, v \in \mathbb{Z}\}.$$

Este conjunto S não é vazio, porque, por exemplo, se $a \neq 0$, então um dos dois inteiros:

$$a = a.1 + b.0 \quad \text{e} \quad -a = a.(-1) + b.0$$

é positivo e pertence a S. Logo, pelo *Princípio da Boa Ordenação*, existe e é único o elemento mínimo d de S: min$S = d > 0$. E, consoante a definição de S, existem inteiros x e y tais que $d = ax + by$.

Posto isto, vamos mostrar que $d = mdc(a, b)$.

Com efeito, pelo algoritmo da divisão aplicado aos inteiros a e d, temos:

$$a = dq + r \quad , \quad \text{com } 0 \leq r < d,$$

o que implica:

$$r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy),$$

isto é, o resto r é uma combinação linear de a e b. Portanto, se $r > 0$, então r pertence a S, o que é impossível , porque $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S. Assim sendo, $r = 0$ e $a = dq$, isto é, $d|a$.

Com raciocínio inteiramente análogo, também se conclui que $d|b$. Logo, d é um divisor comum de a e b.

Finalmente, se c é um divisor comum positivo qualquer de a e b, então:

$$c|(ax + by) \quad \text{ou} \quad c|d \quad \text{e} \quad c \leq d,$$

isto é, d é o maior divisor comum positivo de a e b, ou seja:

$$mdc(a,b) = d = ax + by \quad , \quad x, y \in \mathbb{Z},$$

e o teorema fica demonstrado. □

2.7.1 Existência e Unicidade do MDC

Faz saber Alencar Filho (1987, p. 187) que, consoante a demonstração do **teorema 2.7.1**:

1. o $mdc(a,b) = d$, e como d é o elemento mínimo do conjunto S, segue-se que existe e é único o $mdc(a,b)$;
2. o $mdc(a,b)$ é o menor inteiro positivo da forma $ax + by$, isto é, que pode ser expresso como combinação linear de a e b.

Importa notar que a representação do $mdc(a,b)$ como combinação linear de a e b não é única, pois, temos:

$$mdc(a,b) = d = a(x + bt) + b(y - at)$$

qualquer que seja o inteiro t.

Teorema 2.7.2. *Se a e b são dois inteiros não conjuntamente nulos, então o conjunto de todos os múltiplos do $mdc(a,b) = d$ é:*

$$T = \{ax + by |\, x, y \in \mathbb{Z}\}.$$

(Fonte: Alencar Filho (1987, p. 188))

Demonstração. Como $d|a$ e $d|b$, segue-se que $d|(ax + by)$, quaisquer que sejam os inteiros x e y, e, por conseguinte, todo elemento do conjunto T é múltiplo do $mdc(a,b) = d$. Por outro lado, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$, de modo que todo múltiplo kd de d é da forma:

$$kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0)$$

□

isto é, kd é uma combinação linear de a e b e, portanto, kd é elemento do conjunto T.

Teorema 2.7.3. *Sejam a e b dois inteiros não conjuntamente nulos. Um inteiro $d(d > 0)$ é o $mdc(a,b)$ se, e somente se, satisfaz às condições:*

1. $d|a$ e $d|b$;

2. se $c|a$ *e se* $c|b$*, então* $c|d$*.*

(Fonte: Alencar Filho (1987, p. 188-189))

Demonstração. Suponhamos que o $mdc(a,b) = d$. Então, $d|a$ e $d|b$; isto é, a condição 1 é satisfeita. Por outro lado, existem inteiros x e y tais que $ax + by = d$ (**Teorema 2.7.1**) e, portanto, se $c|a$ e se $c|b$, então $c|(ax + by)$ e $c|d$, isto é, a condição 2 também é satisfeita.

Reciprocamente, seja d um inteiro positivo qualquer que satisfaz às condições 1 e 2. Então, pela condição 2, todo divisor comum c de a e b também é divisor de d, isto é, $c|d$, o que implica $c \leq d$. Logo, pela definição de mdc, d é o $mdc(a,b)$. □

Teorema 2.7.4. *Se* a *e* b *são dois inteiros não conjuntamente nulos, então*

$$mdc(a,b) = mdc(a + kb, b),$$

para todo inteiro k*.*

(Fonte: Alencar Filho (1987, p. 189))

Demonstração. Sejam d o $mdc(a,b)$ e d_1 o $mdc(a + kb, b)$. Então, $d|a$ e $d|b$. Portanto:

$$d|(a + kb) \quad \text{e} \quad d|b.$$

Logo, pelo **Teorema 2.7.3**: $d|d_1$.
Analogamente, $d_1|(a + kb)$ e $d_1|b$. Portanto:

$$d_1|(a + kb - kb), \text{ isto é, } d_1|a \text{ e } d_1|b.$$

Logo, pelo mesmo **Teorema 2.7.3**: $d_1|d$.
Assim, $d|d_1$ e $d_1|d$, o que implica $d = d_1$. □

2.7.2 Inteiros Primos Entre Si

Faz saber Alencar Filho (1987, p. 196) que, dados os inteiros a e b não conjuntamente nulos, diz-se que a e b são *primos entre si* se, e somente se, o $mdc(a,b) = 1$.

Se a e b são primos entre si, também se diz que a é primo com b, ou ainda, que são primos relativos (ou relativamente primos).

Segundo Hefez (2013, p. 96): Dois números inteiros a e b serão ditos *primos entre si* , ou *coprimos*, se $mdc(a,b) = 1$; ou seja, se o único divisor comum positivo de ambos é 1.

Teorema 2.7.5. *Dois inteiros* a *e* b*, não conjuntamente nulos, são primos entre si, ou coprimos se, e somente se, existem inteiros* x *e* y *tais que* $ax + by = 1$*.*

(Fonte: Alencar Filho (1987, p. 196))

Demonstração. Se a e b são primos entre si, então o $mdc(a,b)=1$, e por conseguinte existem inteiros x e y tais que $ax+by=1$ (**Teorema 2.7.1**).

Reciprocamente, se existem inteiros x e y tais que $ax+by=1$ e se o $mdc(a,b)=d$, então $d|a$ e $d|b$. Logo, $d|(ax+by)$ e $d|1$, o que implica $d=1$ ou $mdc(a,b)=1$; isto é, a e b são primos entre si. □

Corolário 2.7.1. *Se o* $mdc(a,b)=d$*, então o* $mdc\left(\frac{a}{d},\frac{b}{d}\right)=1.$

(Fonte: Alencar Filho (1987, p. 196-197))

Demonstração. Preliminarmente, note-se que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros porque d é um divisor comum de a e b.

Se o $mdc(a,b)=d$, então existem inteiros x e y tais que $ax+by=d$; ou seja, dividindo ambos os membros desta igualdade por d:

$$\frac{a}{d}x+\frac{b}{d}y=1.$$

Logo, pelo **Teorema 2.7.5**, os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, isto é, $mdc\left(\frac{a}{d},\frac{b}{d}\right)=1.$ □

Teorema 2.7.6 (Lema de Gauss)**.** *Se* $a|bc$ *e se o* $mdc(a,b)=1$*, então* $a|c.$

(Fonte: Alencar Filho (1987, p. 197))

Demonstração.

(i) se $a|bc$, então $bc=aq$, com $q\in\mathbb{Z}$;

(ii) se o $mdc(a,b)=1$, então:

$$ax+by=1 \quad \text{e} \quad acx+bcy=c, \qquad \text{com } x,y\in\mathbb{Z}.$$

Portanto:

$$c=acx+aqy=a(cx+qy) \quad \text{e} \quad a|c.$$

□

Teorema 2.7.7. *Se* $a|c$ *e se* $b|c$*, com* $mdc(a,b)=1$*, então* $ab|c.$

(Fonte: Alencar Filho (1987, p. 198))

Demonstração.

Com efeito:

(i) se $a|c$, então $c=aq_1$, com $q_1\in\mathbb{Z}$;

(ii) se $b|c$, então $c=bq_2$, com $q_2\in\mathbb{Z}$;

(iii) se o $mdc(a,b)=1$, então:

$$ax + by = 1 \quad \text{e} \quad acx + bcy = c \quad , \quad \text{com } x, y \in \mathbb{Z}.$$

Portanto:

$$c = a(bq_2)x + b(aq_1)y = ab(q_2x + q_1y) \quad \text{e} \quad ab|c.$$

□

Corolário 2.7.2. *O produto de três inteiros consecutivos é divisível por* 6.
(Fonte: Alencar Filho (1987, p. 198))

Demonstração. Em três inteiros consecutivos $n, n+1$ e $n+2$, um pelo menos é par, e um sempre é divisível por 3. Logo, o produto $n(n+1)(n+2)$ é divisível por 2 e por 3, inteiros primos entre si, e, por conseguinte, é divisível por $2.3 = 6$ (**Teorema 2.7.7**). □

Teorema 2.7.8. *Se* $a|b$ *e se o* $mdc(b, c) = 1$*, então, o* $mdc(a, c) = 1$.
(Fonte: Alencar Filho (1987, p. 198-199))

Demonstração.
Com efeito:
(i) se $a|b$, então $b = aq$, com $q \in \mathbb{Z}$;
(ii) se o $mdc(b, c) = 1$, então $bx + cy = 1$, com $x, y \in \mathbb{Z}$.
Portanto:

$$a(qx) + cy = 1 \quad \text{e o } mdc(a, c) = 1.$$

□

Teorema 2.7.9. *Se o* $mdc(a, b) = 1 = mdc(a, c)$*, então, o* $mdc(a, bc) = 1$.
(Fonte: Alencar Filho (1987, p. 199))

Demonstração.
Com efeito:
(i) se o $mdc(a, b) = 1$, então $ax + by = 1$, com $x, y \in \mathbb{Z}$;
(ii) se o $mdc(a, c) = 1$, então $az + ct = 1$, com $z, t \in \mathbb{Z}$.
Portanto:

$$1 = ax + by(az + ct) = a(x + byz) + bc(yt),$$

o que implica $mdc(a, bc) = 1$.

□

Teorema 2.7.10. *Se o* $mdc(a, bc) = 1$*, então: o* $mdc(a, b) = 1 = mdc(a, c)$*.*

(Fonte: Alencar Filho (1987, p. 199))

Demonstração. Com efeito, se o $mdc(a, bc) = 1$, então:

$$ax + (bc)y = 1, \text{ com } x, y \in \mathbb{Z}.$$

Portanto:

$$\begin{array}{lll} ax + b(cy) = 1 & \text{e o} & mdc(a, b) = 1, \\ ax + c(by) = 1 & \text{e o} & mdc(a, c) = 1. \end{array}$$

□

Note-se que este teorema é o recíproco do teorema anterior.

Lema 2.7.1. *Se* $a = bq + r$*, então o* $mdc(a, b) = mdc(b, r)$*.*

(Fonte: Alencar Filho (1987, p. 218))

Demonstração. Com efeito, se o $mdc(a, b) = d$, então $d|a$ e $d|b$, o que implica:

$$d|(a - bq) \quad \text{ou} \quad d|r,$$

isto é, d é um divisor comum de b e r ($d|b$ e $d|r$).

Por outro lado, se c é um divisor comum qualquer de b e r ($c|b$ e $c|r$), então:

$$c|(bq + r) \quad \text{ou} \quad c|a,$$

isto é, c é um divisor comum de a e b, o que implica $c \leq d$. Portanto, o $mdc(b, r) = d$. □

2.8 Algoritmo de Euclides

Hefez (2013, p. 89-91) apresenta a prova construtiva da existência do mdc dada por Euclides, chamado de *Algoritmo de Euclides*.

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b|a$, já vimos que $mdc(a, b) = a$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever

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

Temos duas possibilidades:

$a)$ $r_1|b$. Em tal caso, $r_1 = mdc(b, r_1)$ e, pelo **Lema 2.7.1**, temos que

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 b) = mdc(b, a) = mdc(a, b),$$

e o algoritmo termina.

$b)$ $r_1 \nmid b$. Em tal caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \quad \text{com } 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:

$a')$ $r_2|r_1$. Nesse caso, $r_1 = mdc(r_1, r_2)$ e novamente, pelo **Lema 2.7.1**, temos que

$$r_2 = mdc(r_1, r_2) = mdc(r_1, b - q_2 r_1) = mdc(r_1, b) = mdc(a - q_1 b, b) = mdc(a, b),$$

e o algoritmo termina.

$b')$ $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \quad \text{com } 0 < r_3 < r_2.$$

Continuamos esse procedimento até que pare. Isto sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > ...$ que não possui menor elemento, o que não é possível pelo *Princípio da Boa Ordenação*. Logo, para algum n temos que $r_n|r_{n-1}$, o que implica que $mdc(a, b) = r_n$.

O algoritmo acima pode ser sintetizado e realizado na prática como mostramos a seguir.

Inicialmente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos

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

Exemplo 2.8.1. *Calcule o* $mdc(372, 162)$.

(Fonte: Hefez (2013, p. 91))

Resolução.

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

Observe que no exemplo anterior o Algoritmo de Euclides fornece-nos:

$$\begin{aligned} 6 &= 18 - 1.12 \\ 12 &= 48 - 2.18 \\ 18 &= 162 - 3.48 \\ 48 &= 372 - 2.162 \end{aligned}$$

Donde segue que:

$$\begin{aligned} 6 &= 18 - 1.12 \\ &= 18 - 1.(48 - 2.18) \\ &= 3.18 - 48 \\ &= 3.(162 - 3.48) - 48 \\ &= 3.162 - 10.48 \\ &= 3.162 - 10.(372 - 2.162) \\ &= 23.162 - 10.372 \end{aligned}$$

Temos, então, que:

$$mdc(372, 162) = 6 = 23.162 + (-10).372.$$

Note que conseguimos, através do uso do Algoritmo de Euclides de trás para frente, escrever $6 = mdc(372, 162)$ como múltiplo de 162 mais um múltiplo de 372.

Teorema 2.8.1. *o* $mdc(ka, kb) = k.mdc(a, b)$*, onde* k *é um inteiro positivo.*

(Fonte: Alencar Filho (1987, p. 223-224))

Demonstração. Multiplicando ambos os membros de cada uma das $n + 1$ igualdades que dão o $mdc(a, b) = r_n$ pelo algoritmo de Euclides pelo inteiro positivo k, obtemos:

$$\begin{array}{rcccc} ak & = & (bk)q_1 + r_1k & , & 0 < r_1k < bk \\ bk & = & (r_1k)q_2 + r_2k & , & 0 < r_2k < r_1k \\ r_1k & = & (r_2k)q_3 + r_3k & , & 0 < r_3k < r_2k \\ & \vdots & & & \vdots \\ r_{n-2}k & = & (r_{n-1}k)q_n + r_nk & , & 0 < r_nk < r_{n-1}k \\ r_{n-1}k & = & (r_nk)q_{n+1} + 0 & & \end{array}$$

Observe que estas $n+1$ igualdades outra coisa não são se não o Algoritmo de Euclides aplicado aos inteiros ak e bk, e, por conseguinte, o último resto $r_nk \neq 0$ é o $mdc(ak, bk)$, isto é:

$$mdc(ka, kb) = r_nk = k.mdc(a, b)$$

□

Corolário 2.8.1. *Para todo inteiro $k \neq 0$, tem-se:*

$$mdc(ka, kb) = |k| .mdc(a, b)$$

(Fonte: Alencar Filho (1987, p. 224))

Demonstração. Se $k > 0$, nada há que demonstrar, e se $k < 0$, então $-k = |k| > 0$, e pelo **Teorema 2.8.1**, temos:

$$\begin{array}{rcl} mdc(ak, bk) & = & mdc(-ak, -bk) \\ & = & mdc(a. |k| , b. |k|) \\ & = & |k| .mdc(a, b) \end{array}$$

□

Hefez (2013, p. 97) faz saber que a noção de mdc pode ser generalizada como a seguir.

Um número natural d será dito mdc de dados números inteiros $a_1, ..., a_n$, não todos nulos, se possuir as seguintes propriedades:

(i) d é um divisor comum de $a_1, ..., a_n$;

(ii) Se c é um divisor comum de $a_1, ..., a_n$, então $c|d$.

A proposição a seguir fornecer-nos-á um método indutivo para o cálculo do mdc de n inteiros, reduzindo-o à aplicação do Algoritmo de Euclides a $n-1$ pares de inteiros.

Proposição 2.8.1. *Dados números inteiros $a_1, ..., a_n$, não todos nulos, existe o seu mdc e*

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

Demonstração. Vamos provar a proposição por indução sobre n (≥ 2). Para $n = 2$ nada temos a provar. Suponha que o resultado vale para n. Para provar que o resultado é válido para $n + 1$, basta provar que se d é o mdc de $a_1, ..., mdc(a_n, a_{n+1})$, então d é o mdc de $a_1, ..., a_n, a_{n+1}$, pois isso provará também a existência.

Seja d o mdc de $a_1, ..., mdc(a_n, a_{n+1})$. Logo, $d|a_1, ..., d|a_{n-1}$ e $d|mdc(a_n, a_{n+1})$. Portanto, $d|a_1, ..., d|a_{n-1}, d|a_n$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, ..., a_n, a_{n+1}$; logo, c é um divisor comum de $a_1, ..., a_{n-1}$ e $mdc(a_n, a_{n+1})$; e, portanto, $c|d$. □

(Fonte: Hefez (2013, p. 97-98))

Os inteiros $a_1, ..., a_n$ serão ditos *primos entre si*, ou *coprimos*, quando $mdc(a_1, ..., a_n) = 1$ (HEFEZ, 2013, p. 89).

Exemplo 2.8.2. *Demonstre:* $mdc(a + b, a - b) \geq mdc(a, b)$.

(Fonte: Alencar Filho (1987, p. 191))

Demonstração. Com efeito, se o $mdc(a, b) = d$, então $d|a$ e $d|b$, o que implica:

$$d|(a + b) \quad \text{e} \quad d|(a - b).$$

Portanto:

$$d|mdc(a + b, a - b)$$

e

$$mdc(a + b, a - b) \geq d = mdc(a, b).$$

□

Exemplo 2.8.3. *Calcule o* $mdc(35 + n, 45n + 76)$*, onde* n *é um inteiro qualquer.*

(Fonte: Alencar Filho (1987, p. 191))

Resolução.
Seja d o mdc procurado. Então:

$$d|(35n + 57) \quad \text{e} \quad d|(45n + 76).$$

Portanto:

$$d|\,[7(45n + 76) - 9(35n + 57)] \quad \text{e} \quad d|19,$$

de modo que $d = 1$ ou $d = 19$.

Exemplo 2.8.4. *Demonstre que o* $mdc(2^m - 1, 2^n + 1) = 1$*, onde* m *e* n *são inteiros positivos, sendo* m *ímpar.*

(Fonte: Alencar Filho (1987, p. 191-192))

Demonstração. Seja $d = mdc(2^m - 1, 2^n + 1)$, de modo que

$$2^m - 1 = hd \quad \text{e} \quad 2^n + 1 = kd, \quad \text{com} \quad h, k \in \mathbb{N},$$

o que implica:

$$2^m = hd + 1 \quad \text{e} \quad 2^{mn} = (hd + 1)^n = rd + 1, \quad \text{com} \quad r \in \mathbb{N},$$

$$2^n = kd - 1 \quad \text{e} \quad 2^{mn} = (kd - 1)^m = ad - 1, \quad \text{com} \quad a \in \mathbb{N}.$$

Portanto:

$$rd + 1 = ad - 1 \quad \text{e} \quad (a - r)d = 2,$$

o que implica: $d|2$, de modo que $d = 1$ ou $d = 2$. E como $2^m - 1$ é ímpar, segue-se que d é ímpar, isto é, $d = 1$. □

Exemplo 2.8.5. *Mostre que, se o* $mdc(a, 3) = 1$*, então o inteiro* $a^2 + 2$ *é divisível por* 3*.*

(Fonte: Alencar Filho (1987, p. 192))

Demonstração. Com efeito, se o $mdc(a, 3) = 1$, então $a = 3k \pm 1$, o que implica:

$$a^2 + 2 = (3k \pm 1)^2 + 2 = 3(3k^2 \pm 2k + 1)$$

e portanto: $3|(a^2 + 1)$. □

Exemplo 2.8.6. *Mostre que dois inteiros ímpares consecutivos quaisquer são primos entre si.*

(Fonte: Alencar Filho (1987, p. 204))

Demonstração. Com efeito, se o $mdc(2n + 1, 2n + 3) = d$, então $d|(2n + 1)$ e $d|(2n + 3)$. Portanto,

$$d|\,[(2n + 3) - (2n + 1)] \quad \text{e} \quad d|2,$$

o que implica $d = 1$ ou $d = 2$. Mas, não pode ser 2, porque os dois inteiros são ímpares, de modo que $d = 1$, isto é, $2n + 1$ e $2n + 3$ são primos entre si. □

Exemplo 2.8.7. *Sendo* n *um inteiro qualquer, mostre que:*

$$6|(n^3 + 5n) \quad \textit{e} \quad 6|(n^3 + 11n).$$

(Fonte: Alencar Filho (1987, p. 204-205))

Demonstração. Com efeito:

$$n^3 + 5n = n^3 + 6n - n = n(n^2 - 1) + 6n = (n-1)n(n+1) + 6n$$

e

$$n^3 + 11n = n^3 + 12n - n = n(n^2 - 1) + 12n = (n-1)n(n+1) + 12n.$$

Como o produto de três inteiros consecutivos é divisível por 6 (**corolário 2.7.2**), temos $(n-1)n(n+1) = 6q$, com $q \in \mathbb{Z}$, o que implica:

$$\begin{aligned} n^3 + 5n = 6q + 6n = 6(q+n) \quad &\text{e} \quad 6|(n^3 + 6n), \\ n^3 + 11n = 6q + 12n = 6(q+2n) \quad &\text{e} \quad 6|(n^3 + 11n). \end{aligned}$$

□

Exemplo 2.8.8. *Os inteiros a e b são primos entre si. Demonstre:*

$$mdc(a+b, a-b) = 1 \text{ ou } 2.$$

(Fonte: Alencar Filho (1987, p. 207))

Demonstração. Seja $d = (a+b, a-b)$. Portanto, $d|(a+b)$ e $d|(a-b)$, o que implica, pelo item vi da **Proposição 2.6.3**, que $d|2a$ e $d|2b$, de modo que

$$d|mdc(2a, 2b)$$

e

$$d \leq mdc(2a, 2b) = 2.mdc(a, b) = 2,$$

isto é, $d = 1$ ou $d = 2$. □

Exemplo 2.8.9. *Sendo n um inteiro par, mostre que $48|(n^3 + 20n)$.*

(Fonte: Alencar Filho (1987, p. 205))

Demonstração. Sendo n par, $n = 2k$, com $k \in \mathbb{Z}$, e temos:

$$n^3 + 20n = 8k(k^2 + 5) = 8k(k^2 - 1) + 48k = 8k(k-1)(k+1) + 48k.$$

Mas, o produto $k(k-1)(k+1)$ é divisível por 6, ou seja, é da forma $6q$, com $q \in \mathbb{Z}$, o que nos dá:

$$n^3 + 20n = 8.6q + 48k = 48(q+k),$$

isto é, $48|(n^3 + 20n)$. □

2.9 Mínimo Múltiplo Comum

Diremos que um número inteiro é um *múltiplo comum* de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números (HEFEZ, 2013, p. 105).

Hefez (2013, p. 105) afirma que um inteiro $m \geq 0$ é um *mínimo múltiplo comum* (mmc) dos números inteiros a e b se possuir as seguintes propriedades:

(i) m é um múltiplo comum de a e b, e

(ii) se c é um múltiplo comum de a e b, então $m|c$.

Se m e m' são dois mínimos múltiplos comuns de a e b, então, do item (ii) da definição acima, temos que $m|m'$ e $m'|m$. Como m e m' são números inteiros não negativos, temos que $m = m'$, o que mostra que o mínimo múltiplo comum, se existe, é único.

Por outro lado, se m é o mmc de a e b, e c é um múltiplo comum de a e b, então $m|c$. Portanto, se c é positivo, temos que $m \leq c$, mostrando que m é o menor dos múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b, se existe, é denotado por $mmc(a, b)$ (alguns autores adotam a notação $[a, b]$).

Caso exista, pode-se demonstrar que

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

Assim, para efeito do cálculo do mmc de dois números, podemos sempre supô-los não negativos.

Também podemos verificar que $mmc(a, b) = 0$ se, e somente, $a = 0$ ou $b = 0$. De fato, se $mmc(a, b) = 0$, então 0 divide ab, que é múltiplo de a e de b; logo, $ab = 0$ e, portanto, $a = 0$ ou $b = 0$. Reciprocamente, se $a = 0$ ou $b = 0$, então 0 é o único múltiplo comum de a e b; logo, $mmc(a, b) = 0$.

Proposição 2.9.1. *Dados dois números inteiros a e b, temos que $mmc(a, b)$ existe e*

$$mmc(a, b)mdc(a, b) = |ab| .$$

(Fonte: Hefez (2013, p. 106))

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade acima é trivialmente satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$. Ponhamos $m = \dfrac{ab}{mdc(a, b)}$. Como

$$m = a\frac{b}{mdc(a, b)} = b\frac{a}{mdc(a, b)},$$

temos que $a|m$ e $b|m$. Portanto, m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b; logo, $c = na = n'b$. Segue daí que

$$n\frac{a}{mdc(a,b)} = n'\frac{b}{mdc(a,b)}.$$

Como, pelo **Corolário 2.7.1**, $\frac{a}{mdc(a,b)}$ e $\frac{b}{mdc(a,b)}$ são primos entre si, segue-se, do Lema de Gauss (**Teorema 2.7.6**), que $\frac{a}{mdc(a,b)}$ divide n', e, portanto, $m = \frac{a}{mdc(a,b)}b$ divide $n'b$, que é igual a c. □

Corolário 2.9.1. *Se a e b são inteiros primos entre si, então* $mmc(a,b) = |ab|$.

(Fonte: Hefez (2013, p. 106))

Demonstração. Como a e b são primos entre si, então $mdc(a,b) = 1$ e, pela **Proposição 2.9.1**, segue que

$$mmc(a,b) = |ab|.$$

□

Diremos que um número natural m é um mmc dos inteiros não nulos $a_1, ..., a_n$, se m é um múltiplo comum de $a_1, ..., a_n$, e, se para todo múltiplo comum m' desses números, tem-se que $m|m'$.

Pode-se verificar que o mmc, se existe, é único, sendo denotado por $mmc(a_1, ..., a_n)$ (alguns autores adotam a notação $[a_1, ..., a_n]$). Além disso, o mmc de vários inteiros não nulos é o menor múltiplo comum positivo desses inteiros (HEFEZ, 2013, p. 107).

Proposição 2.9.2. *Sejam $a_1, ..., a_n$ números inteiros não nulos. Então existe o número $mmc(a_1, ..., a_n)$ e*

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

(Fonte: Hefez (2013, p. 107))

Demonstração. Basta provar que, se existe $mmc(a_1, ..., mmc(a_{n-1}, a_n))$, vale a igualdade acima.

A existência do mmc segue facilmente disso, por indução.

Seja $m = mmc(a_1, ..., mmc(a_{n-1}, a_n))$. logo, $a_1, ..., a_{n-2}$ e $mmc(a_{n-1}, a_n)$ dividem m.

Como $a_{n-1}|mmc(a_{n-1}, a_n)$ e $a_n|mmc(a_{n-1}, a_n)$, segue que m é um múltiplo comum de $a_1, ..., a_n$.

Por outro lado, suponha que m' seja um múltiplo comum de $a_1, ..., a_n$.

Logo, $a_1|m', ..., a_{n-2}|m'$ e $mmc(a_{n-1}, a_n)|m'$; daí segue que m' é múltiplo de $m = mmc(a_1, ..., mmc(a_{n-1}, a_n))$. □

2.10 Teorema Fundamental da Aritmética

Um número natural maior que 1 que só possui como divisores positivos 1 e ele próprio é chamado *número primo* (HEFEZ, 2013, p. 140).

Segundo Hefez (2013, p. 140), dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

(i) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

(ii) Se $p \nmid a$, então $mdc(p, a) = 1$

De fato, se $mdc(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$, e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será dito *composto*.

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n, tal que $1 < n_1 < n$. Logo, existirá um divisor natural n_2, tal que

$$n = n_1 n_2, \quad \text{com} \quad 1 < n_1 < n \quad \text{e} \quad 1 < n_2 < n.$$

Proposição 2.10.1 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

(Fonte: Hefez (2013, p. 141))

Demonstração. Basta provar que, se $p|ab$ e $p \nmid a$, então $p|b$. Mas, se $p \nmid a$, temos que $mdc(p, a) = 1$, e o resultado segue-se do Lema de Gauss (**Teorema 2.7.6**). □

Teorema 2.10.1. *Se p é um primo tal que $p|a_1a_2...a_n$, então $p|a_k$, sendo k um dos inteiros $1, 2, ..., n$.*

(Fonte: Alencar Filho (1987, p. 283))

Demonstração. A proposição é verdadeira para $n = 1$ (imediato) e para $n = 2$ (pelo Lema de Euclides). Suponhamos, pois, $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (hipótese de indução).

Pelo Lema de Euclides, se $p|a_1a_2...a_n$, então:

$$p|a_n \quad \text{ou} \quad p|a_1a_2...a_{n-1}$$

Se $p|a_n$, a proposição está demonstrada, e se $p|a_1a_2...a_{n-1}$, então, a hipótese de indução assegura que $p|a_k$, com $1 \leq k \leq n - 1$. Em qualquer dos dois casos, p divide um dos inteiros $a_1a_2...a_n$ □

Corolário 2.10.1. *Se p é um primo tal que $p|a^n$, então $p|a$.*

(Fonte: Alencar Filho (1987, p. 283))

Demonstração. Como $a^n = a.a...a$ (n fatores), se $p|a^n$, então $p|a.a...a$. Logo, pelo **Teorema 2.10.1**, $p|a$. □

Corolário 2.10.2. *Se $p, q_1, q_2, ..., q_n$ são todos primos e se p divide o produto $q_1.q_2...q_n$, então $p = q_k$, sendo k um dos inteiros $1, 2, ..., n$.*

(Fonte: Alencar Filho (1987, p. 283-284))

Demonstração. Pelo **Teorema 2.10.1**, $p|q_k$, sendo k um dos inteiros $1, 2, ..., n$, e como os únicos divisores positivos de q_k são 1 e q_k, porque q_k é primo, segue-se que $p = 1$ ou $p = q_k$. Mas, $p > 1$, porque p é primo. Logo, $p = q_k$. □

Teorema 2.10.2 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

(Fonte: Hefez (2013, p. 141-142))

Demonstração. Usaremos a segunda forma do Princípio da Indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, .., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1...p_r$ e $n_2 = q_1, ..., q_s$. Portanto, $n = p_1...p_r q_1, ..., q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1...p_r = q_1, ..., q_s$, onde os p_i e os q_i são números primos. Como $p_1|q_1...q_s$, pelo **Corolário 2.10.2**, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto,

$$p_2...p_r = q_2...q_s$$

Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares. □

2.11 Congruências

2.11.1 Inteiros Congruentes

Alencar Filho (1986, p. 9) apresenta a seguinte definição de dois inteiros congruentes módulo m: Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. *Diz-se que a é congruente a b módulo m* se, e somente se, m divide a diferença $a - b$.

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

Com a notação de Gauss:

$$a \equiv b\,(mod\,m)$$

indica-se que a *é congruente a* b *módulo* m. Portanto, simbolicamente:

$$a \equiv b\,(mod\,m) \Longleftrightarrow m|(a-b),$$

ou seja:

$$a \equiv b\,(mod\,m) \Longleftrightarrow \exists k \in \mathbb{Z}|a - b = km.$$

Se m não divide a diferença $a - b$, então, diz-se que a *é incongruente a* b *módulo* m, o que se indica pela notação:

$$a \not\equiv b\,(mod\,m).$$

Note-se que dois inteiros quaisquer são congruentes módulo 1, enquanto que dois inteiros são congruentes módulo 2 somente se ambos são pares ou se ambos são ímpares.

Em particular, $a \equiv 0\,(mod\,m)$ se, e somente se, o módulo m divide a $(m|a)$; isto é: $a = mk$, com $k \in \mathbb{Z}$.

Teorema 2.11.1. *Dois inteiros* a *e* b *são congruentes módulo* m *se, e somente se,* a *e* b *deixam o mesmo resto quando divididos por* m*.*

(Fonte: Alencar Filho (1986, p. 10-11))

Demonstração. Suponhamos que $a \equiv b\,(mod\,m)$. Então, pela definição de congruência, temos:

$$a - b = km, \quad k \in \mathbb{Z}.$$

Seja r o resto da divisão de b por m; então, pelo algoritmo da divisão:

$$b = mq + r, \quad 0 \leq r < m.$$

Portanto:

$$a = km + b = km + mq + r = (k + q)m + r,$$

e isto significa que r também é o resto da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo resto r.

Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever:

$$a = mq_1 + r \quad \text{e} \quad b = mq_2 + r \ , \quad 0 \leq r < m.$$

Portanto:

$$a - b = (q_1 - q_2)m,$$

o que implica:

$$m|(a-b) \quad \text{e} \quad a \equiv b\,(mod\,m)\,.$$

□

Teorema 2.11.2. *Seja m um inteiro positivo fixo e sejam a, b e c inteiros quaisquer.*

1. $a \equiv a\,(mod\,m)$*;*
2. *Se* $a \equiv b\,(mod\,m)$*, então* $b \equiv a\,(mod\,m)$*;*
3. *Se* $a \equiv b\,(mod\,m)$ *e se* $b \equiv c\,(mod\,m)$*, então* $a \equiv c\,(mod\,m)$.

(Fonte: Alencar Filho (1986, p. 11-12))

Demonstração.

1. $a|0$ ou $a|(a-a)$, o que implica: $a \equiv a\,(mod\,m)$.
2. Se $a \equiv b\,(mod\,m)$, então $a - b = km$, $k \in \mathbb{Z}$. Portanto:

$$b - a = (-k)m \quad \text{e} \quad b \equiv a\,(mod\,m).$$

3. Se $a \equiv b\,(mod\,m)$ e se $b \equiv c\,(mod\,m)$, então existem inteiros h e k tais que

$$a - b = hm \quad \text{e} \quad b - c = km.$$

Portanto:

$$a - c = (a-b) + (b-c) = hm + km = (h+k)m.$$

e isto significa que $a \equiv c\,(mod\,m)$ □

Faz saber Alencar Filho (1986, p. 12) que, consoante este **Teorema 2.11.2**, a congruência, módulo um inteiro fixado m é uma relação de equivalência em $\mathbb{Z}$, pois é reflexiva, simétrica e transitiva.

2.11.2 Propriedades das Congruências

Teorema 2.11.3. *Se* $a \equiv b\,(mod\,m)$ *e se* $c \equiv d\,(mod\,m)$*, então:*

$$a + c \equiv b + d\,(mod\,m);$$
$$a - c \equiv b - d\,(mod\,m);$$
$$ac \equiv bd\,(mod\,m).$$

(Fonte: Alencar Filho (1986, p. 21))

Demonstração. Se $a \equiv b\,(mod\,m)$ e se $c \equiv d\,(mod\,m)$, então existem inteiros h e k tais que

$$a - b = hm \quad \text{e} \quad c - d = km.$$

Portanto:

$$(a + c) - (b + d) = (a - b) + (c - d) = (h + k)m;$$
$$(a - c) - (b - d) = (a - b) - (c - d) = (h - k)m;$$
$$ac - bd = (b + hm)(d + km) - bd = (bk + dh + hkm)m.$$

o que implica:

$$a + c \equiv b + d\,(mod\,m);$$
$$a - c \equiv b - d\,(mod\,m);$$
$$ac \equiv bd\,(mod\,m).$$

□

Corolário 2.11.1. *Se* $a \equiv b\,(mod\,m)$ *e se* c *é um inteiro qualquer, então:*

$$a \pm c \equiv b \pm c\,(mod\,m) \quad \textit{e} \quad ac \equiv bc\,(mod\,m).$$

(Fonte: Alencar Filho (1986, p. 22))

Demonstração. Temos:

$$a \equiv b\,(mod\,m) \quad \text{e} \quad c \equiv c\,(mod\,m).$$

Logo, pelo **Teorema 2.11.3**:

$$a \pm c \equiv b \pm c\,(mod\,m) \quad \text{e} \quad ac \equiv bc\,(mod\,m).$$

□

Em particular, se $c = -1$ e $a \equiv b\,(mod\,m)$, então:

$$a(-1) \equiv b(-1)\,(mod\, m) \quad \text{ou} \quad -a \equiv -b\,(mod\, m).$$

Corolário 2.11.2. *Se* $a + b \equiv c + d\,(mod\, m)$*, então:*

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

(Fonte: Alencar Filho (1986, p. 23))

Demonstração. Com efeito, somando ordenadamente as congruências:

$$\begin{aligned} a + b &\equiv c + d\,(mod\, m) \\ -b &\equiv -b\,(mod\, m) \\ -d &\equiv -d\,(mod\, m) \end{aligned}$$

obtemos:

$$a + b + (-b) + (-d) \equiv c + d + (-b) + (-d)\,(mod\, m),$$

ou, simplificando:

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

□

Portanto, numa congruência, pode-se “passar" um termo de um membro para o outro trocando-lhe o sinal.

Faz saber Alencar Filho (1986, p. 23) que não é permitido dividir ordenadamente duas congruências com o mesmo módulo. Assim, por exemplo:

$$48 \equiv 18\,(mod\, 10) \quad \text{e} \quad 12 \equiv 2\,(mod\, 10),$$

mas é falso:

$$4 \equiv 9\,(mod\, 10).$$

Teorema 2.11.4. *Se* $a \equiv b\,(mod\, m)$*, então* $a^n \equiv b^n\,(mod\, m)$ *para todo inteiro positivo* n*.*

(Fonte: Alencar Filho (1986, p. 23-24))

Demonstração. Usando o *Teorema da Indução Matemática*, a proposição é verdadeira para $n = 1$, e suposta verdadeira para o inteiro positivo k, temos:

$$a^k \equiv b^k\,(mod\, m) \quad \text{e} \quad a \equiv b\,(mod\, m).$$

Portanto, pelo **Teorema 2.11.3**:

$$a^k.a \equiv b^k.b\,(mod\, m) \quad \text{ou} \quad a^{k+1} \equiv b^{k+1}\,(mod\, m),$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, a proposição é verdadeira para todo inteiro positivo n. □

2.11.3 Mudança de Módulo numa Congruência

Teorema 2.11.5. *Se $a \equiv b\,(mod\,m)$ e se $n|m$, sendo n um inteiro positivo, então $a \equiv b\,(mod\,n)$.*

(Fonte: Alencar Filho (1986, p. 24))

Demonstração. Com efeito:

$$a \equiv b\,(mod\,m) \Longrightarrow a - b = km$$
$$n|m \Longrightarrow m = nq$$

onde k e $q > 0$ são inteiros. Portanto:

$$a - b = (kq)n \quad \text{e} \quad a \equiv b\,(mod\,n).$$

□

Teorema 2.11.6. *Se $a \equiv b\,(mod\,n)$ e se c é um inteiro positivo, então $ac \equiv bc\,(mod\,mc)$.*

(Fonte: Alencar Filho (1986, p. 24-25))

Demonstração. Com efeito, se $a \equiv b\,(mod\,m)$, então:

$$a - b = km \quad \text{e} \quad ac - bc = k(mc).$$

e, portanto:

$$ac \equiv bc\,(mod\,mc).$$

□

Teorema 2.11.7. *Se $a \equiv b\,(mod\,m)$ e se a, b e m são todos divisíveis pelo inteiro positivo d, então:*

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

(Fonte: Alencar Filho (1986, p. 25))

Demonstração. Com efeito, se $a \equiv b\,(mod\,m)$, então:

$$a - b = km \quad \text{e} \quad \frac{a}{d} - \frac{b}{d} = k.\frac{m}{d},$$

e, portanto:

$$\frac{a}{d} \equiv \frac{b}{d} (mod \frac{m}{d}).$$

□

Teorema 2.11.8. *Sejam* $a, b \in \mathbb{Z}$ *e* $m, m_1, ..., m_r$ *inteiros maiores do que 1. Temos que:*

$$a \equiv b (mod\, m_i), \forall i = 1, ..., r \iff a \equiv b (mod\, m), \textit{ onde } m = mmc(m_1, ..., m_r).$$

(Fonte: Hefez (2013, p. 197-198))

Demonstração. Se $a \equiv b (mod\, m_i)$, $i = 1, ..., r$, então $m_i | b - a$, para todo i. Sendo $b - a$ um múltiplo de cada m_i, segue-se que $m = mmc(m_1, ..., m_r) | b - a$, o que prova que $a \equiv b (mod\, m)$, onde $m = mmc(m_1, ..., m_r)$.
A recíproca decorre do **Teorema 2.11.5**. □

2.11.4 Simplificação das Congruências

Teorema 2.11.9. *Se* $ac \equiv bc (mod\, m)$ *e se o* $mdc(c, m) = 1$*, então* $a \equiv b (mod\, m)$ *.*

(Fonte: Alencar Filho (1986, p. 26))

Demonstração. Com efeito, se $ac \equiv bc (mod\, m)$, então:

$$m | (ac - bc) \quad \text{e} \quad m | (a - b)c.$$

Como o $mdc(c, m) = 1$, segue-se do Lema de Gauss que $m | (a - b)$ e, portanto:

$$a \equiv b (mod\, m) .$$

□

Corolário 2.11.3. *Se* $ac \equiv bc (mod\, p)$*, com* p *primo, e se* p *não divide* c*, então* $a \equiv b (mod\, p)$.

(Fonte: Alencar Filho (1986, p. 27))

Demonstração. As condições: p não divide c e p primo implicam ser o $mdc(c, p) = 1$ e, portanto, pelo **Teorema 2.11.9**:

$$a \equiv b (mod\, p).$$

□

Teorema 2.11.10. *Se* $ac \equiv bc (mod\, m)$ *e se o* $mdc(c, m) = d$*, então* $a \equiv b \left(mod \frac{m}{d}\right)$ *.*

(Fonte: Alencar Filho (1986, p. 27-28))

Demonstração. Com efeito, se $ac \equiv bc (mod\, m)$, então:

$$ac - bc = (a - b)c = km, \quad \text{com } k \in \mathbb{Z}.$$

Como $mdc(c, m) = d$, existem inteiros r e s tais que $c = dr$ e $m = ds$, com r e s primos entre si. Portanto:

$$(a - b)dr = kds \quad \text{ou} \quad (a - b)r = ks,$$

o que implica:

$$s|(a - b)r, \qquad \text{com o } mdc(r, s) = 1.$$

Logo:

$$s|(a - b) \quad \text{e} \quad a \equiv b\,(mod\, s) \quad \text{ou} \quad a \equiv b\,\left(mod\, \tfrac{m}{d}\right).$$

□

Exemplo 2.11.1. *Dados os inteiros $a, b \in \mathbb{Z}$. Sendo m um inteiro maior do que 1, demonstre que se $a \equiv b\,(mod\, m)$, então:*

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

(Fonte: Hefez (2013, p. 197-198))

Demonstração. Se $a \equiv b\,(mod\, m)$, então $m|b - a$ e, portanto, $b = a + tm$, com $t \in \mathbb{Z}$. Logo, pelo **Lema 2.7.1**, temos que:

$$mdc(a, m) = mdc(a + tm, m) = mdc(b, m).$$

□

Teorema 2.11.11 (Pequeno Teorema de Fermat)**.** *Seja p um primo. Se p não divide a, então:*

$$a^{p-1} \equiv 1\,(mod\, p).$$

(Fonte: Feitosa (2012))

Demonstração. Considere o conjunto de inteiros $B = \{a, 2a, 3a, ..., (p - 1)a\}$ onde a é um inteiro satisfazendo $mdc(a, p) = 1$. Nenhum deles é divisível por p e quaisquer dois deles são incongruentes módulo p, em virtude do **Teorema 2.11.9**. Assim, o conjunto dos restos dos elementos de B coincide com o conjunto dos restos não nulos na divisão por p, a saber, $\{1, 2, 3, ..., p - 1\}$. Portanto,

$$a\,.\,2a\,.\,3a\,...\,(p - 1)a \equiv 1\,.\,2\,.\,3\,...\,(p - 1)\,(mod\, p)$$
$$a^{p-1}(p - 1)! \equiv (p - 1)!\,(mod\, p)$$

Podemos cancelar o termo $(p-1)!$ em ambos os lados, pois $mdc((p-1)!, p) = 1$, concluindo, assim, a demonstração do teorema. □

Corolário 2.11.4. *Se p é um primo, então $a^p \equiv a\,(mod\,p)$, qualquer que seja o inteiro a.*
(Fonte: Alencar Filho (1986, p. 64))

Demonstração. Se p divide a $(p|a)$, então $a \equiv 0\,(mod\,p)$ e $a^p \equiv 0\,(mod\,p)$, o que implica

$$a^p \equiv a\,(mod\,p).$$

Se p não divide a $(p \nmid a)$, sabendo que $a \equiv a\,(mod\,p)$, temos pelo Pequeno Teorema de Fermat:

$$a^{p-1} \equiv 1\,(mod\,p) \text{ e } a^p \equiv a\,(mod\,p).$$

□

Observação: Este corolário nada mais é do que uma outra versão para o Pequeno Teorema de Fermat.

Exemplo 2.11.2. *Sejam p um número primo e $a, b \in \mathbb{Z}$. Vamos mostrar que*

$$(a+b)^p \equiv a^p + b^p\,(mod\,p)$$

(Fonte: Hefez (2013, p. 195))

Demonstração. O resultado decorre do Pequeno Teorema de Fermat, pois

$$a^p \equiv a\,(mod\,p)$$
$$b^p \equiv b\,(mod\,p)$$
$$(a+b)^p \equiv (a+b)\,(mod\,p).$$

Daí, $a^p + b^p \equiv (a+b)\,(mod\,p)$. Portanto:

$$(a+b)^p \equiv a^p + b^p\,(mod\,p).$$

□

Exemplo 2.11.3. *Se $a, b \in \mathbb{Z}$ e p é primo, então $(a-b)^p \equiv a^p - b^p\,(mod\,p)$.*
(Fonte: Hefez (2013, p. 195))

Demonstração. Pelo **Exemplo 2.11.2**, temos que

$$a^p = (a-b+b)^p \equiv (a-b)^p + b^p\,(mod\,p),$$

ou seja,

$$(a-b)^p \equiv a^p - b^p\,(mod\,p).$$

□

Exemplo 2.11.4. *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Vamos mostrar que*

$$a^p \equiv b^p \,(mod\, p) \Longrightarrow a^p \equiv b^p \,(mod\, p^2).$$

(Fonte: Hefez (2013, p. 195-196))

Demonstração. De fato, sabemos pelo **Exemplo 2.11.3** que

$$a^p - b^p \equiv (a-b)^p \,(mod\, p).$$

Como, por hipótese, temos que p divide $a^p - b^p$, segue-se, da congruência acima, que $p|(a-b)^p$; logo, $p|(a-b)$; ou seja, $a \equiv b \,(mod\, p)$. Isto implica que $a^i \equiv b^i \,(mod\, p)$ para todo $i \in \mathbb{N}$. Decorre daí que

$$a^{p-1} + ba^{p-2} + ... + b^{p-2}a + b^{p-1} \equiv pb^{p-1} \equiv 0 \,(mod\, p)$$

Logo, o resultado decorre, pois

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

e ambos os fatores no lado direito são divisíveis por p. □

Lema 2.11.1. *Se $mdc(a, m) = 1$, então existe um inteiro x tal que*

$$ax \equiv 1 \,(mod\, m).$$

Tal x é único módulo m. Se $mdc(a, m) > 1$, então não existe tal x.

(Fonte: Feitosa (2012))

Demonstração. Pelo **Teorema 2.7.5**, existem inteiros x e y tais que $ax + my = 1$. Analisando essa congruência módulo m, obtemos $ax \equiv 1 \,(mod\, m)$. Se y é outro inteiro que satisfaz a congruência, temos $ax \equiv ay \,(mod\, m)$. Pelo **Teorema 2.11.9**, $x \equiv y \,(mod\, m)$. Se $d = mdc(a, m) > 1$, não podemos ter $d|m$ e $m|ax - 1$ pois $d \nmid ax - 1$. □

Teorema 2.11.12 (Teorema de Wilson)**.** *Se p é primo, então*

$$(p-1)! \equiv -1 \,(mod\, p).$$

(Fonte: Feitosa (2012))

Demonstração. Em virtude do lema anterior, para cada $a \in \{2, 3, ..., p-2\}$ existe um resto $x \in \{0, 1, 2, ..., p-1\}$ tal que $ax \equiv 1 \,(mod\, p)$. Se $x = 1$ ou $x = p-1$, teríamos $a = 1$ ou $p-1$. Além disso, não podemos ter $a = x$, pois os únicos restos que satisfazem $a^2 \equiv 1 \,(mod\, p)$ são 1 e $p-1$. Com isso, podemos agrupar os números de $\{2, 3, ..., p-2\}$ em pares onde o produto deixa resto 1 por p, o que nos permite concluir que o produto de todos eles também deixa resto 1 por p. Logo,

$$(p-1)! \equiv -1.(p-1) \equiv -1 \,(mod\, p).$$

□

Um conjunto S é chamado de sistema completo de resíduos módulo n, denotado abreviadamente por **scr**, se para cada $0 \leq i \leq n-1$ existe um elemento $s \in S$ tal que $i \equiv s\,(mod\,n)$. Para qualquer a, o conjunto $\{a, a+1, a+2, ..., a+(n-1)\}$ é um exemplo de **scr**.

(Fonte: Feitosa (2012))

Exemplo 2.11.5. *Se $mdc(m,s) = 1$, mostre que $\{t, t+s, t+2s, t+(m-1)s\}$ é um **scr**.*

(Fonte: Feitosa (2012))

Demonstração. Pelo **Teorema 2.11.9**, se $t+is \equiv t+js\,(mod\,m)$, temos $is \equiv js\,(mod\,m)$ e $i \equiv j\,(mod\,m)$. Como $i, j \in \{0, 1, ..., m-1\}$, $i = j$. Isso nos diz que temos m inteiros que deixam restos distintos na divisão por m. Como existem exatamente m restos na divisão por m, o conjunto é um **scr**. □

Dado $n \in \mathbb{N}$, denotaremos o número de naturais menores ou iguais a n e relativamente primos com n por $\phi(n)$.

Segue imediatamente da definição de $\phi(n)$ que $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(5) = 4$ e $\phi(6) = 2$. Se p é primo, $\phi(p) = p - 1$.

(Fonte: Feitosa (2012))

Lema 2.11.2. *Se p é um número primo e k um número natural, então:*

$$\phi(p^k) = p^{k-1}(p-1).$$

(Fonte: Feitosa (2012))

Demonstração. Os únicos números do conjunto $\left\{1, 2, ..., p^k\right\}$ que não são relativamente primos com p^k são aqueles que são divisíveis por p. A quantidade de tais números é $\dfrac{p^k}{p} = p^{k-1}$. Sendo assim, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Lema 2.11.3. *Sejam m um número natural, l um número natural relativamente primo com m, e r um inteiro arbitrário. Então, o conjunto*

$$r, l+r, 2l+r, ..., (m-1)l+r$$

é um sistema completo de restos módulo m.

(Fonte: Feitosa (2012))

Demonstração. Suponha, por absurdo, que existem dois inteiros i e j com $0 \leq i < j < m$ e para os quais tenhamos $r + il \equiv r + jl\,(mod\,m)$. Assim, $(j-i)l \equiv 0\,(mod\,m)$. Como l é relativamente primo com m, devemos ter $j - i \equiv 0\,(mod\,m)$. Obtemos um absurdo, pois $0 < j - i < m$. Consequentemente, temos um conjunto de m inteiros todos incongruentes módulo m e, portanto, tal conjunto é um sistema completo de restos. □

Teorema 2.11.13. *Se l e m são números naturais primos entre si, então:*

$$\phi(ml) = \phi(m)\phi(l)$$

(Fonte: Feitosa (2012))

Demonstração. Como $\phi(1) = 1$, o teorema anterior é válido quando $m = 1$ ou $l = 1$. Suponha, então, que $m, l > 1$. Façamos uma contagem dupla. Primeiramente, usando a definição $\phi(ml)$ é o número de inteiros da tabela abaixo que são relativamente primos com ml.

1,	2,	...,	r,	...,	l,
$l+1$	$l+2$	...,	$l+r$	...,	$2l$
$2l+1$	$2l+2$	...,	$2l+r$	...,	$3l$
...,	...,	...,	...,	...,	...,
$(m-1)l+1$	$(m-1)l+2$	...,	$(m-1)l+r$	...,	ml

Seja $r \leq m$ um número natural qualquer. Considerando a r-ésima coluna da tabela, se $mdc(r, l) > 1$, nenhum de seus elementos é relativamente primo com l. Então, se buscamos os elementos que não possuem nenhum fator em comum com ml, devemos nos ater às colunas com $mdc(r, l) = 1$. O número de tais colunas é $\phi(l)$. Considerando agora a r-ésima coluna, e supondo que $mdc(r, l) = 1$, em virtude do lema anterior, sabemos que os restos de seus elementos na divisão por m formam exatamente o conjunto $\{0, 1, ..., m\}$, e dentre eles existem exatamente $\phi(m)$ números relativamente primos com m. Sendo assim, podemos contar os números relativamente primos com ml através do número de colunas “boas" e do número de “bons" elementos em cada uma delas, obtendo: $\phi(m)\phi(l)$. □

Corolário 2.11.5. *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ é a fatoração em primos de n, então:*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

(Fonte: Feitosa (2012))

Demonstração.

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)...p_k^{\alpha_k - 1}(p_k - 1) \\
&= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} ... p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)...(p_k - 1) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

□

Teorema 2.11.14 (Teorema de Euler)**.** *Se* $mdc(a, m) = 1$*, então*

$$a^{\phi(m)} \equiv 1 \,(mod\, m).$$

(Fonte: Feitosa (2012))

Demonstração. A prova deste teorema será muito similar à prova do Pequeno Teorema de Fermat.

Sejam $r_1, r_2, ..., r_{\phi(m)}$ os restos em $\{0, 1, 2, ..., m-1\}$ que são relativamente primos com m. Considere o conjunto $\left\{ar_1, ar_2, ..., ar_{\phi(m)}\right\}$. Se dois de seus membros deixam o mesmo resto por m, digamos:

$$ar_i \equiv ar_j \,(mod\, m);$$

temos $r_i \equiv r_j \,(mod\, m)$ pois $mdc(a, m) = 1$. Claramente isso é uma contradição. Além disso, $mdc(ar_i, m) = mdc(m, r_i) = 1$. Analisando os restos na divisão por m dos membros desse novo conjunto, podemos concluir que tal conjunto coincide com o conjunto dos restos iniciais. Assim,

$$\begin{aligned} r_1, r_2, ..., r_{\phi(m)} &\equiv ar_1, ar_2, ..., ar_{\phi(m)} \\ &\equiv a^{\phi(m)} r_1.r_2...r_{\phi(m)}. \end{aligned}$$

Como $mdc(r_1.r_2...r_{\phi(m)}, m) = 1$, podemos cancelar esse termo em ambos os membros da congruência anterior, obtendo, assim, o teorema de Euler. □

2.12 Classes Residuais

Seja dado um inteiro $m > 1$. Vamos repartir o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Isso nos dá a seguinte partição de $\mathbb{Z}$:

$$\begin{aligned} [0] &= \{x \in \mathbb{Z};\, x \equiv 0 \,(mod\, m)\} \\ [1] &= \{x \in \mathbb{Z};\, x \equiv 1 \,(mod\, m)\} \\ &\vdots \\ [m-1] &= \{x \in \mathbb{Z};\, x \equiv m-1 \,(mod\, m)\} \end{aligned}$$

Paramos em $[m-1]$, pois tem-se que $[m] = [0]$, $[m+1] = [1], ...$

O conjunto

$$[a] = \{x \in \mathbb{Z};\, x \equiv a \,(mod\, m)\}$$

é chamado de *classe residual módulo m* do elemento a de $\mathbb{Z}$. O conjunto de todas as classes residuais módulo m será representado por $\mathbb{Z}_m$. Portanto,

$$\mathbb{Z}_m = \{[0], [1], ..., [m-1]\}.$$

(Fonte: Hefez (2013, p. 263))

Exemplo 2.12.1. *Seja* $m = 2$*. Então,*
$[0] = \{x \in \mathbb{Z};\ x \equiv 0\,(mod\,2)\} = \{x \in \mathbb{Z};\ x$ *é par* $\}$*, e*
$[1] = \{x \in \mathbb{Z};\ x \equiv 1\,(mod\,2)\} = \{x \in \mathbb{Z};\ x$ *é ímpar* $\}$*.*
Temos, portanto, que $[a] = [0]$ *se, e somente se,* a *é par e* $[a] = [1]$ *se, e somente se,* a *é ímpar.*

(Fonte: Hefez (2013, p. 263))

Exemplo 2.12.2. *Seja* $m = 3$*. Então,*

$$\begin{aligned} [0] &= \{3t;\ t \in \mathbb{Z}\} \\ [1] &= \{3t+1;\ t \in \mathbb{Z}\} \\ [2] &= \{3t+2;\ t \in \mathbb{Z}\} \end{aligned}$$

Tem-se que

$$x \in \begin{cases} [0] & , \text{ se a múltiplo de } 3 \\ [1] & , \text{ se a tem resto } 1 \text{ quando dividido por } 3 \\ [2] & , \text{ se a tem resto } 2 \text{ quando dividido por } 3 \end{cases}$$

(Fonte: Hefez (2013, p. 264))

2.12.1 Propriedades das Classes Residuais

Consideremos a relação de equivalência R em $\mathbb{Z}$ definida por

$$aRb \Longleftrightarrow a \equiv b\,(mod\,).$$

Segundo a definição (de classe residual), a classe residual módulo m de um inteiro qualquer a outra coisa não é senão a classe de equivalência segundo esta relação R de a; isto é, toda classe residual é uma classe de equivalência. Assim sendo, as classes residuais módulo m de dois inteiros quaisquer a e b gozam das propriedades:

(1) $[a] = [b] \Longleftrightarrow a \equiv b\,(mod\,m)$
(2) $[a] \cap [b] \neq \phi \Longrightarrow [a] = [b]$
(3) $[a] \neq [b] \Longrightarrow [a] \cap [b] = \phi$

(Fonte: Alencar Filho (1986, p. 16))

Em $\mathbb{Z}_m$ podemos definir as seguintes operações:
Adição: $[a] + [b] = [a + b]$ e
Multiplicação: $[a].[b] = [a.b]$,
que gozam das seguintes propriedades:
Propriedades da adição:
Para todos $[a], [b], [c] \in \mathbb{Z}_m$, temos
A$_1$) **Associatividade** $([a] + [b]) + [c] = [a] + ([b] + [c])$;

A$_2$) **Comutatividade** $[a] + [b] = [b] + [a]$;
A$_3$) **Existência de zero** $[a] + [0] = [a]$ para todo $[a] \in \mathbb{Z}_m$;
A$_4$) **Existência de simétrico** $[a] + [-a] = [0]$.
Propriedades da multiplicação:
Para todos $[a], [b], [c] \in \mathbb{Z}_m$, temos
M$_1$) **Associatividade** $([a].[b]).[c] = [a].([b].[c])$;
M$_2$) **Comutatividade** $[a].[b] = [b].[a]$;
M$_3$) **Existência da unidade** $[a].[1] = [a]$;
AM) **Distributividade** $[a].([b] + [c]) = [a].[b] + [a].[c]$.
(Fonte: Hefez (2013, p. 265-266))

Um elemento $[a] \in \mathbb{Z}_m$ será dito *invertível* quando existir $[b] \in \mathbb{Z}_m$ tal que $[a].[b] = 1$. Nesse caso, diremos que $[b]$ é o inverso de $[a]$.

Proposição 2.12.1. *Um elemento* $[a] \in \mathbb{Z}_m$ *é invertível se, e somente se,* $mdc(a, m) = 1$.
(Fonte: Hefez (2013, p. 269))

Demonstração. Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a].[b] = [a.b]$. Logo, $a.b \equiv 1\,(mod\, m)$, isto é, existe um inteiro t tal que $a.b + t.m = 1$ e, consequentemente, $mdc(a, m) = 1$.

Reciprocamente, se $mdc(a, m) = 1$, existem inteiros b e t tais que $a.b + m.t = 1$ e, consequentemente, $[1] = [a.b + m.t] = [a.b] + [m.t] = [a].[b] + [0] = [a].[b]$. Portanto, $[a]$ é invertível. □

Exemplo 2.12.3. *Construa as tabelas da adição e da multiplicação em* $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$, *e* $\mathbb{Z}_5$.
(Fonte: Hefez (2013, p. 267-268))

Resolução.
Em $\mathbb{Z}_2 = \{[0], [1]\}$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$.$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Em $\mathbb{Z}_3 = \{[0], [1], [2]\}$

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$.$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Em $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$.$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Em $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$.$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Observe que:
em $\mathbb{Z}_2$, $[1]$ é invertível, pois $[1].[1] = [1]$. Além disso, $mdc(1, 2) = 1$.
em $\mathbb{Z}_3$, todo elemento não nulo é invertível, pois $[1].[1] = [1]$ e $[2].[2] = [1]$. Além disso, $mdc(1, 3) = 1 = mdc(2, 3)$.
em $\mathbb{Z}_4$, $[1]$ e $[3]$ são invertíveis, pois $[1].[1] = [1]$ e $[3].[3] = [1]$. Além disso, $mdc(1, 4) = 1 = mdc(3, 4)$.
em $\mathbb{Z}_5$, todo elemento não nulo é invertível, pois $[1].[1] = [1]$, $[2].[3] = [3].[2] = [1]$ e $[4].[4] = [1]$. Além disso, $mdc(1, 5) = mdc(2, 5) = mdc(3, 5) = mdc(4, 5) = 1$.

Exemplo 2.12.4. *Resolver a congruência* $4x \equiv 3\,(mod\,5)$ *equivale a resolver em* $\mathbb{Z}_5$ *a equação*

$$[4]Z = [3] \tag{2.1}$$

(Fonte: Hefez (2013, p. 269))

Olhando a tabela da multiplicação de $\mathbb{Z}_5$, vemos que $[4].[4] = [1]$. Logo, $[4]$ é invertível em $\mathbb{Z}_5$ com inverso $[4]$. Portanto, multiplicando ambos os membros da equação (2.1) por $[4]$ obtemos

$$[1]Z = [4][4]Z = [4][3] = [2].$$

Portanto, $Z = [2]$, o que nos diz que as soluções de (2.1) são $x = 2 + 5t$, onde $t \in \mathbb{Z}$.

3 EQUAÇÕES DIOFANTINAS LINEARES

Neste capítulo, estudaremos o clássico teorema que versa sobre a resolução de equações diofantinas lineares nas incógnitas x e y, além dos métodos de Euler e dos “múltiplos". Usando congruências e noções de classes residuais, resolveremos algumas equações diofantinas lineares. Também veremos alguns casos práticos, a saber: Critério do Algarismo Final, Critério da Multiplicidade e Critério do Agrupamento que, em certas condições específicas, podem reduzir os passos na resolução de problemas. Destacamos que grande parte dos métodos utilizados para resolver equações diofantinas lineares nas incógnitas x e y também foram utilizados na resolução de equações diofantinas do tipo $ax + by + cz = c$, nas incógnitas x, y e z.

3.1 Generalidades

Para Alencar Filho (1987, p. 372-373), o tipo mais simples de equação diofantina é a equação diofantina linear com duas incógnitas x e y:

$$ax + by = c,$$

onde a, b e c são inteiros dados, sendo $ab \neq 0$.

Todo par de inteiros x_0, y_0 tais que $ax_0 + by_0 = c$ diz-se uma *solução inteira* ou apenas uma *solução* da equação $ax + by = c$.

Consideremos, p. ex., a equação diofantina linear com duas incógnitas x e y:

$$3x + 6y = 18$$

Temos:

$$3.4 + 6.1 = 18$$

$$3(-6) + 6.6 = 18$$

$$3.10 + 6(-2) = 18$$

Logo, os pares de inteiros 4 e 1, -6 e 6, 10 e -2 são *soluções* da equação $3x + 6y = 18$.

Existem equações diofantinas lineares com duas incógnitas que não têm solução. Assim, p. ex., a equação diofantina linear com duas incógnitas x e y:

$$2x + 4y = 7$$

não tem solução, porque $2x + 4y$ é um inteiro par, quaisquer que sejam os valores inteiros x e y, enquanto 7 é um inteiro ímpar (observe que $mdc(2, 4) = 2$ e 2 não divide 7).

3.2 Condição de existência de solução da equação $ax + by = c$

Teorema 3.2.1. *A equação diofantina linear com duas incógnitas x e y:*

$$ax + by = c$$

tem solução se, e somente se, d divide c, sendo $d = mdc(a, b)$.

(Fonte: Alencar Filho (1987, p. 373-374))

Demonstração. $(\Longrightarrow)$ Suponhamos que a equação $ax + by = c$ tem solução, i. é., que existe um par de inteiros x_0, y_0 tais que $ax_0 + by_0 = c$.

Por ser o $mdc(a, b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, o que implica:

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$$

E como $rx_0 + sy_0$ é um inteiro, segue-se que d divide c ($d|c$).

$(\Longleftarrow)$ Reciprocamente, suponhamos que d divide c ($d|c$); isto é, que $c = dt$, onde t é um inteiro.

Por ser o $mdc(a, b) = d$, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$, o que implica:

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$$

isto é, o par de inteiros:

$$tx_0 = (c/d)x_0 \quad , \quad ty_0 = (c/d)y_0$$

é uma solução da equação $ax + by = c$. □

3.3 Soluções da equação $ax + by = c$

Teorema 3.3.1. *Se d divide c, sendo $d = mdc(a, b)$, e se o par de inteiros x_0, y_0 é uma solução particular da equação diofantina linear com duas incógnitas x e y:*

$$ax + by = c$$

então, todas as soluções desta equação são dadas pelas fórmulas:

$$x = x_0 + (b/d)t \quad , \quad y = y_0 - (a/d)t$$

onde t é um inteiro arbitrário.

(Fonte: Alencar Filho (1987, p. 374-375))

Demonstração. Suponhamos que o par de inteiros x_0, y_0 é uma solução particular da equação $ax + by = c$, e seja x_1, y_1 um outro par qualquer de inteiros que também é solução desta mesma equação. Então, temos:

$$ax_0 + by_0 = c = ax_1 + by_1$$

e, portanto:

$$a(x_1 - x_0) = b(y_0 - y_1)$$

Como $mdc(a, b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, com r e s primos entre si. Substituindo estes valores de a e b na igualdade anterior, e cancelando o fator comum d, obtemos:

$$r(x_1 - x_0) = s(y_0 - y_1)$$

Assim sendo, $r|s(y_0 - y_1)$, e como r é primo com s, segue-se que r divide $(y_0 - y_1)$, isto é:

$$y_0 - y_1 = rt \quad \text{e} \quad x_1 - x_0 = st$$

onde t é um inteiro. Logo, temos as fórmulas:

$$x_1 = x_0 + st = x_0 + (b/d)t$$

$$y_1 = y_0 - rt = y_0 - (a/d)t$$

□

Podemos verificar que estes x_1 e y_1 satisfazem realmente a equação $ax + by = c$, qualquer que seja o inteiro t, pois temos:

$$ax_1 + by_1 = a[x_0 + (b/d)t] + b[y_0 - (a/d)t] =$$

$$= (ax_0 + by_0) + (ab/d - ab/d)t = c + 0.t = c$$

Corolário 3.3.1. *Se o $mdc(a, b) = d = 1$ e se x_0, y_0 é uma solução particular da equação diofantina linear $ax + by = c$, então todas as soluções desta equação são dadas pelas fórmulas:*

$$x = x_0 + bt \qquad , \qquad y = y_0 - at$$

onde t é inteiro arbitrário.

(Fonte: Alencar Filho (1987, p. 375-376)

Observação 3.3.1. *Alencar Filho (1987, p. 376) afirma que, consoante o* ***Teorema 3.3.1****, a determinação das soluções da equação diofantina linear* $ax + by = c$ *reduz-se em achar uma solução particular* x_0*,* y_0 *desta equação, porque, conhecida esta, as fórmulas gerais:*

$$x = x_0 + (b/d)t \qquad , \qquad y = y_0 - (a/d)t$$

dão diretamente todas as soluções, fazendo nelas, sucessivamente, $t = \pm 1, \pm 2, \pm 3, ...$

3.4 Resolução da equação $ax + by = c$ pelo algoritmo de Euclides

Segundo Alencar Filho (1987, p. 379-380), uma solução particular x_0, y_0 da equação diofantina linear $ax + by = c$ pode sempre ser obtida por intermédio do **algoritmo de Euclides**, conforme será mostrado no exemplo a seguir.

Exemplo 3.4.1. *Usando o algoritmo de Euclides, resolva a equação diofantina linear:*

$$172x + 20y = 1000.$$

$$\begin{aligned} 172 &= 20.8 + 12 \\ 20 &= 12.1 + 8 \\ 12 &= 8.1 + 4 \\ 8 &= 4.2 \end{aligned}$$

	8	1	1	2
172	20	12	8	4
12	8	4	0	

Portanto, o $mdc(172, 20) = 4$, e como 4 divide 1000 ($4|1000$), segue-se que a equação dada admite soluções.

Posto isto, cumpre agora obter a expressão do inteiro 4 como combinação linear de 172 e 20, para o que, basta eliminar sucessivamente os restos 8 e 12 entre as três primeiras igualdades anteriores do seguinte modo:

$$\begin{aligned} 4 &= 12 - 8 \\ 4 &= 12 - (20 - 12) \\ 4 &= 2.12 - 20 \\ 4 &= 2(172 - 20.8) - 20 \\ 4 &= 172.2 + 20.(-17) \end{aligned}$$

Multiplicando ambos os membros da última igualdade por $1000/4 = 250$, obtemos:

$$1000 = 172.500 + 20.(-4250)$$

Portanto, o par de inteiros $x_0 = 500$, $y_0 = -4250$ é uma solução particular da equação proposta e, por conseguinte, todas as soluções desta equação são dadas pelas fórmulas:

$$x = 500 + (20/4)t = 500 + 5t$$

$$y = -4250 - (172/4)t = -4250 - 43t$$

onde t é um inteiro arbitrário.

NOTA As soluções inteiras e positivas se obtêm atribuindo ao inteiro t valores para os quais se tem:

$$500 + 5t > 0 \qquad \text{e} \qquad -4250 - 43t > 0$$

isto é:

$$t > -100 \qquad \text{e} \qquad t < -98\frac{36}{43}$$

o que implica $t = -99$ e, portanto:

$$x = 500 + 5(-99) = 5 \qquad , \qquad y = -4250 - 43(-99) = 7$$

Assim, o par de inteiros $x = 5$ e $y = 7$ é a única solução **inteira e positiva** da equação $172x + 20y = 1000$.

3.5 Resolução da equação $ax + by = c$ pelo método de Euler

As equações diofantinas com duas incógnitas podem também ser resolvidas por um método devido a L. EULER, que vamos explanar com detalhes através de um exemplo numérico.

Exemplo 3.5.1. *Resolva a equação diofantina linear:*

$$370x + 153y = 2001.$$

(Fonte: Alencar Filho (1987, p. 381-383))

Resolução. (Método de EULER). O $mdc(370, 153) = 1$, de modo que a equação dada admite soluções. Suponhamos que o par de inteiros x e y é uma destas soluções. Resolvendo-se a equação em relação a y (incógnita de menor coeficiente), temos:

$$y = \frac{2001 - 370x}{153} = 13 - 2x + \frac{12 - 64x}{153} = 13 - 2x + 4.\frac{3 - 16x}{153}$$

Sendo x e y inteiros, então $\dfrac{3 - 16x}{153}$ deve também ser um inteiro t:

$$\frac{3 - 16x}{153} = t \qquad \text{ou} \qquad 16x + 153t = 3$$

que é uma equação diofantina linear nas incógnitas x e t. Resolvendo esta equação em relação a x (incógnita de menor coeficiente), temos:

$$x = \frac{3 - 153t}{16} = -9t + \frac{3 - 9t}{16} = -9t + 3.\frac{1 - 3t}{16}$$

Sendo x e t inteiros, então $\frac{1 - 3t}{16}$ deve também ser um inteiro u:

$$\frac{1 - 3t}{16} = u \qquad \text{ou} \qquad 3t + 16u = 1$$

que é uma equação diofantina linear nas incógnitas t e u. Resolvendo esta equação em relação a t (incógnita de menor coeficiente), temos:

$$t = \frac{1 - 16u}{3} = -5u + \frac{1 - u}{3}$$

Como t e u são inteiros, então $\frac{1 - u}{3}$ deve também ser inteiro v:

$$\frac{1 - u}{3} = v \qquad \text{ou} \qquad u + 3v = 1$$

que é uma equação diofantina linear nas incógnitas u e v, e como o coeficiente de u é a unidade, uma solução particular desta equação é $u = 1$, $v = 0$, e por meio de substituições sucessivas, obtemos:

$$t = -5u + v = -5.1 + 0 = -5$$

$$x = -9t + 3u = (-9)(-5) + 3.1 = 48$$

$$y = 13 - 2x + 4t = 13 - 2.48 + 4(-5) = -103$$

Portanto, o par de inteiros $x = 48$, $y = -103$ é uma solução particular da equação diofantina linear $370x + 153y = 2001$, de modo que todas as soluções desta equação são dadas pelas fórmulas:

$$x = x_0 + (b/d)w = 48 + 153w$$

$$y = y_0 - (a/d)w = -103 - 370w$$

onde w é um inteiro arbitrário.

Exemplo 3.5.2. *Resolva a equação diofantina linear* $13x + 24y = 17$*, sabendo que ela admite a solução* $x = 5$ *e* $y = -2$*.*

(Fonte: Alencar Filho (1987, p. 383-384))

Resolução. Seja (x, y) uma solução qualquer da equação dada. Então:

$$13x + 24y = 17 \tag{3.1}$$

E como $x = 5$, $y = -2$ é uma solução particular da mesma equação, temos:

$$13.5 + 24.(-2) = 17 \tag{3.2}$$

Subtraindo ordenadamente (3.1) e (3.2), obtemos:

$$13.(x - 5) + 24.(y + 2) = 0$$

ou seja:

$$\frac{x-5}{24} = -\frac{y+2}{13} = t$$

Portanto, todas as soluções são dadas pelas fórmulas:

$$x = 5 + 24t \qquad , \qquad y = -2 - 13t,$$

onde t é um inteiro arbitrário.

Exemplo 3.5.3. *Resolva o sistema de duas equações diofantinas lineares com três incógnitas, x, y e z:*

$$\begin{cases} 3x + 5y + 6z = 104 \\ 9x + 3y + 8z = 164 \end{cases}$$

(Fonte: Alencar Filho (1987, p. 384-385))

Resolução. Como os coeficientes de y são primos entre si, é esta incógnita que cumpre eliminar de preferência, a fim de simplificar os cálculos, com o que obtemos a equação diofantina linear nas incógnitas x e z:

$$18x + 11z = 254$$

cujas soluções são dadas pelas fórmulas:

$$x = -3 + 11t \quad , \quad z = 28 - 18t$$

Substituindo estes valores de x e z numa das equações do sistema dado, na primeira, por exemplo, vem:

$$-9 + 33t + 5y + 168 - 108t = 104$$

ou

$$75t - 5y = 55 \quad \Longrightarrow \quad y = -11 + 15t$$

Portanto, todas as soluções do sistema proposto são dadas pelas fórmulas:

$$x = -3 + 11t \ , \ y = -11 + 15t \ , \ z = 28 - 18t, \quad t \in \mathbb{Z}$$

As **soluções inteiras e positivas** obtêm-se atribuindo ao inteiro t valores para os quais se tem:

$$-3 + 11t > 0 \ , \ -11 + 15t > 0 \ , \ 28 - 18t > 0$$

isto é:

$$t > \frac{3}{11} \ , \ t > \frac{11}{15} \ , \ t < \frac{14}{9} = 1\frac{5}{9}$$

o que implica $t = 1$ e, portanto: $x = 8$, $y = 4$ e $z = 10$ é a **única solução inteira e positiva** que admite o sistema proposto.

Exemplo 3.5.4. *Resolva o sistema de duas equações diofantinas lineares com três incógnitas x, y e z:*

$$\begin{cases} 6x + 9y + 14z = 77 \\ 4x + 15y + 7z = 51 \end{cases}$$

(Fonte: Alencar Filho (1987, p. 385-386))

Resolução. Eliminando uma das incógnitas, por exemplo, a incóginta z, obtemos a equação diofantina linear nas incógnitas x e y:

$$2x + 21y = 25$$

cujas soluções são dadas pelas fórmulas:

$$x = 2 + 21t \ , \ y = 1 - 2t$$

Substituindo estes valores de x e y numa das equações do sistema dado, na primeira, por exemplo, vem:

$$12 + 126t + 9 - 18t + 14z = 77$$

ou

$$7z + 54t = 28$$

equação diofantina linear nas incógnitas z e t, cujas soluções são dadas pelas fórmulas:

$$z = 4 - 54u \ , \ t = 7u$$

Substituindo o valor de t nos valores de x e y, temos, finalmente:

$$x = 2 + 147u \ , \ y = 1 - 14u \ , \ z = 4 - 54u,$$

fórmulas que dão a solução do sistema proposto.

As soluções inteiras e positivas obtêm-se atribuindo ao inteiro u valores para os quais se tem:

$$2 + 147u > 0 \ , \ 1 - 14u > 0 \ , \ 4 - 54u > 0$$

isto é:

$$u > -\frac{2}{147} \ , \ u < \frac{1}{14} \ , \ u < \frac{4}{54}$$

o que implica $u = 0$ e, portanto: $x = 2$, $y = 1$, $z = 4$ é a única solução inteira e positiva que admite o sistema proposto.

Exemplo 3.5.5. *Resolva a equação diofantina linear com três incógnitas x, y e z:*

$$10x + 9y + 7z = 58.$$

(Fonte: Alencar Filho (1987, p. 387-388))

Resolução. Resolvendo a equação dada em relação a z, incógnita de menor coeficiente, temos:

$$z = \frac{58 - 10x - 9y}{7} = 8 - x - y + \frac{2 - 3x - 2y}{7} = 8 - x - y + t$$

onde

$$\frac{2 - 3x - 2y}{7} = t \quad \text{ou} \quad 2 - 3x - 2y = 7t$$

Resolvendo esta última equação em relação a y, temos:

$$y = \frac{2 - 3x - 7t}{2} = 1 - x - 3t - \frac{x + t}{2} = 1 - x - 3t - u,$$

onde

$$\frac{x + t}{2} = u \quad \text{ou} \quad x = -t + 2u$$

Portanto:

$$y = 1 + t - 2u - 3t - u = 1 - 2t - 3u$$

e

$$z = 8 + t - 2u - 1 + 2t + 3u + t = 7 + 4t + u$$

são as fórmulas que dão todas as soluções da equação diofantina linear dada, atribuindo a t e u valores inteiros arbitrários.

As soluções inteiras e positivas obtêm-se atribuindo aos inteiros t e u valores para os quais se tem:

$$-t + 2u > 0 \ , \ 1 - 2t - 3u > 0 \ , \ 7 + 4t + u > 0$$

isto é:

$$t < 2u \ , \ t < \frac{1 - 3u}{2} \ , \ t > \frac{-7 - u}{4}$$

o que implica:

$$2u > \frac{-7 - u}{4} \quad \text{e} \quad \frac{1 - 3u}{2} > \frac{-7 - u}{4}$$

ou seja:

$$u > -\frac{7}{9} \quad \text{e} \quad u < \frac{9}{5} = 1\frac{4}{5}$$

de modo que só pode ser $u = 0$ e $u = 1$. Para $u = 0$, temos:

$$t < 0, \quad t < \frac{1}{2}, \quad t > -\frac{7}{4} = -1\frac{3}{4}$$

o que implica $t = -1$.

Para $u = 1$, temos:

$$t < 2, \quad t < -1, \quad t > -2,$$

o que é impossível.

Portanto, os únicos valores inteiros de t e u são $t = -1$ e $u = 0$, o que dá $x = 1$, $y = z = 3$ como única solução inteira e positiva da equação proposta.

NOTA: Uma equação diofantina linear com três incógnitas x, y e z: $ax + by + cz = d$ admite solução se, e somente se o $mdc(a, b, c)|d$, como é fácil provar.

(Fonte: Alencar Filho (1987, p. 388))

3.6 Soluções alternativas da equação $ax + by = c$

3.6.1 Forma geral para resolver uma equação diofantina linear de duas variáveis

Segundo Vera (2014, p. 11), para que a equação diofantina linear $ax + by = c$ nas incógnitas x e y, com $\{a, b, c, x, y\} \subset \mathbb{Z}$ e $ab \neq 0$ tenha solução, deve ocorrer que:

$$c = \overset{\circ}{\overline{mdc(a, b)}}$$

isto é, c tem que ser múltiplo do $mdc(a, b)$ ou, de modo análogo, o $mdc(a, b)$ tem que ser divisor de c.

Observação: O círculo $(\circ)$ sobre o inteiro x, isto é, o símbolo $\overset{\circ}{x}$ representa um múltiplo qualquer de x.

PASSOS A SEREM SEGUIDOS:

1. Calcula-se o mdc dos coeficientes de x e y, isto é, o $mdc(a, b)$;
2. Dividem-se ambos os lados da equação pelo $mdc(a, b)$;
3. Expressam-se todas as constantes em função do múltiplo do menor dos coeficientes (de preferência o menor, mas também podemos escolher o maior dos coeficientes). **Ter em conta que o múltiplo que se tome “absorve" uma das variáveis**;
4. Expressa-se a variável remanescente em função do múltiplo escolhido, para logo substituí-la na equação original, e assim obter o valor da segunda variável.

Exemplo 3.6.1. *Resolva a seguinte equação diofantina:*

$$5x + 2y = 17.$$

(Fonte: Vera (2014, p. 12-13))

Resolução.

Passo 1

$mdc(5, 2) = 1$

Observemos que $17 = \overset{\circ}{\overline{mdc(5, 2)}} = \overset{\circ}{1}$, isto é, 17 é múltiplo de 1 (ou 1 divide 17). Isto significa que a equação tem solução.

Passo 2

Dividimos ambos os membros da equação por 1 e obtemos:

$$5x + 2y = 17$$

Passo 3

Agora, expressamos todos os coefientes em função do múltiplo do menor deles, isto é, em função de 2. Neste caso, temos:

$$(\overset{\circ}{2} + 1)x + \overset{\circ}{2}\, y = \overset{\circ}{2} + 1$$

Passo 4

Isolamos a variável x, pois y será "absorvida" pelo múltiplo de 2.

$$\overset{\circ}{2}\, x + x + \overset{\circ}{2}\, y = \overset{\circ}{2} + 1$$

ou

$$\overset{\circ}{2} + x + \overset{\circ}{2} = \overset{\circ}{2} + 1$$

daí

$$x = \overset{\circ}{2} + 1$$

logo

$$x = 2n + 1$$

onde n é um inteiro qualquer.

Substituímos $x = 2n + 1$ na equação do **passo 2** e obtemos

$$y = 6 - 5n$$

Vamos, agora, expressar os coeficientes em função de 5 (o maior dos coeficientes) e retomemos o passo 3

Passo 3

$$\overset{\circ}{5}\, x + 2y = \overset{\circ}{5} + 2$$

Passo 4

Isolamos a variável y, pois x será "absorvida" pelo múltiplo de 5.

$$2y \overset{\circ}{=} 5 + 2$$

logo

$$y = 5n + 1$$

onde n é um inteiro qualquer.

Substituímos $y = 5n + 1$ na equação do **passo 2** e obtemos $x = -2n + 3$

NOTA: Com base na equação $2y \overset{\circ}{=} 5 + 2$, temos, de forma equivalente, a equação $2y = 5k + 2$, com k inteiro. Para que esta última igualdade se verifique, k tem que ser, necessariamente, par; isto é, k tem que ser da forma $2n, n \in \mathbb{Z}$. Daí:

$$2y = 5.(2n) + 2 \text{ ou } 2y = 2.(5n + 1)$$

Portanto, $y = 5n + 1$

Observe que a solução $y = 5n + 1$ e $x = -2n + 3$ é a mesma encontrada anteriormente, trocando-se n por $-n + 1$. Veja:

$$x = -2(-n + 1) + 3 \quad \text{e} \quad y = 5(-n + 1) + 1$$

ou seja,

$$x = 2n + 1 \quad \text{e} \quad y = -5n + 6$$

Na tabela abaixo, encontramos algumas soluções da equação:

n	...	-3	-2	-1	0	1	2	3	...
x=2n+1	...	-5	-3	-1	1	3	5	7	...
y=6-5n	...	21	16	11	6	1	-4	-9	...

Exemplo 3.6.2. *Resolva a seguinte equação diofantina:*

$$27x + 63y = 45.$$

(Fonte: Vera (2014, p. 13))

Resolução.

Passo 1

$mdc(27, 63) = 9$

Observemos que $45 \overset{\circ}{=} \overline{mdc(27, 63)} \overset{\circ}{=} 9$, isto é, 45 é múltiplo de 9 (ou 9 divide 45). Isto significa que a equação tem solução.

Passo 2

Dividimos ambos os membros da equação por 9 e obtemos:

$$3x + 7y = 5$$

Passo 3

Agora, expressamos todos os coeficientes em função do múltiplo do menor deles, isto é, em função de 3. Neste caso, temos:

$$\overset{\circ}{3}\, x + (\overset{\circ}{3} + 1)y = \overset{\circ}{3} + 2$$

Passo 4

Isolamos a variável y, pois x será "absorvida" pelo múltiplo de 3.

$$\overset{\circ}{3}\, x + \overset{\circ}{3}\, y + y = \overset{\circ}{3} + 2$$

ou

$$\overset{\circ}{3} + \overset{\circ}{3} + y = \overset{\circ}{3} + 2$$

daí

$$y = \overset{\circ}{3} + 2$$

logo

$$y = 3n + 2$$

onde n é um inteiro qualquer.

Substituímos $y = 3n + 2$ na equação do **passo 2** e obtemos

$$x = -7n - 3$$

Vamos, agora, expressar os coeficientes em função de 7 (o maior dos coeficientes) e retomemos o passo 3

Passo 3

$$3x + \overset{\circ}{7}\, y = 5$$

Passo 4

Isolamos a variável x, pois y será "absorvida" pelo múltiplo de 7.

$$\begin{aligned} 3x &= \overset{\circ}{7} + 5. \text{ Como } \quad 5 = 14 - 9 = \overset{\circ}{7} - 9, \text{ temos,} \\ 3x &= \overset{\circ}{7} - 9, \text{ portanto,} \\ x &= 7n - 3 \end{aligned}$$

onde n é um inteiro qualquer.

Substituímos $x = 7n - 3$ na equação do **passo 2** e obtemos $y = -3n + 2$.

Observe que a solução $x = 7n - 3$ e $y = -3n + 2$ é a mesma encontrada anteriormente, trocando-se n por $-n$. Veja:

$$x = 7(-n) - 3 \quad \text{e} \quad y = -3(-n) + 2$$

ou seja,

$$x = -7n - 3 \quad \text{e} \quad y = 3n + 2$$

Na tabela abaixo, encontramos algumas soluções da equação:

n	...	-3	-2	-1	0	1	2	3	...
x=-7n-3	...	18	11	4	-3	-10	-17	-24	...
y=3n+2	...	-7	-4	-1	2	5	8	11	...

Exemplo 3.6.3. *Resolva a seguinte equação diofantina:*

$$25x - 35y = 100.$$

(Fonte: Vera (2014, p. 13-14))

Resolução.

Passo 1

$mdc(25, 35) = 5$

Observemos que $100 = \overset{\circ}{mdc(25, 35)} = \overset{\circ}{5}$, isto é, 100 é múltiplo de 5 (ou 5 divide 100). Isto significa que a equação tem solução.

Passo 2

Dividimos ambos os membros da equação por 5 e obtemos:

$$5x - 7y = 20$$

Passo 3

Agora, expressamos todos os coeficientes em função do múltiplo do menor deles, isto é, em função de 5. Neste caso, temos:

$$\overset{\circ}{5}\, x - (\overset{\circ}{5} + 2)y = \overset{\circ}{5}$$

Passo 4

Isolamos a variável y, pois x será “absorvida" pelo múltiplo de 5.

$$\overset{\circ}{5}\, x - \overset{\circ}{5}\, y - 2y = \overset{\circ}{5}$$

ou

$$\overset{\circ}{5} - \overset{\circ}{5} - 2y = \overset{\circ}{5}$$

ou

$$-2y = \overset{\circ}{5}$$

daí

$$y = \overset{\circ}{5}$$

logo

$$y = 5n$$

onde n é um inteiro qualquer.

Observação:
Com base na equação $-2y = \overset{\circ}{5}$, temos, de forma equivalente, a equação $2y = 5k$, com k inteiro. Para que esta última igualdade se verifique, k tem que ser par, isto é, k tem que ser da forma $2n, n \in \mathbb{Z}$. Daí:

$$2y = 5.(2n) \text{ ou } 2y = 2.(5n)$$

Portanto, $y = 5n$

Substituímos $y = 5n$ na equação do **passo 2** e obtemos

$$x = 7n + 4$$

Na tabela abaixo, encontramos algumas soluções da equação:

n	...	-3	-2	-1	0	1	2	3	...
x=7n+4	...	-17	-10	-3	4	11	18	25	...
y=5n	...	-15	-10	-5	0	5	10	15	...

Exemplo 3.6.4. *Resolva a seguinte equação diofantina:*

$$36x + 28y = 52.$$

(Fonte: Vera (2014, p. 11-12))

Resolução.
Passo 1
$mdc(36, 28) = 4$
Observemos que $52 = \overset{\circ}{mdc(36, 28)} = \overset{\circ}{4}$, isto é, 52 é múltiplo de 4 (ou 4 divide 52). Isto significa que a equação tem solução.

Passo 2

Dividimos ambos os membros da equação por 4 e obtemos:

$$9x + 7y = 13$$

Passo 3

Agora, expressamos todos os coeficientes em função do múltiplo do menor deles, isto é, em função de 7. Neste caso, temos:

$$(\overset{\circ}{7} + 2)x + \overset{\circ}{7}\, y = \overset{\circ}{7} + 6$$

Passo 4

Isolamos a variável x, pois y será "absorvida" pelo múltiplo de 7.

$$\overset{\circ}{7}\, x + 2x + \overset{\circ}{7}\, y = \overset{\circ}{7} + 6$$

ou

$$\overset{\circ}{7} + 2x + \overset{\circ}{7} = \overset{\circ}{7} + 6$$

ou

$$2x = \overset{\circ}{7} + 6$$

logo

$$x = 7n + 3$$

onde n é um inteiro qualquer.

Observação:

Com base na equação $2x = \overset{\circ}{7} + 6$, temos, de forma equivalente, a equação $2x = 7k + 6$, com k inteiro. Para que esta última igualdade se verifique, k tem que ser par, isto é, k tem que ser da forma $2n, n \in \mathbb{Z}$. Daí:

$$2x = 7.(2n) + 6 \text{ ou } 2x = 2.(7n + 3)$$

Portanto, $x = 7n + 3$

Substituímos $x = 7n + 3$ na equação do **passo 2** e obtemos

$$y = -9n - 2$$

Na tabela abaixo, encontramos algumas soluções da equação:

n	...	-3	-2	-1	0	1	2	3	...
x=7n+3	...	-18	-11	-4	3	10	17	24	...
y=-9n-2	...	25	16	7	-2	-11	-20	-29	...

Exemplo 3.6.5. *Resolva nos inteiros a equação* $2x + 3y + 5z = 11$.

(Fonte: Feitosa (2012)

Resolução. Como $mdc(2, 3, 5) = 1$ e $1|11$, a equação tem solução. Expressando todos os coeficientes em função do múltiplo do menor deles, isto é, em função de 2, temos

$$\overset{\circ}{2}\, x + (\overset{\circ}{2} + 1)y + (\overset{\circ}{2} + 1)z = \overset{\circ}{2} + 1$$

ou

$$\overset{\circ}{2}\, x + \overset{\circ}{2}\, y + y + \overset{\circ}{2}\, z + z = \overset{\circ}{2} + 1$$

ou

$$\overset{\circ}{2} + \overset{\circ}{2} + y + \overset{\circ}{2} + z = \overset{\circ}{2} + 1$$

daí,

$$y = \overset{\circ}{2} - z + 1$$

logo,

$$y = 2n - z + 1, \quad n \in \mathbb{Z}$$

que, substituído na equação original, dá-nos $x = -3n - z + 4$. Portanto, todas as soluções são dadas por

$$(x, y, z) = (-3n - z + 4, 2n - z + 1, z), \quad n, z \in \mathbb{Z}.$$

Observação 3.6.1. *Podemos encontrar uma solução particular da equação diofantina* $ax + by = c$ *seguindo os passos:*
$i)$ *determinamos os valores de* x_1 *e* y_1 *tais que* $ax_1 + by_1 = mdc(a, b)$
$ii)$ *multiplicamos a equação anterior por um inteiro* $P \neq 0$ *tal que* $P.mdc(a, b) = c$ *e, neste caso, teremos*

$$a(x_1P) + b(y_1P) = P.mdc(a, b) = c$$

Ou seja, pela equação anterior, $x_0 = x_1P$ *e* $y_0 = y_1P$ *é uma solução paticular da equação diofantina* $ax + by = c$.

Outra resolução para a equação $2x + 3y + 5z = 11$.

Podemos transformar esse problema isolando qualquer uma das variáveis no problema que já sabemos resolver. Por exemplo, podemos resolver $2x + 3y = 11 - 5z$, supondo z fixo.

Como $mdc(2, 3) = 1$ e $1|11 - 5z$, a equação tem solução.

Assim, pela **Observação 3.6.1**, temos

$$\begin{aligned} 2.(-1) + 3.(1) &= 1, \quad \text{multiplicando por } 11 - 5z \text{ (veja que } 11 - 5z \neq 0, \forall z \in \mathbb{Z}), \\ 2.(-11 + 5z) + 3.(11 - 5z) &= 11 - 5z \end{aligned}$$

Assim, temos que $x_0 = -11 + 5z$ e $y_0 = 11 - 5z$ é uma solução particular de $2x + 3y = 11 - 5z$.

Aplicando o **Corolário 3.3.1**, temos $x = -11 + 5z + 3t$ e $y = 11 - 5z - 2t$, $t \in \mathbb{Z}$. Consequentemente, todas as soluções são dadas por

$$(x, y, z) = (-11 + 5z + 3t, 11 - 5z - 2t, z), \quad z, t \in \mathbb{Z}.$$

Observe que, se na solução $(x, y, z) = (-11 + 5z + 3t, 11 - 5z - 2t, z)$ trocarmos t por $-t - 2z + 5$, obtemos a solução $(x, y, z) = (-3t - z + 4, 2t - z + 1, z)$, que é a mesma obtida na primeira resolução.

3.6.1.1 Resolução de equações diofantinas lineares por congruências

Segundo Alencar Filho (1981, p. 175-176), de acordo com o **Teorema 3.2.1**, a equação diofantina linear

$$ax + by = c \tag{3.3}$$

tem solução se, e somente se, $d|c$, sendo $d = mdc(a, b)$. Neste caso, se o par de inteiros x_0, y_0 é uma solução particular qualquer desta equação, então:

$$ax_0 + by_0 = c \quad \text{e} \quad ax_0 - c = -by_0$$

o que implica:

$$ax_0 \equiv c\,(mod\, b) \tag{3.4}$$

Assim sendo, para obter uma solução particular da equação diofantina linear (3.3) basta determinar uma solução qualquer $x = x_0$ da congruência linear

$$ax \equiv c\,(mod\, b) \tag{3.5}$$

e substituir este valor x_0 de x na equação (3.3) a fim de encontrar o valor correspondente y_0 de y, isto é, tal que $ax_0 + by_0 = c$.

Também se pode obter uma solução particular da equação diofantina linear (3.3) determinando uma solução qualquer $y = y_0$ da congruência linear:

$$by \equiv c\,(mod\, a) \tag{3.6}$$

Para exemplificar o método, vamos resolver alguns exemplos.

Exemplo 3.6.6. *Resolva por congruência a equação diofantina linear:*

$$48x + 7y = 17.$$

(Fonte: Alencar Filho (1981, p. 176-177))

Resolução. Como o $mdc(48, 7) = 1$, a equação dada tem solução e, portanto, para obter uma solução particular desta equação cumpre determinar uma solução qualquer da congruência linear:

$$48x \equiv 17\,(mod\,7)$$

Por ser $48x \equiv -x\,(mod\,7)$, temos:

$$\begin{aligned} -x &\equiv 17 \equiv 3\,(mod\,7) \\ x &\equiv -3 \equiv 4\,(mod\,7) \end{aligned} \tag{3.7}$$

Substituindo este valor $x = 4$ na equação diofantina linear dada, temos:

$$48.4 + 7y = 17 \Longrightarrow y = -25.$$

Logo, o par de inteiros $(x_0, y_0) = (4, -25)$ é uma solução particular da equação original. Assim, pelo **Corolário 3.3.1** todas as soluções são dadas por:

$$x = 4 + 7t, \qquad y = -25 - 48t$$

onde t é um inteiro arbitrário qualquer.

Observe que, a partir de (3.7), podemos concluir que $x = 4 + 7t$, que substituído na equação $48x + 7y = 17$, dá-nos:

$$48(4 + 7t) + 7y = 17 \Longrightarrow y = -25 - 48t.$$

Exemplo 3.6.7. *Resolva por congruência a equação diofantina linear:*

$$9x + 16y = 35.$$

(Fonte: Alencar Filho (1981, p. 177))

Resolução. A equação dada tem solução, pois $mdc(9, 16) = 1$. A partir da equação dada, temos a congruência linear:

$$16y \equiv 35\,(mod\,9)$$

Por ser $16y \equiv 7y\,(mod\,9)$, temos $7y \equiv 35\,(mod\,9)$ ou $7.y \equiv 7.5\,(mod\,9)$. Como $mdc(7, 9) = 1$, podemos aplicar a lei do corte. Daí,

$$y \equiv 5\,(mod\,9) \Longrightarrow y = 5 + 9t,$$

onde t é um inteiro arbitrário. Substituindo este valor de y na equação $9x + 16y = 35$, obtemos:

$$9x + 16(5 + 9t) = 35 \Longrightarrow x = -5 - 16t.$$

Exemplo 3.6.8. *Resolva a equação*

$$3x + 4y + 5z = 6. \tag{3.8}$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 70-71))

Resolução. Trabalhando a equação módulo 5, temos $3x + 4y \equiv 1\,(mod\,5)$. Daí,

$$3x + 4y = 1 + 5s, \quad s \in \mathbb{Z}. \tag{3.9}$$

Agora, basta resolver a equação (3.9) nas incógnitas x e y.
Como $mdc(3, 4) = 1$ e $1|1 + 5s$, a equação (3.9) tem solução.
Assim, pela **Observação 3.6.1**, temos

$$\begin{aligned} 3.(-1) + 4.(1) &= 1, \quad \text{multiplicando por } 1 + 5s \text{ (veja que } 1 + 5s \neq 0, \forall s \in \mathbb{Z}), \\ 3.(-1 - 5s) + 4.(1 + 5s) &= 1 + 5s \end{aligned}$$

Assim, temos que $x_0 = -1 - 5s$ e $y_0 = 1 + 5s$ é uma solução particular de (3.9).
Aplicando o **Corolário 3.3.1**, temos $x = -1 - 5s + 4t$ e $y = 1 + 5s - 3t$, $t \in \mathbb{Z}$, que substituídos na equação (3.8), dá-nos $z = 1 - s$.
Consequentemente, todas as soluções são dadas por

$$(x, y, z) = (-1 - 5s + 4t, 1 + 5s - 3t, 1 - s), \quad s, t \in \mathbb{Z}.$$

Observação 3.6.2. *Podemos resolver a equação (3.8) sem a necessidade de aplicar congruência. Neste caso, podemos transformar esse problema isolando qualquer uma das variáveis no problema que já sabemos resolver. Por exemplo, podemos resolver $3x + 4y = 6 - 5z$, supondo z fixo. Usando a **Observação 3.6.1**, podemos encontrar a solução particular $(x_0, y_0) = (-6 + 5z, 6 - 5z)$. Assim, todas as soluções são da forma:*

$$(x, y) = (-6 + 5z + 4t, 6 - 5z - 3t),$$

ou seja, as soluções da equação original são da forma $(x, y, z) = (-6 + 5z + 4t, 6 - 5z - 3t, z)$, com t e z inteiros. Note que a solução $(x, y, z) = (-6 + 5z + 4t, 6 - 5z - 3t, z)$ é igual à solução $(x, y, z) = (-1 - 5s + 4t, 1 + 5s - 3t, 1 - s)$, trocando z por $1 - s$.

Exemplo 3.6.9. *Resolva a equação*

$$6x + 10y - 15z = 1. \tag{3.10}$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 265))

Resolução. Trabalhando a equação módulo 3, temos $y \equiv 1\,(mod\,3)$; então, $y = 1 + 3s$, $s \in \mathbb{Z}$. A equação torna-se

$$6x - 15z = -9 - 30s,$$

ou, de forma equivalente, $2x - 5z = -3 - 10s$. Passando para módulo 2, temos $z \equiv 1\,(mod\,2)$, isto é, $z = 1 + 2t,\ t \in \mathbb{Z}$ e $x = 1 - 5s + 5t$, que, substituídos na equação (3.10), dão-nos $y = 1 + 3s$. Portanto, as soluções são:

$$(x, y, z) = (1 - 5s + 5t, 1 + 3s, 1 + 2t), \qquad s, t \in \mathbb{Z}.$$

Outra resolução. Reescrevendo a equação (3.10), temos $6x + 10y = 1 + 15z$. Agora, basta resolver a equação nas incógnitas x e y.

Como $mdc(6, 10) = 2$, a equação tem solução quando $2|1 + 15z$, ou seja, quando $1 + 5z$ for par, o que ocorrerá quando z for ímpar. Assim, tomando $z = 1 + 2k, k \in \mathbb{Z}$, temos

$$6x + 10y = 1 + 15(1 + 2k),$$

ou de forma equivalente

$$3x + 5y = 8 + 15k \tag{3.11}$$

Usando a **Observação 3.6.1**, podemos encontrar a solução particular $(x_0, y_0) = (16 + 30k, -8 - 15k)$ para (3.11). Assim, todas as soluções de (3.11) são da forma:

$$(x, y) = (16 + 30k + 5w, -8 - 15k - 3w),$$

ou seja, as soluções da equação (3.10) são da forma $(x, y, z) = (16 + 30k + 5w, -8 - 15k - 3w, 1 + 2k)$, com k e w inteiros.

Note que, se na solução $(x, y, z) = (16+30k+5w, -8-15k-3w, 1+2k)$ trocarmos w por $-5k - w - 3$, obtemos a solução $(x, y, z) = (1 - 5w + 5k, 1 + 3w, 1 + 2k)$, que é a mesma solução encontrada quando aplicamos congruência.

3.6.2 Resolução da equação $ax + by = c$ usando noções de Classes Residuais

Fazendo uso das Classes Residuais, podemos resolver a equação diofantina linear $ax + by = c$ nas incógnitas x e y , com $\{a, b, c, x, y\} \subset \mathbb{Z}$ e $ab \neq 0$, conforme veremos a seguir.

Recordemos que, dados $[a], [b] \in \mathbb{Z}_m$, o elemento $[a]$ é inverso de $[b]$ se, e somente, $[a].[b] = [1]$.

Lembremos que o elemento $[a] \in \mathbb{Z}_m$ é invertível se, e somente se, o $mdc(a, m) = 1$.

Assim, por exemplo, em $\mathbb{Z}_5$, $[2]$ possui inverso, pois o $mdc(2, 5) = 1$. De fato, $[2].[3] = [1]$. Temos, ainda: $[2].[2] = [4] = -[1]$.

Para exemplificar o método, vamos resolver as equações diofantinas:

$$a) \quad 2x + 5y = 51 *$$

Observemos que $mdc(2, 5) = 1$ e $1|51$. Logo, a equação tem solução.

Escolhemos o coeficiente de uma das variáveis. De preferência, a de menor valor, isto é, 2.

Agora, determinamos a classe residual módulo 2 dos inteiros $2, 5$ e 51. Assim, em $\mathbb{Z}_2$ teremos, respectivamente, $[0], [1]$ e $[1]$. Daí, a equação * fica na forma:

$$[1]y = [1] \qquad \text{ou} \qquad y = [1]$$

Portanto, $y = 2n + 1$, que substituída em * dá-nos $x = -5n + 23$, onde n é um inteiro qualquer.

$$b) \quad 17x + 13y = 100 * *$$

Tomemos o coeficiente 13 de y (de preferência o de menor valor). Agora, determinamos a classe residual dos inteiros $17, 13$ e 100. Assim, em $\mathbb{Z}_{13}$, temos, respectivamente, $[4], [0]$ e $[9]$. Daí a equação ** fica na forma:

$$\begin{aligned} [4]x &= [9]. \quad \text{Como} \quad [3].[4] = [12] = -[1], \text{ temos :} \\ [3]\,[4]\,x &= [3]\,[9]\,, \text{ ou} \\ -[1]\,x &= [1]\,, \text{ ou} \\ x &= -[1] \end{aligned}$$

Portanto, $x = 13n - 1$, que, substituído em ** dá-nos: $y = -17n + 9$ para todo inteiro n.

Escolhendo, agora, o coeficiente 17, temos, em $\mathbb{Z}_{17}$ as classes $[0], [13]$ e $[15]$, como representante dos inteiros $17, 13$ e 100, respectivamente.

Assim, ** fica na forma:

$$\begin{aligned} [13]y &= [15]. \quad \text{Como} \quad [13] = -[4] \text{ e } [15] = -[2], \text{ temos} \\ -[4]\,y &= -[2]\,, \text{ ou} \\ -[2]\,[2]\,y &= -[2]\,, \text{ aplicando a lei do corte (lembrando que } mdc(2, 17) = 1), \text{ temos} \\ [2]\,y &= [1]\,, \text{ como } [9]\,[2] = [1]\,, \text{ temos} \\ [9]\,[2]\,y &= [9]\,[1]\,, \text{ ou} \\ y &= [9] \end{aligned}$$

Portanto, $y = 17n + 9$, que, substituído em **, dá-nos $x = -13n - 1$, sendo n um inteiro qualquer.

Observe que a solução $x = -13n - 1$ e $y = 17n + 9$ é a mesma encontrada anteriormente, trocando-se n por $-n$. Veja:

$$x = -13(-n) - 1 \quad \text{e} \quad y = 17(-n) + 9$$

ou seja,

$$x = 13n - 1 \quad \text{e} \quad y = -17n + 9$$

3.6.3 Casos práticos

Existem algumas equações diofantinas lineares de duas variáveis que, em determinadas condições, podemos reduzir os passos na resolução.

Estudaremos três casos a saber: Critério do algarismo final, Critério da multiplicidade e Critério do agrupamento.

3.6.3.1 Critério do Algarismo Final

Pode-se trabalhar com o último algarismo para encontrar uma solução particular da equação diofantina linear $ax + by = c$ sempre que um dos coeficientes for múltiplo de 5, uma vez que, deste modo, podemos assegurar que tal coeficiente terá como algarismo final 0 ou 5.

Exemplo 3.6.10. *Resolva a equação diofantina*

$$5x + 49y = 37.$$

(Fonte: Vera (2014, p. 16-17))

Resolução. Como $mdc(5, 49) = 1$ e $1|37$, a equação tem solução.

Observamos que o coeficiente de x é múltiplo de 5. Portanto, temos duas opções para o último algarismo de $5x$: 0 ou 5.

Suponhamos que $5x = ...0$.

Então, para que se cumpra a equação, deve ocorrer que

$49y = ...7$.

Para isso, devemos ter $y = 3$ ou deve terminar em 3; então, substituindo na equação original, temos $x = -22$. Assim, $x_0 = -22$ e $y_0 = 3$ é uma solução particular da equação.

Sabendo-se que o $mdc(5, 49) = 1$, temos que o conjunto solução é dado por:

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 - at \end{aligned} \qquad \text{ou seja,} \qquad \begin{aligned} x &= -22 + 49t \\ y &= 3 - 5t \end{aligned}$$

onde t é um inteiro qualquer.

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão 49)	x=-22+49t	...	-22	27	76	125	174	223	...
y (razão -5)	y=3-5t	...	3	-2	-7	-12	-17	-22	...

Agora, supondo que $5x$ termine em 5, isto é,

$5x = ...5$

Então, para que se cumpra a equação, devemos ter

$49y = ...2$

Para isso, $y = 8$ ou deve terminar em 8. Substituindo na equação original, temos $x = -71$. Assim, $x_0 = -71$ e $y_0 = 8$ é uma solução particular da equação dada. Neste caso, o conjunto solução é dado por:

$$\begin{aligned} x &= -71 + 49t \\ y &= 8 - 5t \end{aligned}$$

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão 49)	x=-71+49t	...	-71	-22	27	76	125	174	...
y (razão -5)	y=8-5t	...	8	3	-2	-7	-12	-17	...

Ou seja, analisando as duas tabelas, observamos que temos o mesmo resultado.

Exemplo 3.6.11. *Resolva a seguinte equação diofantina*

$$13x - 25y = 54.$$

(Fonte: Vera (2014, p. 17))

Resolução. Observe que $mdc(13, 25) = 1$ e $1|54$. Logo, a equação tem solução. Observamos que o coeficiente de y é múltiplo de 5; então, para o último algarismo de $25y$ temos duas opções: 0 ou 5.

Suponhamos que

$25y = ...0$

Para que se cumpra a igualdade anterior, deve ocorrer que

$13x = ...4$

Para isso, $x = 8$, ou deve terminar em 8. Substituindo na equação original, temos $y = 2$. Portanto, $x_0 = 8$ e $y_0 = 2$ é uma solução particular. Assim, o conjunto solução será obtido conforme descrevemos abaixo.

Sejam:

$13x - 25y = 54$ *

$13(8) - 25(2) = 54$**

Subtraindo ordenadamente * e **, temos:

$13(x-8) - 25(y-2) = 0 \quad \text{ou} \quad 13(x-8) = 25(y-2) \quad \text{ou} \quad \dfrac{x-8}{25} = \dfrac{y-2}{13} = t, \quad t \in \mathbb{Z}$

Daí, todas as soluções são dadas por $x = 8 + 25t$ e $y = 2 + 13t$, $t \in \mathbb{Z}$.

Agora, supondo que $25y$ termine em 5, isto é, $25y = ...5$, teremos, então, para que se cumpra a equação, que $13x = ...3$, ou deve terminar em 3. Substituindo na equação original, temos $25y = -15$, que nos dá um valor não inteiro para y. Se testarmos $x = 13$, $x = 23$, $x = 33$ ou algum outro valor terminado em 3, seguramente iremos encontrar um valor adequado; porém, devemos sempre considerar o caso mais simples. Para este caso, temos $x = 33$, que substituído na equação original nos dá $y = 15$. Portanto, todas as soluções são dadas por:

$$x = 33 + 25t \quad \text{e} \quad y = 15 + 13t, \quad \text{com} \quad t \in \mathbb{Z}$$

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão 25)	x=33+25t	...	33	58	83	108	133	158	...
y (razão 15)	y=15+15t	...	15	28	41	54	67	80	...

3.6.3.2 Critério da Multiplicidade

Podemos encontrar uma solução particular rapidamente quando o termo independente da equação for múltiplo de um dos coeficientes.

Para este caso prático, devemos ter em mente que se $A + B = C$ e, além disso, A e C são múltiplos de n, então, necessariamente, B deve ser múltiplo de n, onde todas as variáveis são inteiras.

Exemplo 3.6.12. *Resolva a seguinte equação diofantina*

$$4x + 7y = 20$$

(Fonte: Vera (2014, p. 18))

Resolução. Como $mdc(4, 7) = 1$ e $1|20$, a equação tem solução.

Observemos que o termo independente, isto é, 20, é múltiplo de 4.

Como

$4x$ é múltiplo de 4

20 é múltiplo de 4

Então,

$7y$ deve ser múltiplo de 4

Portanto, $y = 4$ ou outro múltiplo de 4, inclusive o 0.

Assim, se $y = 4$, então, substituindo na equação inicial, temos $x = -2$. Assim, o

conjunto solução será obtido conforme descrevemos abaixo.

Sejam:

$4x + 7y = 20$ *

$4(-2) + 7(4) = 20$**

Subtraindo ordenadamente * e **, temos:

$$4(x+2)+7(y-4) = 0 \quad \text{ou} \quad 4(x+2) = -7(y-4) \quad \text{ou} \quad \frac{x+2}{-7} = \frac{y-4}{4} = t, \quad \text{com} \quad t \in \mathbb{Z}$$

Daí, todas as soluções são dadas por $x = -2 - 7t$ e $y = 4 + 4t$, com $t \in \mathbb{Z}$.

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão -7)	x=-2-7t	...	-2	-9	-16	-23	-30	-37	...
y (razão 4)	y=4+4t	...	4	8	12	16	20	24	...

Outra resolução para a equação $4x + 7y = 20$.

Como $4x$ e 20 são múltiplos de 4, então, para que a igualdade se verifque, $7y$ também deve ser múltiplo de 4, o que ocorre quando $y = 4t$, com $t \in \mathbb{Z}$, que substituído na equação $4x + 7y = 20$, dá-nos:

$$4x + 7.4t = 20$$

ou seja,

$$x = 5 - 7t.$$

Portanto, as soluções são dadas por $x = 5 - 7t$ e $y = 4t$, com $t \in \mathbb{Z}$.

Observe que, se na primeira solução $(x, y) = (-2 - 7t, 4 + 4t)$ trocarmos t por $t - 1$, obtemos a solução $(x, y) = (5 - 7t, 4t)$.

No exemplo seguinte, apresentaremos uma pequena variação do método da multiplicidade, que leva em conta a paridade dos termos envolvidos.

Exemplo 3.6.13. *Determine todas as soluções inteiras da equação* $2x + 3y = 5$.

(Fonte: Feitosa (2012))

Observe, inicialmente, que a soma de um inteiro par com um ímpar resulta num ímpar. Como 5 é a soma de $2x$ com $3y$ e 5 ímpar e $2x$ é par, segue que $3y$ deve ser ímpar, o que ocorre quando y é ímpar, ou seja, quando $y = 2k + 1$ para algum inteiro k. Daí,

$$2x + 3.(2k + 1) = 5$$

ou

$$x = 1 - 3k,$$

e, consequentemente, todas as soluções da equação são da forma $(x, y) = (1-3k, 2k+1)$, $k \in \mathbb{Z}$.

3.6.3.3 Critério do Agrupamento

Neste caso prático, buscamos reagrupar os termos de tal modo que a equação possa reduzir-se a algum dos casos anteriores.

Exemplo 3.6.14. *Resolva a seguinte equação diofantina*

$$8x + 3y = 47.$$

(Fonte: Vera (2014, p. 19))

Resolução. Como $mdc(8, 3) = 1$ e $1|47$, então a equação tem solução.

Decompondo $8x$ em $5x + 3x$ com a finalidade de reagrupá-lo, temos

$5x + 3x + 3y = 47$

Colocando-se 3 em evidência, temos

$5x + 3(x + y) = 47$ *

Observe, agora, que a equação tem a forma do primeiro caso prático: **critério do algarismo final**. Então, $5x$ deve terminar em 0 ou 5.

Suponhamos que

$5x = ...0$

Para que esta igualdade se cumpra, devemos ter, necessariamente,

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

Para isto $(x + y) = 9$ ou deve terminar em 9. Então, substituindo na equação *, temos $x = 4$

Como $x + y = 9$ e $x = 4$, então $y = 5$. Assim, $x_0 = 4$ e $y_0 = 5$ é uma solução particular da equação.

Sabendo-se que o $mdc(8, 13) = 1$, temos que o conjunto solução é dado por:

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 - at \end{aligned} \qquad \text{ou seja,} \qquad \begin{aligned} x &= 4 + 3t \\ y &= 5 - 8t \end{aligned}$$

onde t é um inteiro qualquer.

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão 3)	x=4+3t	...	4	7	10	13	16	19	...
y (razão -8)	y=5-8t	...	3	-3	-11	-19	-27	-35	...

Exemplo 3.6.15. *Resolva a seguinte equação diofantina*

$$6x - 13y = 49.$$

(Fonte: Vera (2014, p. 19-20))

Resolução. Decompondo $13y$ em $6y + 7y$ com a finalidade de reagrupá-lo, temos

$6x - (6y + 7y) = 49$

Reagrupando, temos,

$(6x - 6y) - 7y = 49$

Colocando 6 em evidência, temos

$6(x - y) - 7y = 49$ **

Agora, a equação tem a forma do segundo caso prático: **Critério da multiplicidade**, pois 49 é múltiplo de 7.

Como

$7y$ é múltiplo de 7

49 é múltiplo de 7

Então, $7(x - y)$ deve ser múltiplo de 7.

Portanto, $(x - y) = 7$ ou algum outro múltiplo de 7, inclusive o 0.

Logo, se $(x - y) = 7$, então, substituindo na equação **, temos $y = -1$

Como $x - y = 7$ e $y = -1$, então, $x = 6$. Assim, $x_0 = 6$ e $y_0 = -1$ é uma solução particular da equação.

Sabendo-se que o $mdc(6, 13) = 1$, temos que o conjunto solução é dado por:

$$\begin{aligned} x &= x_0 + bt \\ y &= y_0 - at \end{aligned} \qquad \text{ou seja,} \qquad \begin{aligned} x &= 6 - 13t \\ y &= -1 - 6t \end{aligned}$$

onde t é um inteiro qualquer.

Na tabela seguinte, encontramos algumas soluções da equação:

	t	...	0	1	2	3	4	5	...
x(razão -13)	x=6-13t	...	6	-7	-20	-32	-45	-58	...
y (razão -6)	y=-1-6t	...	-1	-7	-13	-19	-25	-31	...

Exemplo 3.6.16. *Resolva a seguinte equação diofantina*

$$2x + 14xy + 7 = 54.$$

(Fonte: Vera (2014, p. 20))

Resolução. Das duas primeiras parcelas da equação, colocamos $2x$ em evidência. Daí

$$2x(1 + 7y) + 7y = 54$$

Somando-se 1 aos dois membros da equação anterior, temos

$$2x(7y + 1) + (7y + 1) = 54 + 1$$

Colocando $(7y + 1)$ em evidência, temos

$$(7y + 1)(2x + 1) = 55$$

Como as variáveis só podem assumir valores inteiros, então, para que esta última igualdade se verifique, devemos ter somente os quatro casos abaixo:

Casos	1	2	3	4
$2x + 1$	1	5	11	55
$7y + 1$	55	11	5	1

Logo, os valores de x e y são os seguintes:

Casos	1	2	3	4
x	0	2	5	27
y	não é inteiro	não é inteiro	não é inteiro	0

Portanto, a equação tem somente a solução $x = 27$ e $y = 0$.

4 EQUAÇÕES DIOFANTINAS NÃO LINEARES

Neste capítulo, abordaremos as triplas pitagóricas, os triângulos pitagóricos e o método geométrico, o descenso infinito de Fermat (ou descida de Fermat) e as equações de Pell. Também veremos os métodos da fatoração e o método aritmético modular. Utilizaremos, ainda, inequações para resolver equações diofantinas.

4.1 Ternas Pitagóricas

Martínez et al. (2013) denominam *triplas* ou *ternas pitagóricas* as triplas de números inteiros positivos (a, b, c) que satisfazem a equação

$$a^2 + b^2 = c^2, \tag{4.1}$$

uma vez que correspondem aos comprimentos dos lados de um triângulo retângulo de lados inteiros pelo Teorema de Pitágoras.

Uma tripla pitagórica cujos termos são primos relativos aos pares é denominada *tripla pitagórica primitiva* (MARTíNEZ et al., 2013).

Nosso objetivo, agora, é encontrar as triplas pitagóricas (a, b, c).

Para tanto, podemos supor que a, b e c são coprimos dois a dois, pois, por exemplo, se houver um primo p tal que p divida $mdc(a, b)$, então p divide $a^2 + b^2 = c^2$, o que implica que p divide c; logo, $\left(\frac{a}{p}, \frac{b}{p}, \frac{c}{p}\right)$ também é tripla pitagórica.

Feitas as considerações iniciais, a e b não podem ser pares ao mesmo tempo; portanto, podemos supor, sem perda de generalidade, que a é ímpar. Além disso, como $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1\,(mod\,4)$ e $(2k)^2 \equiv 0\,(mod\,4)$, ou seja, quadrados perfeitos são congruentes ou a 0 ou a 1 módulo 4. Portanto, b não pode ser ímpar, pois, caso contrário, $c^2 \equiv a^2 + b^2 \equiv 2\,(mod\,4)$, o que é um absurdo. Resumindo, temos que a é ímpar, b é par e, então, c é ímpar. Por outro lado,

$$b^2 = c^2 - a^2 = (c - a)(c + a). \tag{4.2}$$

Seja $d = mdc(c - a, c + a)$, então d divide

$$(c + a) + (c - a) = 2c \text{ e } (c + a) - (c - a) = 2a$$

e, daí, $d|mdc(2a, 2c) = 2mdc(a, c) = 2$, pois $mdc(a, c) = 1$. Mas, como $c - a$ e $c + a$ são ambos pares (pois a e c são ambos ímpares), segue que $d = 2$ e, pelo **Corolário 2.7.1**, $mdc\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$. Podemos, então, escrever (4.2) como

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right)$$

Como $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são coprimos e seu produto é um quadrado perfeito, temos, pelo Teorema Fundamental da Aritmética, que cada um destes fatores deve ser o quadrado de um número natural. Assim,

$$\frac{c+a}{2} = m^2, \quad \frac{c-a}{2} = n^2, \quad b = 2mn,$$

com $mdc(m,n) = 1$. Escrevendo a, b, c em termos de m e n, obtemos, portanto,

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

com $m > n$.

Ademais, como $c = m^2 + n^2$ é ímpar, m e n têm paridades distintas.

Todas as triplas pitagóricas se encontram a partir de uma tripla pitagórica primitiva multiplicando por uma constante.

Dentre as triplas pitagóricas primitivas, Moreira, Martínez e Saldanha (2012) destacam as *triplas pitagóricas clássicas de primeiro tipo*, que são aquelas em que um dos catetos e a hipotenusa são inteiros consecutivos, ou seja, as triplas da forma $(a, b, b+1)$, que foram estudadas por Pitágoras. Para encontrarmos uma fórmula que gere *triplas pitagóricas clássicas de primeiro tipo* é suficiente observar que

$$a^2 = (b+1)^2 - b^2 = 2b + 1$$

logo, a é um número ímpar; portanto, $a = 2k + 1$ com k natural que, substituído na equação anterior, dá-nos:

$$4k^2 + 4k + 1 = 2b + 1 \text{ ou seja, } b = 2k^2 + 2k \text{ e } c = 2k^2 + 2k + 1$$

e, assim, obtemos a família de triplas pitagóricas $(2k+1, 2k^2+2k, 2k^2+2k+1)$.

Moreira, Martínez e Saldanha (2012) destacam, ainda, as *triplas pitagóricas clássicas de segundo tipo*, que são aquelas em que a diferença entre a hipotenusa e um cateto é igual 2, ou seja, as triplas da forma $(a, b, b+2)$, que foram estudadas por Platão. Para encontrarmos uma fórmula que gere *triplas pitagóricas clássicas de segundo tipo*, seguiremos o argumento anterior, ou seja

$$a^2 = (b+2)^2 - b^2 = 4b + 4 = 2(2b+2)$$

assim, a é par, isto é $a = 2s$, que substituído na equação anterior nos dá $s^2 = b + 1$. Mas b não pode ser par, pois estamos interessados somente nas triplas pitagóricas primitivas, de sorte que s não pode ser ímpar. Logo, $s = 2k$ com k inteiro e, neste caso, a família de triplas pitagóricas é dada por

$$(4k, 4k^2 - 1, 4k^2 + 1).$$

Fazem observar Moreira, Martínez e Saldanha (2012) que as triplas pitagóricas encontradas por Pitágoras correspondem ao caso em que $m = k + 1$ e $n = k$, e as triplas encontradas por Platão se reduzem ao caso em que $m = 2k$ e $n = 1$.

Exemplo 4.1.1. *Encontre todas as triplas de números (a, b, c) tais que a^2, b^2 e c^2 estão em progressão aritmética.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 186-187))

Resolução. Numa progressão aritmética, a diferença de dois termos consecutivos é constante; assim, o problema se reduz a encontrar todas as triplas de números (a, b, c) tais que

$$b^2 - a^2 = c^2 - b^2,$$

isto é, $a^2 + c^2 = 2b^2$, donde se conclui que a e c têm a mesma paridade, pois, caso contrário, $a^2 + c^2$ seria ímpar. Assim, tomando $r = \dfrac{c+a}{2}$ e $s = \dfrac{c-a}{2}$, temos $c = r + s$ e $a = r - s$. Deste modo, substituindo, teremos que

$$2b^2 = a^2 + c^2 = (r - s)^2 + (r + s)^2 = 2(r^2 + s^2)$$

ou

$$b^2 = r^2 + s^2$$

donde (r, s, b) é uma tripla pitagórica. Portanto, existem inteiros m e n tais que $r = m^2 - n^2$, $s = 2mn$ e $b = m^2 + n^2$, e se conclui que

$$a = |m^2 - n^2 - 2mn|, \quad b = m^2 + n^2, \quad c = m^2 - n^2 + 2mn,$$

com $m > n$ e $m + n$ ímpar, é uma tripla que satisfaz o pedido. Além disso, todas as triplas primitivas são desta forma.

Teorema 4.1.1. *Todas as soluções para a equação*

$$x^2 + y^2 + z^2 = t^2 \tag{4.3}$$

em inteiros positivos x, y, z, t, com y, z pares são dadas por

$$x = \frac{l^2 + m^2 - n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2 + m^2 + n^2}{n} \tag{4.4}$$

onde l, m são inteiros positivos arbitrários e n é qualquer divisor de $l^2 + m^2$ menor que $\sqrt{l^2 + m^2}$. Toda solução é obtida exatamente deste modo.

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 79-80))

Demonstração. A identidade

$$\left(\frac{l^2+m^2-n^2}{n}\right)^2+(2l)^2+(2m)^2=\left(\frac{l^2+m^2+n^2}{n}\right)^2$$

mostra que a quádrupla dada em (4.4) é uma solução para a equação (4.3), donde y e z são pares. Por outro lado, note que pelo menos dois dos números inteiros x, y, z devem ser par; caso contrário, $t^2 \equiv 2, 3\,(mod\,4)$, o que é uma contradição. Suponha que $y = 2l$, $z = 2m$ para alguns inteiros positivos l e m. Tomando $t - x = u$, obtemos

$$x^2+4l^2+4m^2=(x+u)^2 \quad \text{ou} \quad u^2=4(l^2+m^2)-2ux.$$

Portanto, u^2 é par, então $u = 2n$ para algum inteiro positivo n. Segue-se que $x=\dfrac{l^2+m^2-n^2}{n}$ e $t=x+u=x+2n=\dfrac{l^2+m^2+n^2}{n}$, onde l, m, n são inteiros positivos e n é divisor de $l^2 + m^2$ menor que $\sqrt{l^2+m^2}$.

Não é difícil perceber que cada solução (x, y, z, t) de (4.3) com y e z pares é obtida exatamente uma vez a partir das fórmulas dadas em (4.4). Na verdade, por (4.4), temos $l=\dfrac{y}{2}, m=\dfrac{z}{2}, n=\dfrac{t-z}{2}$; daí, os inteiros l, m, n são unicamente determinados por (x, y, z, t). □

Observação 4.1.1. *Uma forma bem conhecida para gerar "quádruplas pitagóricas" é:*

$$x=l^2+m^2-n^2, \quad y=2lm, \quad z=2mn, \quad t=l^2+m^2+n^2,$$

onde l, m, n são inteiros positivos . Sabe-se também que nem todas quádruplas são geradas desta forma; por exemplo, $(3, 36, 8, 37)$ é excluída. Por outro lado , esta família de soluções é bastante semelhante à família de soluções para (4.1).

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 81))

Observação 4.1.2. *As seguintes fórmulas geram todas as "quádruplas pitagóricas" de inteiros:*

$$\begin{aligned} x &= m^2+n^2-p^2-q^2, \\ y &= 2(mp+nq), \\ z &= 2(np-mq), \\ t &= m^2+n^2+p^2+q^2, \end{aligned}$$

em que m, n, p, q são inteiros arbitrários.

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 81))

Nota: Se a quádrupla (x, y, z, t) de inteiros satisfaz (4.3), então todas as quádruplas (dx, dy, dz, dt), $d \in \mathbb{Z}$ também satisfazem.

Para uma prova das fórmulas apresentadas na **Observação 4.1.2** são utilizados recursos de inteiros Gaussianos, que não são objeto de estudo desta pesquisa.

Observação 4.1.3. *A equação*

$$x_1^2 + x_2^2 + ... + x_k^2 = x_{k+1}^2 \tag{4.5}$$

é a extensão natural para (4.1) *e* (4.3)*. Do ponto de vista geométrico, as soluções* $(x_1, x_2, ..., x_k, x_{k+1})$ *representam as dimensões* $x_1, x_2, ..., x_k$ *de um cuboide em* $\mathbb{R}^k$ *e o comprimento* x_{k+1} *da sua diagonal, respectivamente. Todas as soluções de inteiros positivos* $(x_1, x_2, ..., x_k, x_{k+1})$ *com* $mdc(x_1, x_2, ..., x_k) = 1$ *para a equação* (4.5) *são dadas por*

$$\begin{aligned}
x_1 &= \frac{1}{q}\left(m_1^2 + m_2^2 + ... + m_{k-1}^2 - m_k^2\right), \\
x_2 &= \frac{2}{q} m_1 m_k, \\
&\vdots \\
x_k &= \frac{2}{q} m_{k-1} m_k, \\
x_{k+1} &= \frac{1}{q}\left(m_1^2 + m_2^2 + ... + m_{k-1}^2 + m_k^2\right).
\end{aligned}$$

onde $m_1, m_2, ..., m_k$ *são inteiros arbitrários e* $q > 0$ *é tomado tal que* $mdc(x_1, x_2, ..., x_k) = 1$.

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 81-82))

Observação 4.1.4. *Para* $k = 5$*, argumentos que envolvem Espinores*[1] *em Física geram as "sêxtuplas pitagóricas":*

$$\begin{aligned}
x_1 &= m^2 - n^2, \\
x_2 &= 2(n_0 m_1 - n_1 m_0 + m_3 n_2 - m_2 n_3), \\
x_3 &= 2(n_0 m_2 - n_2 m_0 + m_1 n_3 - m_3 n_1), \\
x_4 &= 2(n_0 m_3 - n_3 m_0 + m_2 n_1 - m_1 n_2), \\
x_5 &= 2mn, \\
x_6 &= m^2 + n^2,
\end{aligned}$$

onde $m, n, m_0, m_1, m_2, m_3, n_0, n_1, n_2, n_3$ *são inteiros tais que*

$$mn = m_0 n_0 + m_1 n_1 + m_2 n_2 + m_3 n_3.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 82))

[1] Espinores são certos objetos matemáticos introduzidos para expandir a noção de espaço vetorial. Eles são necessários porque a estrutura completa de rotações num dado número de dimensões exige algum número extra de dimensões para exibi-la. Do ponto de vista formal, espinores são objetos geométricos construídos a partir de um dado espaço vetorial por meio de um procedimento de quantização ou através de um procedimento algébrico. Com isso, podemos dizer que espinores formam uma representação projetiva do grupo de rotações. Fonte: <http://www2.dbd.puc-rio.br/pergamum/tesesabertas/0610633_08_cap_03.pdf>. Data do acesso: 25/06/2016.

Exemplo 4.1.2 (Equação pitagórica “negativa"). *Resolva em inteiros positivos a equação*

$$x^{-2} + y^{-2} = z^{-2}. \tag{4.6}$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 82-83))

Resolução. A equação é equivalente a

$$x^2 + y^2 = \left(\frac{xy}{z}\right)^2$$

Isto significa que $z|xy$ e que $x^2 + y^2$ é um quadrado perfeito. Tomando

$$t = \frac{xy}{z} \tag{4.7}$$

temos a equação $x^2 + y^2 = t^2$ para algum inteiro positivo t.

Seja $d = mdc(x, y, t)$. Então, $x = ad$, $y = bd$, $t = cd$, onde $a, b, c \in \mathbb{Z}_+$, com $mdc(a, b, c) = 1$, e a equação (4.7) reduz-se a

$$z = \frac{abd}{c}. \tag{4.8}$$

A partir da escolha de t, decorre que

$$a^2 + b^2 = c^2; \tag{4.9}$$

portanto, a, b, c são primos relativos dois a dois. Em seguida, usando (4.6) deduz-se que $c|d$, isto é, $d = kc$, $k \in \mathbb{Z}_+$. Obtemos

$$x = ad = kac, \quad y = bd = kbc, \quad t = cd = kc^2, \quad z = kab.$$

Tendo em conta (4.9), temos como solução

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

Portanto, as soluções em inteiros positivos para a equação (4.6) são dadas por

$$x = k\left(m^4 - n^4\right), \quad y = 2kmn\left(m^2 + n^2\right), \quad z = 2kmn(m^2 - n^2).$$

onde $k, m, n \in \mathbb{Z}_+$ e $m > n$.

Exemplo 4.1.3. *Encontrar todas as quádruplas* (x, y, z, w) *tal que*

$$x^2 + y^2 + z^2 + xy + yz + zx = 2w^2.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 86-87))

Resolução. Escrevendo a equação como

$$(x+y)^2+(y+z)^2+(z+x)^2=(2w)^2$$

Do **Teorema 4.1.1**, temos

$$\begin{aligned} x+y &= \frac{l^2+m^2-n^2}{n}, \\ y+z &= 2l, \\ z+x &= 2m, \\ 2w &= \frac{l^2+m^2+n^2}{n}, \end{aligned}$$

onde $n|l^2+m^2$. Segue-se que todos as quádruplas procuradas são dadas por

$$\begin{aligned} x &= m-l+\frac{l^2+m^2-n^2}{2n}, \\ y &= l-m+\frac{l^2+m^2-n^2}{2n}, \\ z &= l+m-\frac{l^2+m^2-n^2}{2n}, \\ w &= \frac{l^2+m^2+n^2}{2n}, \end{aligned}$$

onde os números inteiros positivos l, m, n são escolhidos de tal modo que x, y, z sejam todos positivos e $2n|l^2+m^2+n^2$.

4.2 Triângulos Pitagóricos e o Método Geométrico

Usando argumentos de geometria analítica, inspirados nas ideias de Moreira, Martínez e Saldanha (2012, p. 190-197), mostraremos como encontrar a forma geral das triplas pitagóricas. Assim como apresentaremos algumas aplicações do método na resolução de problemas relacionados com a geometria euclidiana plana, mormente problemas relacionados com triângulos com lados inteiros, que obedeçam a certas condições específicas.

Assim, observando que a equação $a^2+b^2=c^2$ é equivalente à $\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$, ou seja, o ponto $\left(\frac{a}{c},\frac{b}{c}\right)$ é um ponto com coordenadas racionais da circunferência *C* com centro na origem e raio 1.

De forma equivalente, $\left(\frac{a}{c},\frac{b}{c}\right)$ é uma solução da equação $x^2+y^2=1$ com coordenadas que são números racionais.

Notemos que os pontos $(1,0),(-1,0),(0,1),(0,-1)$ pertencem à circunferência.

Consideremos, agora, uma reta $\mathfrak{L}$ que passa pelo ponto $(0,-1)$ e tem inclinação racional $\frac{m}{n}$. Portanto, a equação da reta é dada por $y=\frac{m}{n}x-1$.

Observemos que o ponto $(0,-1)$ é comum à reta e à circunferência. Para

encontrarmos um outro ponto comum, devemos resolver o sistema de equações

$$\begin{cases} x^2 + y^2 = 1 \\ y = \frac{m}{n}x - 1 \end{cases}$$

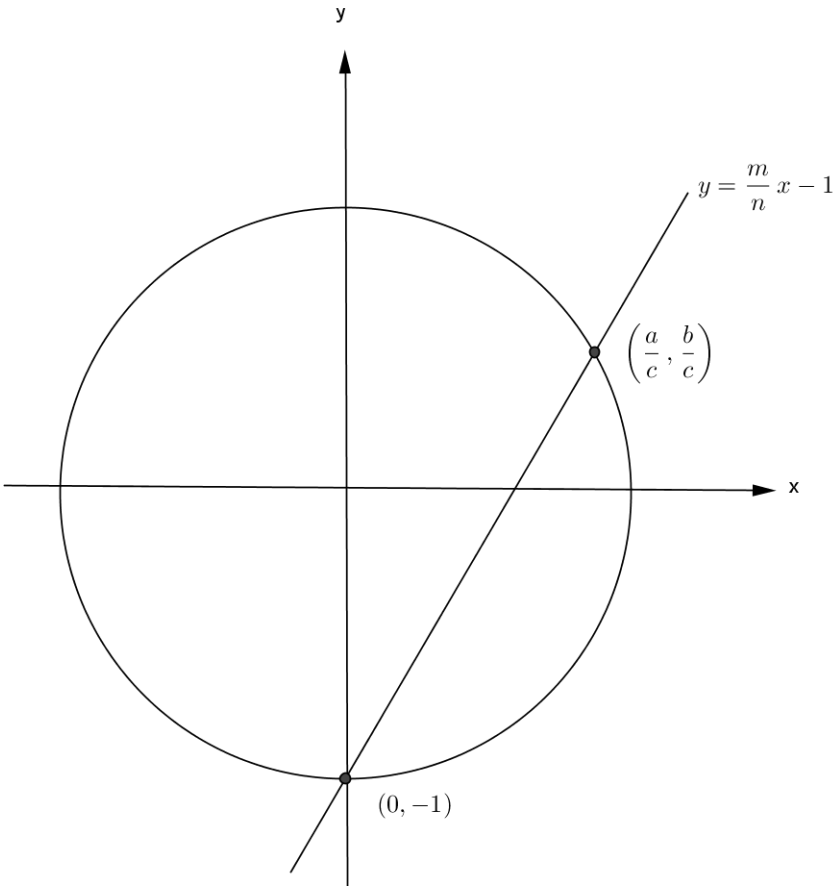

Figura 2 – Interseção entre a circunferência *C* e a reta $\mathfrak{L}$.
Fonte: Moreira, Martínez e Saldanha (2012, p. 190).

Assim, substituindo $y = \frac{m}{n}x - 1$ na equação da circunferência, temos a equação:

$$1 = x^2 + \left(\frac{m}{n}x - 1\right)^2 = x^2 + \frac{m^2}{n^2}x^2 - 2\frac{m}{n}x + 1.$$

Cujas soluções são $x = 0$ e $x = \dfrac{2mn}{m^2 + n^2}$. Portanto,

$$x = \frac{a}{c} = \frac{2mn}{m^2 + n^2} \quad \text{e} \quad y = \frac{b}{c} = \frac{m}{n}\frac{2mn}{m^2 + n^2} - 1 = \frac{m^2 - n^2}{m^2 + n^2}$$

Agora, como as frações que aparecem em cada igualdade são iguais, supondo que $mdc(m, n) = 1$, segue-se que, no caso em que $m + n$ é ímpar, existe um inteiro k tal que

$$a = 2mnk, \quad b = (m^2 - n^2)k, \quad c = (m^2 + n^2)k.$$

E, no caso em que $m+n$ é par, existe um inteiro k tal que

$$a = mnk, \quad b = \frac{(m^2-n^2)}{2}k \quad \text{e} \quad c = \frac{(m^2+n^2)}{2}k.$$

Exemplo 4.2.1. *Determine todas as soluções da equação* $a^2 + 2b^2 = 11c^2$.

(Fonte: Moreira, Martínez e Saldanha (2012, p. 191-192))

Resolução. Dividindo por c^2 obtemos $\left(\frac{a}{c}\right)^2 + 2\left(\frac{b}{c}\right)^2 = 11$; assim, queremos encontrar as soluções racionais da equação $x^2 + 2y^2 = 11$, que é uma elipse centrada na origem do plano cartesiano. Por inspeção direta, temos que os pares ordenados $(3,1), (-3,-1), (3,-1), (-3,1)$ são soluções. A equação da reta que passa pelo ponto $(-3,-1)$ e tem inclinação $\frac{m}{n}$ é $y = \frac{m}{n}(x+3) - 1 = \frac{m}{n}x + \frac{3m-n}{n}$

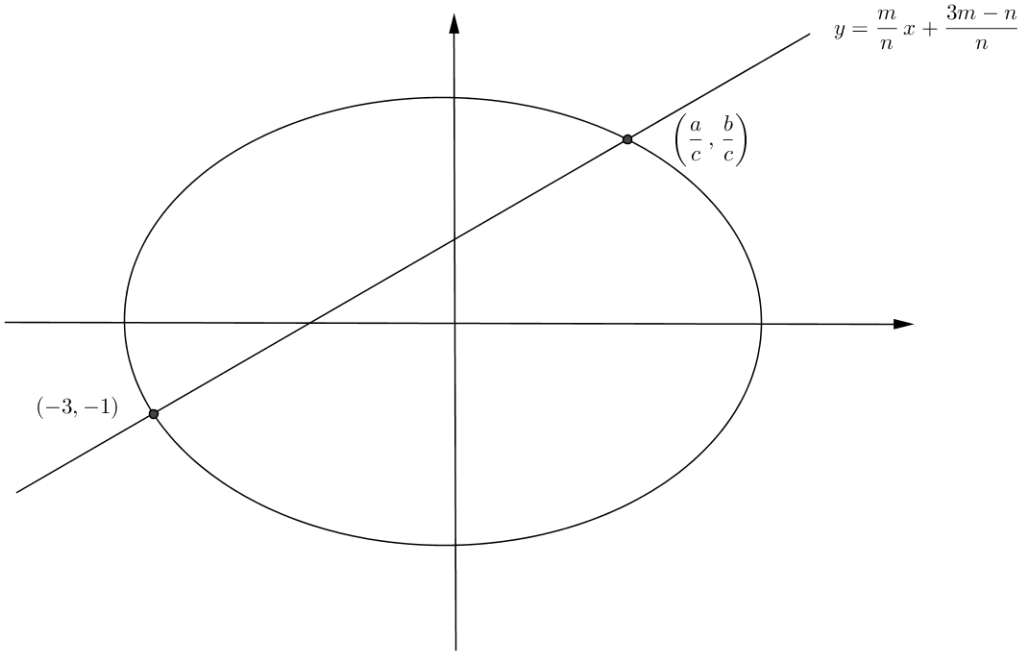

Figura 3 – Interseção entre reta elipse.
Fonte: Moreira, Martínez e Saldanha (2012, p. 191).

Os pontos de interseção da reta com a elipse são as soluções obtidas quando resolvemos o sistema de equações

$$\begin{cases} x^2 + 2y^2 = 11 \\ y = \frac{m}{n}x + \frac{3m-n}{n} \end{cases}$$

agora, substituindo y na equação da elipse, obtemos que

$$\begin{aligned} 11 &= x^2 + 2\left(\frac{m}{n}x + \frac{3m-n}{n}\right)^2 \\ &= \frac{n^2+2m^2}{n^2}x^2 + 4\frac{m(3m-n)}{n^2}x + 2\frac{9m^2-6mn+n^2}{n^2}, \end{aligned}$$

assim, x é solução da equação quadrática

$$x^2 + 4\frac{m(3m-n)}{n^2+2m^2}x - 3\frac{3n^2+4mn-6m^2}{n^2+2m^2} = 0.$$

Como $(-3,-1)$ é um ponto comum à reta e à elipse, segue-se que $x=-3$ é uma solução desta equação. Agora, usando o fato que o coeficiente independente de uma equação quadrática é o produto das raízes, temos que a outra raiz é

$$\frac{a}{c} = x = \frac{3n^2+4mn-6m^2}{n^2+2m^2}$$

e assim

$$\frac{b}{c} = y = \frac{m}{n}\left(\frac{3n^2+4mn-6m^2}{n^2+2m^2}\right) + \frac{3m-n}{n} = \frac{2m^2+6mn-n^2}{n^2+2m^2}.$$

Como as frações que aparecem em cada igualdade são iguais, então existirá um inteiro k tal que

$$a = \frac{k}{d}(3n^2+4mn-6m^2), \quad b = \frac{k}{d}(2m^2+6mn-n^2) \quad \text{e} \quad c = \frac{k}{d}(n^2+2m^2)$$

(onde $d = mdc(3n^2+4mn-6m^2, 2m^2+6mn-n^2, n^2+2m^2)$, que pertence a $\{1,2,11\}$, caso $mdc(m,n)=1$), e usando a simetria da elipse, podemos considerar os valores positivos de a,b e c. A tabela seguinte ilustra algumas soluções a partir das equações anteriores supondo $k=1$

Tabela 1 – Algumas soluções para a equação $a^2+2b^2=11c^2$

m	n	(a,b,c)
1	-1	$(7,5,3)$
0	1	$(3,1,1)$
1	1	$(1,7,3)$
2	1	$(13,19,9)$
3	1	$(39,37,19)$
4	1	$(77,55,33)$
4	3	$(21,95,25)$

Fonte: Moreira, Martínez e Saldanha (2012).

Agora, iremos determinar todos os triângulos $\triangle ABC$ com lados de comprimentos inteiros a,b e c e que tenham seus ângulos em progressão aritmética.

Como a soma dos ângulos internos de um triângulo é 180^o, considerando que a razão da progressão é α, então os ângulos terão medidas $60^o-\alpha, 60^o$ e $60^o+\alpha$.

Suponhamos que o ângulo em B mede 60^o e o ângulo A é o maior, e seja D o pé da altura desde o vértice A. Assim, no triângulo retângulo $\triangle ADB$, temos

$$cos\,60^o = \frac{BD}{c}$$

Como $cos\, 60^{\circ} = \frac{1}{2}$, conclui-se que $BD = \frac{c}{2}$.

Aplicando o teorema de Pitágoras nos triângulos retâgulos $\triangle ADB$ e $\triangle ADC$, temos

$$c^2 - \left(\frac{c}{2}\right)^2 = AD^2 = b^2 - \left(a - \frac{c}{2}\right)^2$$

que equivale a

$$\frac{3}{4}c^2 = b^2 - a^2 + ac - \frac{1}{4}c^2,$$

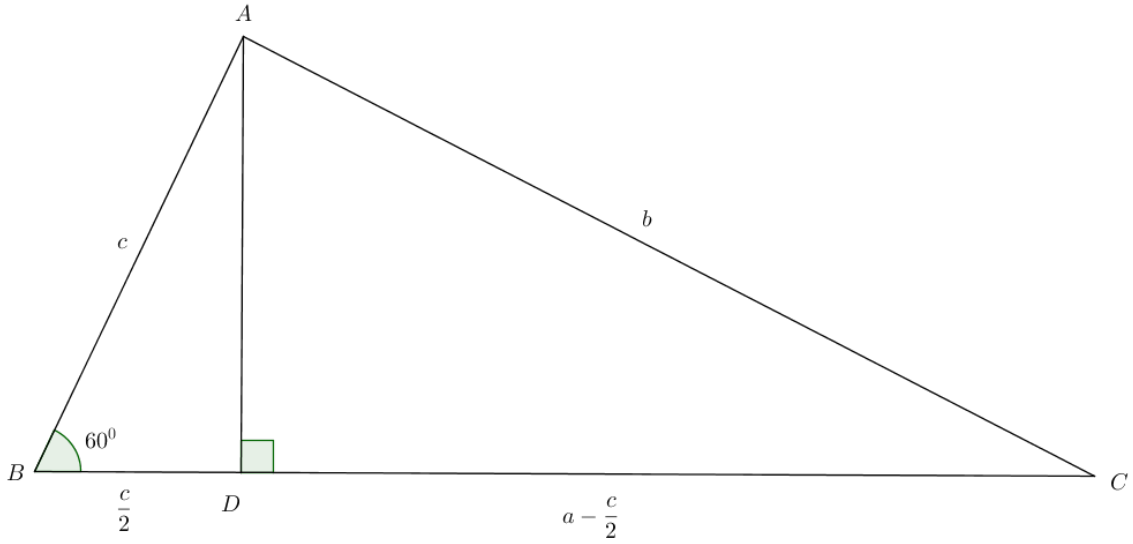

Figura 4 – Triângulo com lados inteiros e ângulos em PA.
Fonte: Moreira, Martínez e Saldanha (2012, p. 194).

ou seja, os triângulos que têm os lados em progressão aritmética são os triângulos que têm lados que satisfazem a relação

$$a^2 - ac + c^2 = b^2,$$

que equivale, usando o método geométrico, a determinar as soluções racionais da equação

$$x^2 - xy + y^2 = 1$$

que representa, no plano cartesiano, uma elipse rotacionada. Observemos que esta equação possui a solução $(0, -1)$. A equação da reta que passa pelo ponto $(0, -1)$ e tem inclinação $\frac{m}{n}$ é $y = \frac{m}{n}x - 1$.

Os pontos de interseção da reta com a elipse são as soluções obtidas quando resolvemos o sistema de equações

$$\begin{cases} x^2 - xy + y^2 = 1 \\ y = \frac{m}{n}x - 1 \end{cases}$$

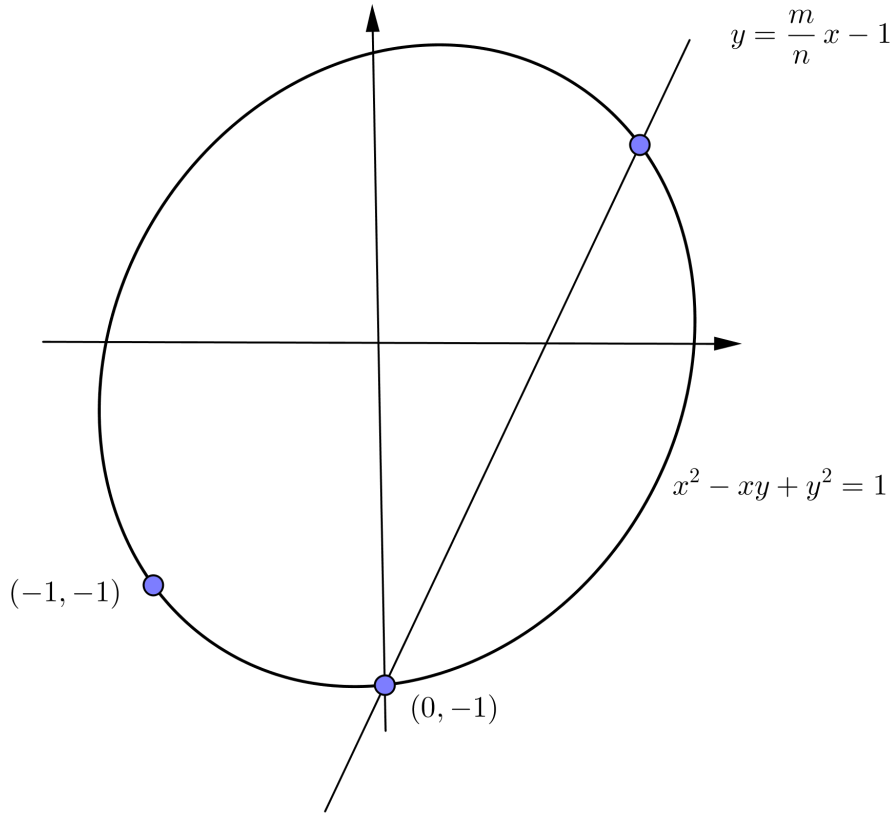

Figura 5 – Interseção entre reta e elipse.
Fonte: Moreira, Martínez e Saldanha (2012, p. 195).

substituindo y na equação da elipse, temos a equação

$$(m^2 - mn + n^2)x^2 - (2m - n)nx = 0$$

cujas soluções são $x = 0$ e $x = \dfrac{2mn - n^2}{m^2 - mn + n^2}$.

Assim,

$$x = \frac{a}{b} = \frac{2mn - n^2}{m^2 - mn + n^2} \quad , \quad y = \frac{c}{b} = \frac{m^2 - n^2}{m^2 - mn + n^2}$$

Portanto,

$$a = k(2mn - n^2), \quad b = k(m^2 - mn + n^2), \quad c = k(m^2 - n^2), \quad k \in \mathbb{Z}.$$

Em continuidade, mostraremos como determinar todos os triângulos com lados inteiros, tais que um ângulo é o dobro do outro. Para isto, suponhamos que temos um triângulo $\triangle ABC$ com lados de comprimentos $a, b,$ e c tal que $\angle A = 2\angle B = 2\beta$. Tracemos a bissetriz desde o vértice A e denotemos por D o pé da bissetriz no lado BC.

Pelas condições acima, segue que o triângulo $\triangle BDA$ é isósceles, e, assim,

$BD = DA = x$. Por outro lado, o ângulo $\angle ADC$ é ângulo externo ao triângulo $\triangle BDA$; logo, ele é a soma dos ângulos não adjacentes, donde $\angle ADC = 2\beta$.

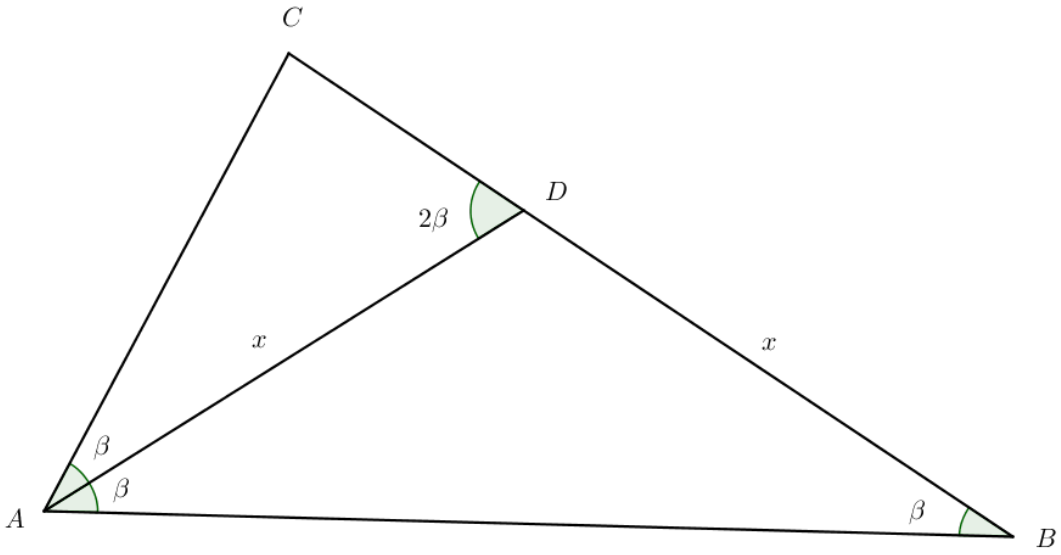

Figura 6 – Triângulo com lados inteiros e $\angle A = 2\angle B = 2\beta$.
Fonte: Moreira, Martínez e Saldanha (2012, p. 197), com adaptações.

Assim, os triângulos $\triangle ABC$ e $\triangle DCA$ são semelhantes, já que seus ângulos são iguais, de onde temos as relações entre os lados

$$\frac{b}{a} = \frac{x}{c} = \frac{a-x}{b}.$$

Da primeira igualdade, temos que $x = \frac{bc}{a}$ e substituindo na segunda igualdade, obtemos que

$$\frac{b}{a} = \frac{a - \dfrac{bc}{a}}{b} = \frac{a^2 - bc}{ab}, \quad \text{assim} \quad b^2 + bc = a^2.$$

Podemos resolver esta equação pelo método geométrico, ou simplesmente, no caso em que $mdc(b, c) = 1$, observando que $b(b + c)$ é um quadrado perfeito, e que b e $b + c$ não têm fator em comum, donde b e $b + c$ têm que ser quadrados de números inteiros; logo, $\begin{cases} b = n^2 \\ b + c = m^2 \end{cases}$ com m e n sem fator comum. Portanto, o conjunto de triângulos procurados é o dos que satisfazem as relações

$$a = kmn, \quad b = kn^2, \quad c = k(m^2 - n^2)$$

com n e m sem fator comum e k inteiro arbitrário.

4.3 Método da Fatoração

Fazem saber Andreescu, Andrica e Cucurezeanu (2010, p. 3) que, dada a equação $f(x_1, x_2, ..., x_n) = 0$, nós podemos escrevê-la na forma equivalente

$$f_1(x_1, x_2, ..., x_n).f_2(x_1, x_2, ..., x_n)....f_k(x_1, x_2, ..., x_n) = a,$$

onde $f_1, f_2, ..., f_k$ possuem coeficientes inteiros e $a \in \mathbb{Z}$.

Fatorando a em números primos, obtemos um número finito de decomposições em k fatores inteiros $a_1, a_2, ..., a_k$. Cada uma dessas decomposições gera um sistema de equações:

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

A solução de todos esses sistemas nos dá o conjunto completo de soluções.

Exemplo 4.3.1. *Encontre todos os triângulos retângulos com lados inteiros e um cateto igual a* 30*.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 179))

Resolução. Precisamos encontrar inteiros positivos b e c tais que $900 + b^2 = c^2$. Esta igualdade pode ser reescrita da seguinte forma:

$$2^2.3^2.5^2 = (c + b).(c - b).$$

Observando que os números $c + b$ e $c - b$ têm a mesma paridade, logo, os dois são pares; e como $c + b$ é maior que $c - b$, as únicas formas de distribuir os fatores de 900 entre estes fatores são

$$\begin{cases} c + b = 450 \\ c - b = 2 \end{cases}, \quad \begin{cases} c + b = 150 \\ c - b = 6 \end{cases}, \quad \begin{cases} c + b = 90 \\ c - b = 10 \end{cases} \quad \text{e} \quad \begin{cases} c + b = 50 \\ c - b = 18 \end{cases}$$

que geram as soluções $(30, 224, 226), (30, 72, 78), (30, 40, 50)$ e $(30, 16, 34)$.

Exemplo 4.3.2. *Resolva a equação seguinte em números inteiros* x, y*:*

$$x^2 + 6xy + 8y^2 + 3x + 6y = 2.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 193))

Resolução. Escrevendo a equação na forma

$$(x+2y)(x+4y)+3(x+2y)=2 \quad \text{ou} \quad (x+2y)(x+4y+3)=2.$$

obtemos os sistemas

$$\begin{cases} x+2y=1 \\ x+4y+3=2 \end{cases}, \quad \begin{cases} x+2y=2 \\ x+4y+3=1 \end{cases}, \quad \begin{cases} x+2y=-1 \\ x+4y+3=-2 \end{cases} \quad \text{e}$$

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

que geram as soluções $(3,-1),(6,-2),(3,-2)$ e $(0,-1)$.

Exemplo 4.3.3. *Sejam p e q dois números primos, resolva em inteiros positivos a equação*

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

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 5))

Resolução. A equação é equivalente à equação diofantina algébrica

$$(x-pq)(y-pq)=p^2q^2.$$

Observe que $\frac{1}{x}<\frac{1}{pq}$; portanto, temos $x>pq$.

Considerando todos os divisores positivos de p^2q^2, obtemos os seguintes sistemas:

$$\begin{cases} x-pq=1 \\ y-pq=p^2q^2 \end{cases}, \quad \begin{cases} x-pq=p \\ y-pq=pq^2 \end{cases}, \quad \begin{cases} x-pq=q \\ y-pq=p^2q \end{cases},$$

$$\begin{cases} x-pq=p^2 \\ y-pq=q^2 \end{cases}, \quad \begin{cases} x-pq=pq \\ y-pq=pq \end{cases}, \quad \begin{cases} x-pq=pq^2 \\ y-pq=p \end{cases},$$

$$\begin{cases} x-pq=p^2q \\ y-pq=q \end{cases}, \quad \begin{cases} x-pq=q^2 \\ y-pq=p^2 \end{cases}, \quad \begin{cases} x-pq=p^2q^2 \\ y-pq=1 \end{cases},$$

que conduzem às soluções:

$$(1+pq,pq(1+pq)), \quad (p(1+q),pq(1+q)), \quad (q(1+p),pq(1+p)),$$

$$(p(p+q),q(p+q)), \quad (2pq,2pq), \quad (pq(1+q),p(1+q)),$$

$$(pq(1+p),q(1+p)), \quad (q(p+q),p(p+q)), \quad (pq(1+pq),1+pq).$$

Exemplo 4.3.4. *Resolva a seguinte equação em números inteiros x, y:*

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

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 7-8))

Resolução. Tomando $x=u+1$, $y=v+1$, a equação torna-se

$$(u+1)^2v+(v+1)^2u=1,$$

equivalente à

$$uv(u+v)+4uv+(u+v)=1.$$

A última equação pode ser escrita como

$$uv(u+v+4)+(u+v+4)=5,$$

ou

$$(u+v+4)(uv+1)=5.$$

Um dos fatores tem que ser igual a 5 ou -5, e o outro, 1 ou -1. Isto significa que a soma $u+v$ e produto uv têm de satisfazer algum dos quatro sistemas de equações:

$$\begin{cases} u+v=1 \\ uv=0 \end{cases}, \quad \begin{cases} u+v=-9 \\ uv=-2 \end{cases}, \quad \begin{cases} u+v=-3 \\ uv=4 \end{cases}, \quad \begin{cases} u+v=-5 \\ uv=-6 \end{cases}.$$

Somente o primeiro e o último desses sistemas têm soluções inteiras. Elas são $(0,1)$, $(1,0)$, $(-6,1)$, $(1,-6)$. Assim, o resultado final $(x,y)=(u+1,v+1)$ são os pares $(1,2),(-5,2),(2,1),(2,-5)$.

Exemplo 4.3.5. *Determine todos os triângulos retângulos com lados de comprimentos inteiros tais que suas áreas e perímetros sejam iguais.*

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 198-199))

Resolução. Sejam x e y os comprimentos dos catetos e z o comprimento da hipotenusa, onde x, y e z são números inteiros positivos. Em seguida, pelo teorema de Pitágoras, $z=\sqrt{x^2+y^2}$.
Igualando a área e o perímetro, temos

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

Multiplicando por 2, isolando o radical, e elevando ao quadrado, isso resulta

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

ou

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

Temos

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

Simplificando a equação anterior por xy, uma vez que $xy \neq 0$, temos:

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

Adicionando 8 a ambos os lados para tornar possível a seguinte fatoração, temos:

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

e, uma vez que as variáveis são inteiros, existe apenas um número finito de possibilidades. As únicas soluções (x, y) são $(6, 8), (8, 6), (5, 12), (12, 5)$, que produzem apenas dois triângulos, os de lados $6 - 8 - 10$ e $5 - 12 - 13$.

4.4 Utilizando Inequações para Resolver Equações Diofantinas

Segundo Andreescu, Andrica e Cucurezeanu (2010, p. 13), este método consiste em restringir os intervalos em que as variáveis se encontram, utilizando desigualdades adequadas. De modo geral, esse processo leva a um número finito de possibilidades para todas as variáveis; ou para algumas delas.

Exemplo 4.4.1. *Encontre todos os triângulos retângulos com lados inteiros e a hipotenusa igual a* 65*.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 179-180))

Resolução. Neste caso, precisamos encontrar dois números inteiros a e b, que podemos supor, sem perda de generalidade, satisfazem $a < b$, tais que $a^2 + b^2 = 65^2 = 4225$. Como $b^2 + (b-1)^2 \geq 4225$, temos que $64 \geq b \geq 47$. Assim, temos 18 possíveis valores de b que precisamos testar se verificam que $4225 - b^2$ é um quadrado perfeito. De fato, este número é quadrado perfeito quando b é igual a $52, 56, 60$ e 63, que geram os triângulos com lados de comprimento $(39, 52, 65), (33, 56, 65), (25, 60, 65)$ e $(16, 63, 65)$

Exemplo 4.4.2. *Resolva em inteiros positivos a equação*

$$3(xy + yz + zx) = 4xyz.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 202))

Resolução. A equação é equivalente a $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{4}{3}$. Por conta da simetria da equação, podemos assumir que $x \leq y \leq z$. Segue-se que $\frac{3}{x} \geq \frac{4}{3}$; isto é, $x \leq \frac{9}{4}$. Portanto, $x \in \{1, 2\}$

Se $x = 1$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{3}$$

Como $z = \dfrac{3y}{y-3}$ e $\dfrac{2}{y} \geq \dfrac{1}{3}$, sendo y e z inteiros positivos, temos as soluções $y = 4$, $z = 12$ e $y = z = 6$.
Se $x = 2$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{5}{6}$$

Como $z = \dfrac{6y}{5y-6}$ e $\dfrac{2}{y} \geq \dfrac{5}{6}$, sendo y e z inteiros positivos, temos a solução $y = 2$ e $z = 3$.

Portanto, para os dois casos, temos as soluções $(1, 4, 12), (1, 6, 6), (2, 2, 3)$ e todas as suas permutações.

Exemplo 4.4.3. *Resolva em inteiros positivos a equação*

$$x^2y + y^2z + z^2x = 3xyz.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 204))

Resolução. Note-se que este é o caso de igualdade na desigualdade entre as médias aritmética e geométrica

$$x^2y + y^2z + z^2x \geq 3\sqrt[3]{(x^2y)(y^2z)(z^2x)} = 3xyz.$$

Por isso, devemos ter $x^2y = y^2z = z^2x$, o que implica $x^2 = yz$, $y^2 = zx$, $z^2 = xy$, isto é,

$$(x-y)^2 + (y-z)^2 + (z-x)^2 = 0.$$

As soluções são (k, k, k), $k \in \mathbb{Z}_+$.
Nota: Dados os números positivos $x_1, x_2, ..., x_n$, definimos:

Média aritmética simples (A)

$$A = \frac{x_1 + x_2 + ... + x_n}{n}$$

Média geométrica simples (G)

$$G = \sqrt[n]{x_1 x_2 ... x_n}$$

Média harmônica simples (H)

$$H = \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + ... + \frac{1}{x_n}}$$

Média quadrática (Q)

$$Q = \sqrt[n]{\frac{x_1^2 + x_2^2 + ... + x_n^2}{n}}$$

Se $x_1, x_2, ..., x_n$ são números positivos e Q, A, G e H são suas médias quadrática, aritmética, geométrica e harmônica, respectivamente, então $Q \geq A \geq G \geq H$. Além disso, duas quaisquer dessas médias são iguais se, e somente se, $x_1 = x_2 = ... = x_n$. Particularmente,

$$\frac{x_1 + x_2 + ... + x_n}{n} \geq \sqrt[n]{x_1 x_2 ... x_n}$$

e

$$\frac{x_1 + x_2 + ... + x_n}{n} = \sqrt[n]{x_1 x_2 ... x_n}$$

se, e somente se, $x_1 = x_2 = ... = x_n$.

Exemplo 4.4.4. *Encontre todos os inteiros positivos $n, k_1, ..., k_n$ tais que*

$$k_1 + ... + k_n = 5n - 4$$

e

$$\frac{1}{k_1} + ... + \frac{1}{k_n} = 1.$$

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 16-17))

Resolução. Pela desigualdade das médias aritmética e harmônica, temos

$$(k_1 + ... + k_n)\left(\frac{1}{k_1} + ... + \frac{1}{k_n}\right) \geq n^2.$$

Devemos ter, portanto, $5n - 4 \geq n^2$; por isso, $n \leq 4$. Sem perda de generalidade, podemos supor que $k_1 \leq ... \leq k_n$.

Se $n = 1$, temos que $k_1 = 5.1 - 4$, isto é $k_1 = 1$, que funciona, pois $\frac{1}{k_1} = 1$. Note-se que daqui em diante não podemos ter $k_1 = 1$.

Se $n = 2$, temos que $k_1 + k_2 = 5.2 - 4 = 6$, então, $(k_1, k_2) \in \{(2, 4), (3, 3)\}$, mas nenhum funciona, pois não satisfazem a condição $\frac{1}{k_1} + ... + \frac{1}{k_n} = 1$.

Se $n = 3$, então $k_1 + k_2 + k_3 = 11$; assim, $2 \leq k_1 \leq 3$.

Daí $(k_1, k_2, k_3) \in \{(2, 2, 7), (2, 3, 6), (2, 4, 5), (3, 3, 5), (3, 4, 4)\}$, e só $(2, 3, 6)$ funciona.

Se $n = 4$, temos a igualdade na desigualdade das médias aritmética e harmônica, o que só acontece quando $k_1 = k_2 = k_3 = k_4 = 4$.

Portanto, as soluções são $n = 1$ e $k_1 = 1$; $n = 3$ e (k_1, k_2, k_3) é uma permutação de $(2, 3, 6)$; e $n = 4$ e $(k_1, k_2, k_3, k_4) = (4, 4, 4, 4)$.

4.5 O Método Aritmético Modular

Andreescu, Andrica e Cucurezeanu (2010, p. 29) destacam que, em muitas situações, as considerações aritméticas modulares simples são utilizadas para provar que certas equações diofantinas não são resolúveis ou para reduzir o intervalo das possíveis soluções.

Exemplo 4.5.1 (Itália)**.** *Ache todos os* x *e* $y \in \mathbb{N}$ *tais que* $x^2 + 615 = 2^y$*.*

(Fonte: Muniz Neto (2012, p. 125-126))

Resolução. Analisando a equação dada módulo 3, obtemos

$$x^2 + 0 \equiv (-1)^y \, (mod\, 3).$$

Como $x^2 \equiv 0$ ou $1\,(mod\, 3)$, então a congruência acima nos dá as seguintes possibilidades:

$$0 \equiv (-1)^y \, (mod\, 3) \text{ ou } 1 \equiv (-1)^y \, (mod\, 3).$$

A primeira possibilidade nunca ocorre, pois $3 \nmid 1$ e $3 \nmid -1$. Quanto à segunda, se y for ímpar, obtemos $1 \equiv -1\,(mod\, 3)$, o que também nunca ocorre, pois $3 \nmid 2$. Portanto, y deve ser par, digamos $y = 2z$, com $z > 0$ inteiro. A equação do enunciado pode ser, agora, escrito como

$$615 = 2^{2z} - x^2 = (2^z - x)(2^z + x).$$

Por fim, como $2^z + x > 2^z - x$ e $615 = 3.5.41$, temos somente as possibilidades.

$$\begin{cases} 2^z + x = 615 \\ 2^z - x = 1 \end{cases}, \quad \begin{cases} 2^z + x = 205 \\ 2^z - x = 3 \end{cases}, \quad \begin{cases} 2^z + x = 123 \\ 2^z - x = 5 \end{cases} \text{ ou } \quad \begin{cases} 2^z + x = 41 \\ 2^z - x = 15 \end{cases}.$$

Somando membro a membro as duas equações em cada uma das possibilidades acima, obtemos respectivamente $2^{z+1} = 616, 208, 128$ ou 56. Mas, uma vez que $2^{z+1} = 128$, de sorte que

$$\begin{cases} 2^z + x = 123 \\ 2^z - x = 5 \end{cases},$$

então $z = 6$ e $x = 59$, de modo que a única solução é $x = 59$ e $y = 12$.

Exemplo 4.5.2 (OIM)**.** *Ache todos os* $m, n \in \mathbb{N}$*, tais que* $2^m + 1 = 3^n$.

(Fonte: Muniz Neto (2012, p. 126-127))

Resolução. Se $m = 1$, então $n = 1$. Se $m \geq 2$, então $2^m \equiv 0\,(mod\,4)$; portanto, analisando a equação módulo 4, obtemos

$$1 \equiv (-1)^n\,(mod\,4),$$

de onde segue que n deve ser par, digamos $n = 2u$, com $u \in \mathbb{N}$. Fazendo esta substituição na equação do enunciado, obtemos $2^m + 1 = 3^{2u}$ ou ainda,

$$2^m = (3^u - 1)(3^u + 1).$$

Para vermos a que fatoração de 2^m corresponde $(3^u - 1)(3^u + 1)$, seja $d = mdc(3^u - 1, 3^u + 1)$. Então,

$$d|\,[(3^u + 1) - (3^u - 1)]\,,$$

ou seja, $d|2$; mas, como $3^u - 1$ e $3^u + 1$ são ambos pares, deve ser $d = 2$. Por outro lado, uma vez que o produto de $3^u - 1$ e $3^u + 1$ é uma potência de base 2, cada um dos fatores $3^u - 1$ e $3^u + 1$ deve ser uma potência de base 2. Ocorre que o mdc de duas potências de 2 só é igual a 2 quando a menor de tais potências for igual a 2, de modo que a única possibilidade é termos

$$\begin{cases} 3^u - 1 = 2 \\ 3^u + 1 = 2^{m-1} \end{cases}$$

Logo, $u = 1$, $m = 3$ e, daí, $n = 2$.

Exemplo 4.5.3. *Prove que a equação $x^2 = 3y^2 + 8$ não possui soluções em inteiros x e y.*

(Fonte: Feitosa (2012))

Resolução. Analisando o resto na divisão por 3, obtemos $x^2 \equiv 2\,(mod\,3)$. Como os únicos restos na divisão de um quadrado por 3 são 0 e 1, então não existem soluções em inteiros.

Exemplo 4.5.4. *Encontre todas as soluções em inteiros da equação $x^2 - 7y = 1004$.*

(Fonte: Feitosa (2012))

Resolução. Analisando os restos na divisão por 7, obtemos $x^2 \equiv 3\,(mod\,7)$. Entretanto, os únicos inteiros que são restos de quadrados perfeitos na divisão por 7 são $0, 1, 2$ e 4. Como $3 \equiv 1004\,(mod\,7)$ não faz parte dessa lista, então não existem soluções inteiras para a equação.

Exemplo 4.5.5. *Mostre que a equação*

$$(x + 1)^2 + (x + 2)^2 + ... + (x + 99)^2 = y^z$$

não tem solução em números inteiros x, y, z, com $z > 1$.

(Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 219))

Resolução. Notemos que

$$\begin{aligned} y^z &= (x+1)^2 + (x+2)^2 + ... + (x+99)^2 \\ &= 99x^2 + 2(1+2+...+99)x + (1^2+2^2+...+99^2) \\ &= 99x^2 + \frac{2.99.100}{2}x + \frac{99.100.199}{6} \\ &= 33(3x^2 + 300x + 50.199), \end{aligned}$$

o que implica $3|y$. Observando que $z \geq 2$, temos que $3^2|y^z$; mas 3^2 não divide $33(3x^2 + 300x + 50.199)$, constituindo uma contradição; o que nos leva a concluir que a equação dada não tem solução em números inteiros x, y, z, com $z > 1$.

Exemplo 4.5.6. *Prove que a equação*

$$4xy - x - y = z^2$$

não tem solução em números inteiros positivos.

(Fonte:Andreescu, Andrica e Cucurezeanu (2010, p. 223-224))

Resolução. A equação é equivalente a

$$(4x-1)(4x-1) = 4z^2 + 1.$$

Seja p um divisor primo de $4x-1$. Então, $4z^2 \equiv -1\,(mod\,p)$; isto é, $(2z)^2 \equiv -1\,(mod\,p)$. Pelo Pequeno Teorema de Fermat, temos $(2z)^{p-1} \equiv 1\,(mod\,p)$. Então,

$$1 \equiv (2z)^{p-1} \equiv ((2z)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\,(mod\,p),$$

e, portanto, $p \equiv 1\,(mod\,4)$.

Assim, qualquer divisor primo de $4x-1$ deve ser congruente a $1\,(mod\,4)$; daí $4x - 1 \equiv 1\,(mod\,4)$, o que é uma contradição.

Exemplo 4.5.7 (Romênia)**.** *Sejam p e q números primos, com $q \neq 5$. Se $q|(2^p + 3^p)$, prove que $q > p$.*

(Fonte: Muniz Neto (2012, p. 135))

Demonstração. Como $q|(2^p + 3^p)$, temos que $q \neq 2, 3$, de modo que $q > 5$. Portanto, podemos supor que $p > 3$. Se $q \leq p$, então $q - 1 < p$, de sorte que $q-1$ e p são primos entre si. Nesse caso, o **Teorema 2.7.5** garante a existência de $x, y \in \mathbb{N}$ tais que $px = (q-1)y+1$. Portanto, a partir de $2^p \equiv -3^p\,(mod\,q)$, obtemos $(2^p)^x \equiv (-3^p)^x\,(mod\,q)$; mas, como $-3^p = (-3)^p$, segue que

$$2^{(q-1)y+1} \equiv (-3)^{(q-1)y+1} \, (mod \, q)$$

Por fim, uma vez que $q \neq 2, 3$, o pequeno Teorema de Fermat nos dá $2^{q-1} \equiv 1 \, (mod \, q)$ e $(-3)^{q-1} \equiv 1 \, (mod \, q)$; a partir daí, a congruência acima se reduz a $2 \equiv -3 \, (mod \, q)$, de maneira que $q = 5$. Por fim, tal conclusão é, claramente, uma contradição. □

Exemplo 4.5.8 (OBM)**.** *Prove que existe um inteiro* $k > 2$ *tal que o número* $1\underbrace{99...9}_{k}1$ *é um múltiplo de* 1991*.*

(Fonte: Muniz Neto (2012, p. 137-138))

Demonstração. Observe primeiramente que

$$1\underbrace{99...9}_{k}1 = 2.10^{k+1} - 9.$$

Portanto, queremos achar $k > 2$ inteiro tal que

$$2.10^{k+1} - 9 \equiv 0 \, (mod \, 1991)$$

ou, ainda, $2.10^{k+1} \equiv 9 \, (mod \, 1991)$. Mas, como $2.10^3 \equiv 9 \, (mod \, 1991)$, temos

$$2.10^{k+1} \equiv 9 \, (mod \, 1991) \Longleftrightarrow 2.10^{k+1} \equiv 2.10^3 \, (mod \, 1991) \Longleftrightarrow 10^{k-2} \equiv 1 \, (mod \, 1991)$$

Para o que falta, veja que $991 = 11.181$ e 181 é primo. Portanto, $\phi(1991) = \phi(11).\phi(181) = 10.180 = 1800$ e segue, pelo teorema de Euler, que $10^{1800} \equiv 1 \, (mod \, 1991)$. Logo, basta tormarmos $k - 2 = 1800$. □

4.6 Descenso Infinito de Fermat (ou Descida de Fermat)

Pierre de Fermat (1601 - 1665), embora não tenha sido um matemático profissional, foi considerado pelo filósofo, físico e matemático francês Blaise Pascal (1623 - 1662) um grande matemático.

Seu interesse na Matemática estava principalmente em questões vinculadas a desafios e problemas. Suas inquirições matemáticas atravessaram várias gerações. Ele fez contribuições importantes para o cálculo geométrico, infinitesimal e, principalmente, para a Teoria dos Números. O Último Teorema de Fermat, como passou a ser indicado, é o mais famoso dos trabalhos de Fermat. O seu enunciado simples diz que a equação: $x^n + y^n = z^n$ não tem solução em números inteiros e positivos para $n > 2$. Fermat escreveu nas margens do livro *Arithmética*, de Diofanto, com o qual estava trabalhando, que conseguira uma demonstração para o problema acima, mas que não havia espaço suficiente para ela na margem do livro (ao que parece, Fermat utilizou o método do *descenso infinito*, objeto de nosso estudo nesta subseção). Hoje, não se acredita que

ele tenha conseguido uma demonstração correta do problema, visto que este Teorema de Fermat, mesmo tendo atraído a atenção de muitos matemáticos, por mais de 300 anos ficou em aberto (NASCIMENTO; FEITOSA, 2013, p. 127).

O matemático Kummer, por exemplo, tentou encontrar a demonstração para o teorema (por algum tempo pensou que havia encontrado). Ele notou que uma afirmação que era verdade para os inteiros relativos não era para formações numéricas mais complexas que, naturalmente, aparecem no estudo do problema de Fermat. Acontece que *números inteiros algébricos* (ou seja, os números são raízes de equações algébricas com coeficientes inteiros racionais e coeficiente da maior potência da variável igual a 1), podem não ter decomposição única em fatores primos da mesma natureza algébrica. Inteiros relativos são decompostos em fatores primos de forma única. Por exemplo, $6 = 2.3$ e o número 6 não admite nenhuma outra decomposição no conjunto dos números inteiros relativos. Considerando, agora, o conjunto de todos os números algébricos da forma $m + n\sqrt{-5}$, onde m e n são números inteiros relativos, pode-se verificar que a soma e o produto de dois números desta forma são números que pertencem a esse mesmo conjunto. Todo conjunto de números que têm a propriedade de conter qualquer soma e produto dos números que lhe pertencem é denominado de *anel*. Por definição, no anel considerado se encontram os números $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$. Pode-se demonstrar que, neste anel, cada um dos números indicados é primo, isto é, não pode ser representado como o produto de números inteiros pertencentes ao anel considerado e diferentes da unidade. Porém,

$$6 = 2.3 = (1 + \sqrt{-5}).(1 - \sqrt{-5}),$$

isto é, neste anel, o número 6 não pode ser decomposto de maneira única em fatores primos.

A não unicidade da decomposição de um número em fatores primos também pode ter lugar em outros anéis mais complexos de números inteiros algébricos. Ao descobrir isso, Kummer se convenceu que sua demonstração do Último Teorema de Fermat não estava correta. Para superar as dificuldades criadas pela não unicidade da decomposição em fatores primos, Kummer criou a *teoria de ideais* , que atualmente desempenha um papel extraordinariamente importante na Álgebra e Teoria dos Números (GUELFOND, 2010, p. 105-107).

Mas esta é uma outra história.

O Último Teorema de Fermat desafiou matemáticos por 358 anos, e apenas em 1993, o matemático britânico Andrew Wiles conseguiu uma demonstração que ainda precisou de reparos, e só tornou-se definitiva em 1995, com a colaboração do também inglês Richard Taylor (ex-aluno de Wiles). Para tanto, Wiles utilizou recursos sofisticados dos quais Fermat não dispunha.

Em alguns casos, é possível mostrar que algumas equações diofantinas

$$f(x_1, ..., x_n) = 0,$$

não possuem solução. O método da descida de Fermat, quando aplicável, permite mostrar que esta equação não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as suas soluções inteiras. Se o conjunto de soluções de f

$$A = \{(x_1, ..., x_n) \in \mathbb{Z}^n \mid f(x_1, ..., x_n) = 0\}$$

é diferente de vazio, então gostaríamos de considerar a solução minimal em certo sentido. Ou seja, queremos construir uma função $\phi : A \to \mathbb{N}$ e considerar a solução $(x_1, ..., x_n) \in A$ com $\phi(x_1, ..., x_n)$ mínimo. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos conduz claramente a uma contradição, provando que A é de fato vazio (MOREIRA; MARTíNEZ; SALDANHA, 2012, p. 238).

O método da descida de Fermat consiste, então, no seguinte esquema (MUNIZ NETO, 2012, p. 55):
$i)$ Supor que uma dada equação possui uma solução em inteiros não nulos.
$ii)$ Concluir daí que ela possui uma solução em inteiros positivos que seja, em algum sentido, mínima.
$iii)$ Deduzir a existência de uma solução positiva menor que a mínima, chegando a uma contradição.

Exemplo 4.6.1. *Prove que a equação $3x^2 + y^2 = 2z^2$ não possui soluções inteiras não nulas.*

(Fonte: Muniz Neto (2012, p. 55-56))

Demonstração. Inicialmente, observe que não podemos ter exatamente um dos inteiros x, y, z igual a 0. Suponha, pois, que a equação dada possua uma solução (x, y, z) com $x, y, z \in \mathbb{N}$ (uma vez que, se (x, y, z) for solução, então todas as triplas obtidas a partir das permutações de $(\pm x, \pm y, \pm z)$ também serão). Então, dentre todas tais soluções (x, y, z), existe uma para a qual z é a menor possível, digamos $x = a, y = b, z = c$. Trabalhemos tal solução.

Se $3 \nmid b$, temos de $3a^2 + b^2 = 2c^2$ que $3 \nmid c$. Daí, como b^2 e c^2 deixam resto 1 na divisão por 3 e a igualdade $3a^2 + b^2 = 2c^2$ nos dá uma contradição, logo, $3|b$, digamos $b = 3b_1$ para algum $b_1 \in \mathbb{N}$, e segue de

$$2c^2 = 3a^2 + b^2 = 3(a^2 + 3b_1^2)$$

que $3|c$. Sendo $c = 3c_1$, para algum $c_1 \in \mathbb{N}$, a igualdade acima nos dá

$$6c_1^2 = a^2 + 3b_1^2,$$

de modo que $3|a$, digamos $a = 3a_1$, com $a_1 \in \mathbb{N}$. Portanto, a última igualdade acima fornece

$$2c_1^2 = 3a_1^2 + b_1^2,$$

de sorte que (a_1, b_1, c_1) é outra solução da equação original no conjunto dos números naturais. Contudo, a relação $0 < c_1 = \frac{c}{3} < c$ é uma contradição, uma vez que partimos de uma solução em naturais (a, b, c) para a qual c era o menor possível. Logo, nossa equação não possui soluções não nulas. □

Exemplo 4.6.2. *Sejam a e b inteiros positivos tais que $b < 2a+1$. Mostre que a equação $bx^2 - 2axy - y^2 = 0$ não possui soluções inteiras positivas.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 238-239))

Demonstração. Suponhamos que a equação possui solução não nula (m, n) com $m, n \in \mathbb{N}$, isto é, $bm^2 - 2amn - n^2 = 0$ e escolhemos esta solução de tal forma que n seja mínimo. Como $n^2 + 2amn = bm^2$, somando ao dois lados a^2m^2 obtemos que

$$(n + am)^2 = (b + a^2)m^2 < (a^2 + 2a + 1)m^2 = (a + 1)^2m^2,$$

e assim $n + am < am + m$, isto é, $n < m$. Observemos que $m(bm - 2an) = n^2$, isto é, m é um divisor de n^2, portanto $n^2 = mq$ onde $0 < q < n < m$ e $q + 2an = bm$. Por outro lado, multiplicando a equação original por b obtemos:

$$0 = bn^2 + 2an(bm) - (bm)^2 = bn^2 + 2an(q + 2an) - (q + 2an)^2 = bn^2 - 2anq - q^2,$$

logo, o par (n, q) é também solução da equação, o que contradiz a minimalidade da solução anterior. □

Exemplo 4.6.3. *Mostre que se k é um inteiro positivo que não é um quadrado perfeito, então $\sqrt{k}$ é irracional.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 239))

Demonstração. De fato, suponhamos por contradição que $\sqrt{k}$ é racional e seja a a sua parte inteira. Logo, existem inteiros não nulos m, n tais que $\sqrt{k} = a + \frac{n}{m}$. Elevando ao quadrado e multiplicando por m^2 obtemos:

$$(k - a^2)m^2 - 2amn - n^2 = 0,$$

isto é, a equação $(k - a^2)x^2 - 2axy - y^2 = 0$ possui solução inteira positiva, mas $k < (a + 1)^2$; portanto, $k - a^2 < 2a + 1$, mas, pelo problema anterior, a equação não possui soluções inteiras positivas; portanto, $\sqrt{k}$ não pode ser racional. □

Exemplo 4.6.4 (Fermat)**.** *Demonstre que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas, isto é, não existem triplas pitagóricas em que os dois catetos sejam quadrados perfeitos.*

(Fonte: Moreira, Martínez e Saldanha (2012, p. 239-240))

Demonstração. Suponhamos que $x^4+y^4=z^2$ possui uma solução inteira com $x,y,z>0$. Logo, existe uma tal solução (a,b,c) na qual c é mínimo. Em particular, temos que a e b são primos entre si, pois se $d=mdc(a,b)>1$ poderíamos substituir (a,b,c) por $\left(\frac{a}{d},\frac{b}{d},\frac{c}{d^2}\right)$ e obter uma solução com c menor. De $(a^2)^2+(b^2)^2=c^2$ temos, portanto, que (a^2,b^2,c) é uma tripla pitagórica primitiva, e, assim, existem inteiros positivos m e n primos relativos, com $m+n$ ímpar tais que

$$a^2=m^2-n^2, \quad b^2=2mn \quad \text{e} \quad c=m^2+n^2.$$

Desde que m e n tenham paridades distintas, um tem que ser par e outro ímpar. Nesse caso, m é ímpar e n é par, pois, do contrário, teríamos $m=2e$ e $n=2f+1$, com e,f inteiros positivos, e então, $a^2\equiv 0-1\equiv 3\,(mod\,4)$, mas desde que a^2 é um quadrado perfeito ímpar, então deveria ser congruente a 1 módulo 4.

Observando que $b^2=(2n)m$ é um quadrado perfeito e $mdc(2n,m)=1$ (pois $mdc(m,n)=1$), concluímos que tanto $2n$ como m são quadrados perfeitos, de onde podemos encontrar inteiros positivos s e t tais que

$$2n=4s^2 \quad \text{e} \quad m=t^2.$$

Por outro lado, dado que $a^2+n^2=m^2$, então existirão inteiros positivos i e j, primos entre si, tais que

$$a=i^2-j^2, \quad n=2ij \quad \text{e} \quad m=i^2+j^2.$$

Portanto, $s^2=\frac{n}{2}=ij$; logo, i e j serão quadrados perfeitos, digamos $i=u^2$ e $j=v^2$.

Logo, temos que $m=i^2+j^2$, $i=u^2$, $j=v^2$ e $m=t^2$, assim,

$$t^2=u^4+v^4,$$

isto é, (u,v,t) é outra solução da equação original. Porém,

$$t\leq t^2=m\leq m^2<m^2+n^2=c$$

e $t\neq 0$ porque m é diferente de 0. Isto contradiz a minimalidade de c, o que conclui a demonstração. □

Observemos que, uma vez que a equação $x^4+y^4=z^2$ não possui soluções inteiras positivas, a equação $x^4+y^4=z^4$ e, mais geralmente $x^{4n}+y^{4n}=z^{4n}$ não possuem soluções inteiras positivas.

4.7 Equação de Pell

Seja A um inteiro positivo. Estamos interessados na equação $x^2 - Ay^2 = 1$, com x e y inteiros. Se A é um quadrado perfeito, digamos $A = k^2$, temos que $x^2 - Ay^2 = (x - ky)(x + ky) = 1$ admite apenas as soluções triviais $y = 0$, $x = \pm 1$, pois teríamos $x - ky = x + ky = \pm 1$. O caso interessante é quando A não é um quadrado perfeito, e portanto $\sqrt{A}$ é um irracional (de fato, se $\sqrt{A} = \frac{p}{q}$, com $mdc(p, q) = 1$ e $q > 1$, teríamos $A = \frac{p^2}{q^2}$, o que é um absurdo, pois $mdc(p, q) = 1 \implies mdc(p^2, q^2) = 1$, donde $\frac{p^2}{q^2}$ não pode ser inteiro). Nesse caso, a equação $x^2 - Ay^2 = 1$, com x e y inteiros e A é um inteiro positivo que não é um quadrado perfeito, é conhecida como *equação de Pell* (MARTíNEZ et al., 2013, p. 163).

Feitas estas considerações iniciais, Andreescu, Andrica e Cucurezeanu (2010, p. 118-121) fazem saber que Euler, após uma leitura superficial de *Opera Mathematica* de Wallis, erroneamente atribuiu o primeiro estudo importante das soluções não triviais para equações da forma $x^2 - dy^2 = 1$, onde $x \neq 1$ e $y \neq 0$, a John Pell. No entanto, não há nenhuma evidência de que Pell, que ensinou na Universidade de Amsterdã, tenha se ocupado em resolver tais equações. Elas provavelmente deveriam ser chamadas equações de Fermat, já que foi Fermat o primeiro a investigar as propriedades das soluções não triviais de tais equações. Não obstante, as *equações de Pell* têm uma longa história e podem ser rastreadas até os gregos . Theon de Smyrna utilizou $\frac{x}{y}$ para a aproximação de $\sqrt{2}$, onde x e y são soluções inteiras para $x^2 - 2y^2 = 1$. Em geral, se $x^2 = dy^2 + 1$, então, $\frac{x^2}{y^2} = d + \frac{1}{y^2}$. Assim, para y grande, $\frac{x}{y}$ é uma boa aproximação para $\sqrt{d}$, um fato bem conhecido por Arquimedes. O *problema bovino*[2] de Arquimedes levou dois mil anos para ser resolvido.

Em *Arithmética*, Diofanto encontrou soluções racionais para equações do tipo $x^2 - dy^2 = 1$. No caso em que $d = m^2 + 1$, Diofanto oferece a solução inteira $x = 2m^2 + 1$ e $y = 2m$. As *equações de Pell* eram conhecidas pelos matemáticos hindus. No século quarto, o matemático hindu Baudhayana observou que $x = 577$ e $y = 408$ é uma solução de $x^2 - 2y^2 = 1$ e utilizou a fração $\frac{577}{408}$ para aproximar $\sqrt{2}$. No século VII, Brahmagupta, considerando as soluções para a equação de Pell $x^2 - 92y^2 = 1$, encontrou como menor solução $x = 1151$ e $y = 120$. No século XII , o matemático hindu Bhaskara encontrou a menor solução positiva da equação de Pell $x^2 - 61y^2 = 1$, que é $x = 1766319049$ e $y = 226153980$.

Em 1657, Fermat afirmou, sem provar, que se d é positivo e não é quadrado de um inteiro, então a *equação de Pell* $x^2 - dy^2 = 1$ tem um número infinito de

[2] O Problema Bovino é uma obra de Arquimedes em que ele apresenta um problema de análise diofantina, o estudo das equações polinomiais com soluções inteiras. O problema envolve o cálculo do número de bovinos em um rebanho do deus do sol, dado um certo conjunto de restrições. O problema foi descoberto por Gotthold Ephraim Lessing em um manuscrito grego contendo um poema de quarenta e quatro linhas, na Biblioteca Herzog August em Wolfenbüttel, Alemanha, em 1773. Fonte: <https://pt.wikipedia.org/wiki/O_Problema_Bovino>. Data do acesso: 20/04/2016.

soluções. Se (x, y) é uma solução da equação $x^2 - dy^2 = 1$, então $1^2 = (x^2 - dy^2)^2 = (x^2+dy^2)^2-(2xy)^2d$. Assim, $(x^2+dy^2, 2xy)$ também é uma solução para $x^2-dy^2 = 1$. Por conseguinte, se a *equação de Pell* tem uma solução, então ela tem infinitas soluções. $[...]$

Em 1766, Lagrange provou que a equação $x^2 - Dy^2 = 1$ tem um número infinito de soluções sempre que D é positivo e não é o quadrado de um número inteiro, dando como solução geral $(u_n, v_n)_{n\geq 0}$,

$$u_{n+1} = u_1u_n + Dv_1v_n, \qquad v_{n+1} = v_1u_n + u_1v_n \tag{4.10}$$

onde (u_1, v_1) é a solução fundamental, isto é, a solução $v_1 > 0$ é minimal.

Não apresentaremos a demonstração, mas, observando que a solução geral (4.10) dada por Lagrange envolve recorrências, apresentaremos fórmulas fechadas que nos permitirão encontrar infinitas soluções de uma *equação de Pell*.

Para tanto, faremos uma breve introdução sobre recorrências.

4.7.0.1 Recorrências

Uma *sequência* de números reais é uma função $a : \mathbb{N} \to \mathbb{R}$, que para cada $n \in \mathbb{N}$ associa um número a_n pertencente aos reais chamado n-ésimo termo.

Uma *relação de recorrência* ou, como também é chamada, uma *equação de recorrência*, é uma relação que determina cada termo de uma dada sequência a partir de certo termo, em função dos termos anteriores.

Uma equação de recorrência na qual cada termo depende exclusivamente dos anteriores é dita *homogênea*. Se, além dos termos anteriores, cada elemento da sequência está também em função de um termo independente da sequência, a recorrência é dita *não-homogênea*.

Uma relação de recorrência é dita *linear* quando a função que relaciona cada termo aos termos anteriores é linear. Além disso, é dita de *primeira ordem* quando cada termo da sequência é obtido a partir do termo imediatamente anterior a ele, ou seja, quando a_n está em função de a_{n-1}.

Resolver uma relação ou equação de recorrência, significa encontrar uma *fórmula fechada* para a recorrência, ou seja, uma expressão que forneça cada termo a_n da sequência em função apenas de n e não dos termos anteriores. Tal expressão é chamada *solução* da recorrência.

Uma *relação de recorrência linear* é dita de *segunda ordem* quando cada termo da sequência é obtido a partir dos dois termos imediatamente anteriores a ele, ou seja, quando a_n está em função de a_{n-1} e a_{n-2} .

Uma recorrência linear de segunda ordem é do tipo:

$$a_n = h(n)a_{n-1} + g(n)a_{n-2} + f(n),$$

onde $g(n)$ é uma função não nula; caso contrário, a recorrência será de primeira ordem. Além disso, se $f(n) = 0$ a recorrência é dita *homogênea*; caso contrário, será não-homogênea.

Quando $h(n)$ e $g(n)$ são constantes e $f(n) = 0$, a relação de recorrência assume a forma

$$a_n = pa_{n-1} + qa_{n-2}$$

Ou ainda,

$$a_n - pa_{n-1} - qa_{n-2} = 0$$

A cada relação de recorrência da forma acima podemos associar uma equação do segundo grau $t^2 - pt - q = 0$, chamada *equação característica*.

Observação 4.7.1. *Se t_1 e t_2 com $t_1 \neq t_2$ e $t_1, t_2 \neq 0$ são raízes da equação característica $t^2 - pt - q = 0$, então todas as soluções da recorrência $a_n - pa_{n-1} - qa_{n-2} = 0$ são da forma $x_n = c_1 t_1^n + c_2 t_2^n$ com c_1 e c_2 constantes.*

Observação 4.7.2. *Se $t_1 = t_2 = t \neq 0$ são raízes da equação característica $t^2 - pt - q = 0$, então todas as soluções da recorrência $a_n - pa_{n-1} - qa_{n-2} = 0$ são da forma $x_n = c_1 t^n + c_2 n t^n$ com c_1 e c_2 constantes.*

Proposição 4.7.1. *Seja $x^2 - Dy^2 = 1$ a Equação de Pell para um certo valor D. Sejam x' e y' os menores valores não nulos que satisfazem a equação e $(a_0, b_0) = (1, 0)$ a solução trivial para todo D. Sejam ainda, (a_n) e (b_n) sequências tais que $a_n = 2x'.a_{n-1} - a_{n-2}$ e $b_n = 2x'.b_{n-1} - b_{n-2}$. Se $a_1 = x'$ e $b_1 = y'$, então, o par ordenado (a_n, b_n) é solução da equação de Pell para todo $n \in \mathbb{N}$.*

(Fonte: Pereira (2014, p. 30-31))

Demonstração. Tanto $a_n = 2x'.a_{n-1} - a_{n-2}$ como $b_n = 2x'.b_{n-1} - b_{n-2}$ têm como equação característica $t^2 - 2x't + 1 = 0$, cujas raízes são $t_1 = x' + \sqrt{(x')^2 - 1}$ e $t_2 = x' - \sqrt{(x')^2 - 1}$.

Mas, como x' e y' são soluções da *equação de Pell*, então $(x')^2 - 1 = D(y')^2$ e, portanto, podemos escrever $t_1 = x' + y'\sqrt{D}$ e $t_2 = x' - y'\sqrt{D}$.

Assim, pela **Observação 4.7.1** as soluções são da forma: $a_n = c_1.t_1^n + c_2.t_2^n$ e $b_n = d_1.t_1^n + d_2.t_2^n$.

Com as expressões de a_0 e a_1 montamos o sistema:

$$\begin{cases} c_1 + c_2 = 1 \\ (x' + y'\sqrt{D})c_1 + (x' - y'\sqrt{D})c_2 = x' \end{cases}$$

que nos fornece os coeficientes $c_1 = c_2 = \frac{1}{2}$ para (a_n).

Portanto, a solução da recorrência é dada por

$$a_n = \frac{1}{2}\left[(x' + y'\sqrt{D})^n + (x' - y'\sqrt{D})^n\right].$$

Já com as expressões de b_0 e b_1 montamos o sistema:

$$\begin{cases} d_1 + d_2 = 0 \\ (x^{'} + y^{'}\sqrt{D})d_1 + (x^{'} - y^{'}\sqrt{D})d_2 = y^{'}, \end{cases}$$

que nos fornece os coeficientes $d_1 = \frac{1}{2\sqrt{D}}$ e $d_2 = -\frac{1}{2\sqrt{D}}$ para (b_n).

Portanto, a solução da recorrência é dada por

$$b_n = \frac{1}{2\sqrt{D}}\left[(x^{'} + y^{'}\sqrt{D})^n - (x^{'} - y^{'}\sqrt{D})^n\right].$$

Reescrevendo as soluções encontradas temos:

$$\begin{cases} 2a_n = (x^{'} + y^{'}\sqrt{D})^n + (x^{'} - y^{'}\sqrt{D})^n \\ 2b_n\sqrt{D} = (x^{'} + y^{'}\sqrt{D})^n - (x^{'} - y^{'}\sqrt{D})^n. \end{cases}$$

Somando as igualdades e em seguida subtraindo a segunda da primeira, obtemos:

$$2a_n + 2b_n\sqrt{D} = 2(x^{'} + y^{'}\sqrt{D})^n$$

e

$$2a_n - 2b_n\sqrt{D} = 2(x^{'} - y^{'}\sqrt{D})^n$$

Eliminando os fatores 2 e multiplicando uma expressão pela outra encontramos:

$$(a_n + b_n\sqrt{D})(a_n - b_n\sqrt{D}) = ((x^{'})^2 - D(y^{'})^2)^n$$

E finalmente:

$$a_n^2 - Db_n^2 = 1$$

□

A **Proposição 4.7.1** considera o par ordenado $(a_n, b_n)_{n\in\mathbb{N}}$ como solução para *equação de Pell*, onde (a_n) e (b_n) são sequências tais que $a_n = 2x^{'}.a_{n-1} - a_{n-2}$ e $b_n = 2x^{'}.b_{n-1} - b_{n-2}$.

A proposição seguinte mostra que as sequências (a_n) e (b_n) satisfazem (4.10).

Proposição 4.7.2. *Seja $a+b\sqrt{d}$ a solução fundamental da equação de Pell $x^2 - dy^2 = 1$. Se $\{(x_n, y_n)\}_{n\in\mathbb{N}}$ é a sequência de soluções da equação, então*

$$x_{n+2} = 2ax_{n+1} - x_n$$
$$y_{n+2} = 2ay_{n+1} - y_n,$$

para todo $n \geq 1$.

(Fonte: Moreira, Martínez e Saldanha (2012, p. 213-214))

Demonstração. Temos que a sequência de soluções satisfaz a recorrência $\begin{cases} x_{n+1} = ax_n + dby_n \\ y_{n+1} = bx_n + ay_n \end{cases}$

Assim, temos que

$$\begin{aligned} x_{n+2} &= ax_{n+1} + dby_{n+1} \\ &= ax_{n+1} + db(bx_n + ay_n) = ax_{n+1} + db^2x_n + a(dby_n) \\ &= ax_{n+1} + db^2x_n + a(x_{n+1} - ax_n) = 2ax_{n+1} - (a^2 - db^2)x_n \\ &= 2ax_{n+1} - x_n. \end{aligned}$$

Por outro lado,

$$\begin{aligned} y_{n+2} &= bx_{n+1} + ay_{n+1} \\ &= b(ax_n + dby_n) + ay_{n+1} \\ &= a(bx_n) + db^2y_n + ay_{n+1} \\ &= a(y_{n+1} - ay_n) + b^2dy_n + ay_{n+1} \\ &= 2ay_{n+1} - (a^2 - db^2)y_n \\ &= 2ay_{n+1} - y_n \end{aligned}$$

□

A **Proposição 4.7.1** considera que x' e y' são os menores valores não nulos que satisfazem a *equação de Pell*, mas não mostra como encontrar tal solução.

O nosso objetivo, agora, é mostrar como encontrar a solução minimal (fundamental) da *equação de Pell*. Antes, porém, inspirados nas ideias de Santos (2003), faremos uma breve introdução sobre *frações contínuas*.

4.7.0.2 Frações Contínuas

Inicialmente, observemos que o número racional $\frac{79}{28}$ pode ser expresso da seguinte forma

$$\begin{aligned} \frac{79}{28} &= 2 + \frac{23}{28} = 2 + \frac{1}{\frac{28}{23}} = 2 + \frac{1}{1 + \frac{5}{23}} = 2 + \frac{1}{1 + \frac{1}{\frac{23}{5}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{3}{5}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{\frac{5}{3}}}} \\ &= 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{2}{3}}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}} = 2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}. \end{aligned}$$

Dizemos que esta última expressão é a fração contínua que representa o número racional $\frac{79}{28}$, ou a expressão de $\frac{79}{28}$ sob a forma de fração contínua e a notação usada é $[2, 1, 4, 1, \overline{1, 2}]$.

De um modo geral, uma expressão da forma

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \ddots}}}}$$

é chamada de *fração contínua*, e será denotada por $[a_1, a_2, a_3, ...]$. Os números $a_1, a_2, ...$ são chamados de quocientes parciais.

Quando todos a_i são inteiros, dizemos que a fração contínua é *simples*. Como vamos nos restringir, apenas, ao caso de frações contínuas simples, a expressão "fração contínua" deverá ser entendida como "fração contínua simples".

Veremos, agora, um processo de obtenção de aproximações sucessivas por racionais, para um número irracional.

Seja α um irracional e seja $a_1 = \lfloor \alpha \rfloor$, isto é, a_1 é o maior inteiro menor do que α . Logo,

$$\alpha = a_1 + \frac{1}{x_1},$$

e, claramente, $x_1 = \dfrac{1}{\alpha - a_1}$ é irracional e $x_1 > 1$. Podemos, pois, escrever x_1 na forma

$$x_1 = a_2 + \frac{1}{x_2}$$

onde $a_2 = \lfloor x_1 \rfloor$, x_2 é irracional e $x_2 > 1$. Podemos repetir este processo, obtendo:

$$\begin{aligned} \alpha &= a_1 + \frac{1}{x_1} \\ x_1 &= a_2 + \frac{1}{x_2} \\ x_2 &= a_3 + \frac{1}{x_3} \\ &\vdots \\ x_n &= a_{n+1} + \frac{1}{x_{n+1}} \end{aligned} \tag{4.11}$$

onde todos $a_i\,(i > 1)$ são inteiros maiores ou iguais a 1 e todos x_i são irracionais maiores do que 1. O fato de cada x_i ser irracional nos garante que este processo pode ser repetido um número qualquer de vezes. Utilizando as equações (4.11) vemos que

$$\alpha = a_1 + \frac{1}{x_1} = a_1 + \frac{1}{a_2 + \frac{1}{x_2}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{x_3}}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{x_4}}}}.$$

Definimos $[a_1, a_2, a_3, ...] = \lim\limits_{n\to\infty} [a_1, a_2, a_3, ..., a_n]$.

Vamos ilustrar este processo obtendo a expansão de $\sqrt{3}$.

Sendo $a_1 = \left\lfloor \sqrt{3} \right\rfloor = 1$ e

$$\sqrt{3} = a_1 + \frac{1}{x_1} = 1 + \frac{1}{x_1}$$

temos:

$$x_1 = \frac{1}{\sqrt{3}-1} = \frac{1}{(\sqrt{3}-1)}\frac{(\sqrt{3}+1)}{(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

Consequentemente,

$$\sqrt{3} = 1 + \frac{1}{x_1} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}}.$$

Como $a_2 = \left\lfloor \frac{\sqrt{3}+1}{2} \right\rfloor = 1$, temos $\frac{\sqrt{3}+1}{2} = 1 + \frac{1}{x_2}$, donde obtemos

$$x_2 = \frac{1}{\frac{\sqrt{3}+1}{2} - 1} = \sqrt{3} + 1$$

Logo, $\sqrt{3} = 1 + \frac{1}{x_1} = 1 + \frac{1}{1 + \frac{1}{x_2}} = 1 + \frac{1}{1 + \frac{1}{\sqrt{3}+1}}$

Como $a_3 = \left\lfloor \sqrt{3} + 1 \right\rfloor = 2$, temos

$$\sqrt{3} + 1 = x_2 = a_3 + \frac{1}{x_3} = 2 + \frac{1}{x_3}.$$

Resolvendo esta última equação para x_3 obtemos:

$$x_3 = \frac{1}{(\sqrt{3}+1-2)} = \frac{\sqrt{3}+1}{2}$$

Sendo $x_3 = x_1$, concluímos que x_4 será igual a x_2 e, desta forma, continuando com este processo, iremos obter para a sequência $a_1, a_2, a_3, ...$ os valores $1, 1, 2, 1, 2, 1, 2, ...$ Logo, a fração contínua infinita representando $\sqrt{3}$ será dada por:

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, ...] = [1, \overline{1, 2}].$$

Chamamos *fração contínua periódica* a uma representação como esta em que uma sequência de números se repete periodicamente. Colocamos uma barra sobre a parte que se repete, que é chamada de *período* da fração contínua.

Fazem observar Andreescu, Andrica e Cucurezeanu (2010, p. 125-126) que o principal método para determinar a solução fundamental da *equação de Pell* $x^2 - Dy^2 = 1$ envolve frações contínuas.

Ela é obtida escrevendo $\sqrt{D}$ como uma fração contínua simples:

$$\sqrt{D} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

onde $a_0 = \left\lfloor \sqrt{D} \right\rfloor$ e $a_1, a_2, a_3, a_4, ...$ é uma sequência periódica de números inteiros positivos. Lembrando que a fração contínua é denotada por $[a_0, a_1, a_2, a_3, a_4, ...]$. O termo $k-$ésimo da sequência convergente $[a_0, a_1, a_2, a_3, a_4, ...]$ é o número

$$\frac{p_k}{q_k} = [a_0, a_1, a_2, a_3, a_4, ..., a_k]$$

com p_k, q_k primos relativos.

Seja $a_1, a_2, ..., a_m$ o período de $\sqrt{D}$. A solução fundamental (minimal) da *equação de Pell* aparece como

$$(x_1, y_1) = \begin{cases} (p_{m-1}, q_{m-1}) & \text{se } m \text{ é par} \\ (p_{2m-1}, q_{2m-1}) & \text{se } m \text{ é ímpar} \end{cases}$$

Por exemplo,

$$\sqrt{3} = [1, 1, 2, 1, 2, ...] = [1, \overline{1, 2}],$$

Como $m = 2$; daí, $(p_{2-1}, q_{2-1}) = (p_1, q_1)$; portanto $[1, 1] = 1 + \frac{1}{1} = \frac{2}{1} = \frac{p_1}{q_1}$. Ou seja, $(x_1, y_1) = (2, 1)$ é a solução fundamental (minimal) de $x^2 - 3y^2 = 1$. Observemos que $2^2 - 3.1^2 = 1$.

Para

$$\sqrt{2} = [1, 2, 2] = [1, \overline{2}],$$

temos $m = 1$; daí, $(p_{2.1-1}, q_{2.1-1}) = (p_1, q_1)$; portanto, $[1, 2] = 1 + \frac{1}{2} = \frac{3}{2} = \frac{p_1}{q_1}$. Ou seja, $(x_1, y_1) = (3, 2)$ é a solução fundamental (minimal) de $x^2 - 2y^2 = 1$. Observemos que $3^2 - 2.2^2 = 1$.

Consideramos útil incluir uma tabela contendo as soluções fundamentais da *equação de Pell* $x^2 - Dy^2 = 1$ para $D \leq 103$.

Tabela 2 – Soluções fundamentais para a *equação de Pell,* $D \leq 103$.

D	u_1	v_1	D	u_1	v_1	D	u_1	v_1
2	3	2	38	37	6	71	3480	413
3	2	1	39	25	4	72	17	2
5	9	4	40	19	3	73	2281249	267000
6	5	2	41	2049	320	74	3699	430
7	8	3	42	13	2	75	26	3
8	3	1	43	3482	531	76	57799	6630
10	19	6	44	199	30	77	351	40
11	10	3	45	161	24	78	53	6
12	7	2	46	24335	3588	79	80	9
13	649	180	47	48	7	80	9	1
14	15	4	48	7	1	82	163	18
15	4	1	50	99	14	83	82	9
17	33	8	51	50	7	84	55	6
18	17	4	52	649	90	85	285769	30996
19	170	39	53	66249	9100	86	10405	1122
20	9	2	54	485	66	87	28	3
21	55	12	55	89	12	88	197	21
22	197	42	56	15	2	89	500001	53000
23	24	5	57	151	20	90	19	2
24	5	1	58	19603	2574	91	1574	165
26	51	10	59	530	69	92	1151	120
27	26	5	60	31	4	93	12151	1260
28	127	24	61	1766319049	226153980	94	2143295	221064
29	9801	1820	62	63	8	95	39	4
30	11	2	63	8	1	96	49	5
31	1520	273	65	129	16	97	62809633	6377352
32	17	3	66	65	8	98	99	10
33	23	4	67	48842	5967	99	10	1
34	35	6	68	33	4	101	201	20
35	6	1	69	7775	936	102	101	10
37	73	12	70	251	30	103	227528	22419

Fonte: Andreescu, Andrica e Cucurezeanu (2010, p. 127).

Exemplo 4.7.1. *Resolva a equação* $x^2 - 6y^2 = 1$.

Resolução. Inicialmente, devemos encontrar a solução fundamental da equação dada. Assim,

$$\begin{aligned} a_0 &= \left\lfloor \sqrt{6} \right\rfloor = 2 \\ x_0 &= \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} \\ a_1 &= \left\lfloor \frac{\sqrt{6}+2}{2} \right\rfloor = 2 \\ x_1 &= \frac{1}{\left(\frac{\sqrt{6}+2}{2}\right)-2} = \sqrt{6}+2 \\ a_2 &= \left\lfloor \sqrt{6}+2 \right\rfloor = 4 \\ x_2 &= \frac{1}{(\sqrt{6}+2)-4} = \frac{\sqrt{6}+2}{2} = x_0 \end{aligned}$$

Como $x_2 = x_0$, vemos que $a_3 = a_1, a_4 = a_2, a_5 = a_1, a_6 = a_2, ...$ Logo,

$$\sqrt{6} = [2, 2, 4, 2, 4, ...] = [2, \overline{2, 4}].$$

Agora, como $m = 2$, temos $(p_{2-1}, q_{2-1}) = (p_1, q_1)$; daí, $[2, 2] = 2 + \frac{1}{2} = \frac{5}{2} = \frac{p_1}{q_1}$. Ou seja, $(x_1, y_1) = (5, 2)$ é a solução fundamental da equação dada (Vide Tabela 2, D=6). Observemos que $5^2 - 6.2^2 = 1$.

Portanto, pela **Proposição 4.7.1**, temos:

$$\begin{aligned} a_n &= \frac{1}{2}\left[(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n\right] = \frac{1}{2}\left[(5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n\right] \\ b_n &= \frac{1}{2\sqrt{D}}\left[(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n\right] = \frac{1}{2\sqrt{6}}\left[(5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n\right] \end{aligned}$$

Fazendo n variar, obtemos:

$$a_n = (1, 5, 49, 485, 4801, ...) \quad \text{e} \quad b_n = (0, 2, 20, 198, 1960, ...)$$

Portanto, as soluções procuradas são $\{(1, 0), (5, 2), (49, 20), (485, 198), (4801, 1960), ...\}$.

5 CONSIDERAÇÕES FINAIS

No decorrer deste trabalho, principalmente nos capítulos 3 e 4, foi possível observar que o tema abordado possui grande importância na Educação Básica, uma vez que as Equações Diofantinas Lineares e Não Lineares possuem uma infinidade de aplicações, inclusive nas geometrias plana e analítica, que são assuntos abordados na Educação Básica.

Neste trabalho, apresentamos diversos métodos de resolução de Equações Diofantinas lineares em duas e três incógnitas. Para tanto, utilizamos conceitos de divisibilidade, divisão euclidiana, máximo divisor comum, múltiplos e divisores, valor absoluto, paridade, números primos entre si, dentre outros, que são assuntos que fazem parte do currículo do Ensino Fundamental.

Destacamos a importância do primeiro capítulo, que aborda as contribuições de Diofanto para a história da Matemática, devido à abertura de novos horizontes, que serviu de incentivo e inspiração para um melhor entendimento da importância da matemática atual, em particular a álgebra, pois foi Diofanto o pioneiro no desenvolvimento da notação algébrica em que algumas operações eram representadas por suas abreviações. A propósito, muitos historiadores consideram-no o “Pai da Álgebra”. Embora não tenha sido o primeiro a trabalhar com equações indeterminadas, ou a resolver equações quadráticas de forma não geométrica, podemos considerar que Diofanto foi o primeiro a iniciar os passos rumo a uma estrutura da simbologia algébrica que estudamos hoje.

Pelos assuntos abordados, destacamos a importância desse conteúdo, que poderia estar no currículo da Educação Básica, pois a base necessária para trabalhá-lo é vista desde o Ensino Fundamental. As Equações Diofantinas Lineares com duas e três variáveis podem ser estudadas a partir dos últimos anos do Ensino Fundamental. No Ensino Médio, seriam vistas as Equações Diofantinas não lineares por meio dos métodos da fatoração, Geométrico, Aritmético, dentre outros.

As Equações Diofantinas constituem um campo propício para investigação matemática. Existem diversas situações-problema que permitem aplicar a teoria aqui estudada. Ainda que as Equações Diofantinas não sejam exploradas na Educação Básica, são perfeitamente passíveis de compreensão nesse nível, exigindo apenas o domínio de assuntos abordados no Ensino Fundamental.

Alunos que estão em preparação para as Olimpíadas de Matemática encontrarão aqui, neste trabalho, uma importante fonte de pesquisa.

Por fim, desejamos que esta pesquisa possa contribuir para uma melhor compreensão do tema Equações Diofantinas e que estas possam ser aplicadas na Educação Básica, ajudando alunos e professores a aprimorarem seus conhecimentos.

REFERÊNCIAS

ALENCAR FILHO, E. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981. Citado 2 vezes nas páginas 102 e 103.

ALENCAR FILHO, E. **Teoria das Congruências**. São Paulo: Nobel, 1986. Citado 9 vezes nas páginas 69, 70, 71, 72, 73, 74, 75, 77 e 82.

ALENCAR FILHO, E. **Aritmética dos Inteiros**. São Paulo: Nobel, 1987. Citado 45 vezes nas páginas 27, 28, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 61, 62, 63, 64, 65, 68, 69, 85, 86, 87, 88, 89, 90, 91, 92, 93 e 94.

ANDREESCU, T.; ANDRICA, D.; CUCUREZEANU, I. **An Introduction to Diophantine Equations**: A problem-based approach. Moscú: Birkhäuser, 2010. Citado 16 vezes nas páginas 104, 116, 117, 118, 119, 127, 128, 129, 130, 131, 132, 133, 135, 141, 147 e 149.

BASHMAKOVA, I. G. **Diofanto y las Ecuaciones Diofánticas**. Moscú: Krasand, 2015. Citado 3 vezes nas páginas 15, 22 e 23.

BOYER, C. B. **História da Matemática**. 3. ed. São Paulo: Blucher, 2010. Citado 2 vezes nas páginas 23 e 24.

EVES, H. **Introdução à História da Matemática**. São Paulo: Unicamp, 2004. Citado 2 vezes nas páginas 15 e 16.

FEITOSA, S. B. **Curso de Teoria dos Números-Nível2**. 2012. Disponível em: <http://poti.impa.br>. Acesso em: 2 dez. 2015. Citado 8 vezes nas páginas 76, 78, 79, 80, 81, 101, 110 e 134.

FERREIRA, J. **A Construção dos Números**. 3. ed. Rio de Janeiro: SBM, 2013. Citado na página 27.

GARBI, G. G. **A Rainha das Ciências**: Um passeio histórico pelo maravilhoso mundo da matemática. 3. ed. São Paulo: Livraria da Física, 2009a. Citado 2 vezes nas páginas 15 e 16.

GARBI, G. G. **O Romance das Equações Algébricas**. 3. ed. São Paulo: Livraria da Física, 2009b. Citado 3 vezes nas páginas 17, 19 e 21.

GUELFOND, A. . **Resolución de Ecuaciones en Números Enteros**. 5. ed. Moscú: Krasand, 2010. Citado na página 137.

HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro: SBM, 2013. Citado 36 vezes nas páginas 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 41, 42, 44, 45, 47, 49, 50, 51, 53, 56, 59, 61, 62, 63, 66, 67, 68, 69, 75, 76, 77, 78, 82, 83 e 84.

LIMA, R. A. **Utilizando a História na Matemática no Ensino de Equação do 2º Grau.** 2011. 37p. Monografia (Graduação)-Universidade Federal da Paraíba, Itaporanga, PB, 2011. Citado na página 19.

MARTíNEZ, F. B. et al. **teoria dos números**: um passeio com primos e outros números familiares pelo mundo inteiro. 2. ed. Rio de Janeiro: IMPA, 2013. Citado 2 vezes nas páginas 114 e 141.

MOREIRA, C. G. T. A.; MARTíNEZ, F. E. B.; SALDANHA, N. C. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012. Citado 14 vezes nas páginas 115, 116, 120, 121, 122, 123, 124, 125, 126, 127, 130, 138, 139 e 144.

MUNIZ NETO, A. C. **Tópicos de Matemática Elementar**. 2. ed. Rio de Janeiro: SBM, 2012. Citado 4 vezes nas páginas 133, 135, 136 e 138.

NASCIMENTO, M. C.; FEITOSA, H. A. **Elementos da Teoria dos Números**. 2013. Disponível em: <http://wwwp.fc.unesp.br/~mauri/TN/TN.pdf>. Acesso em: 13 jun. 2016. Citado na página 137.

OLIVEIRA, S. B. **As Equações Diofantinas Lineares e o Livro Didático de Matemática para o Ensino Médio**. Dissertação (Mestrado) — Pontifícia Universidade Católica de São Paulo, São Paulo, 2006. Citado na página 25.

PEREIRA, M. V. **Recorrências – Problemas e Aplicações**. Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2014. Citado na página 143.

POLYA, G. **A Arte de Resolver Problemas**. Rio de Janeiro: Interciência, 1995. Citado na página 12.

POMMER, S. V.; POMMER, C. P. C. R. Equações diofantinas lineares: um viés histórico epistemológico como recurso para introduzir diferentes estratégias de resolução de problemas. **REnCiMa**, v. 3, n. 1, p. 28–43, jan./jul. 2012. Citado na página 25.

RIBEIRO, R. **Equações Diofantinas**: uma abordagem para o ensino médio. Dissertação (Mestrado) — Universidade de Brasília, Brasília, 2014. Citado na página 25.

ROQUE, T. **História da Matemática**: uma visão crítica, desfazendo mitos e lendas. 3. ed. Rio de Janeiro: Zahar, 2012. Citado 3 vezes nas páginas 17, 18 e 19.

SANTOS, J. P. O. **Introdução à Teoria dos Números**. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003. Citado na página 145.

SAVóIS, J. N.; FREITAS, D. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. **Ciência e Natura**, v. 37, p. 47–57, 2015. Ed. Especial PROFMAT. Citado na página 25.

VERA, O. A. B. **Ecuaciones diofánticas**: Teoría y práctica. 1. ed. Lima: Asociación Fondo de Investigadores y Editores, 2014. Citado 11 vezes nas páginas 12, 94, 95, 96, 98, 99, 107, 108, 109, 111 e 112.

ZERHUSEN, A.; RAKES, C.; MEECE, S. **Diophantine Equations**. 1999. Disponível em: <http://www.ms.uky.edu/~carl/ma330/projects/diophanfin1.html>. Acesso em: 2 jan. 2015. Citado na página 25.