Universidade Federal do Pará
Instituto de Ciências Extas e Naturais
Programa de Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Andrey Uchôa Fernandes

Um breve comentário sobre números inteiros - Equações Diofantinas e Aplicações

Brasil

2021

Andrey Uchôa Fernandes

Um breve comentário sobre números inteiros - Equações Diofantinas e Aplicações

Dissertação apresentada, como requisito parcial, para obtenção do título de Mestre em Matemática do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, sob orientação do Prof. Dr. Augusto César dos Reis Costa

Brasil

2021

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

U17b Uchôa, Andrey.
Um breve comentário sobre números inteiros : Equações Diofantinas e Aplicações / Andrey Uchôa. — 2021.
50 f. : il.

Orientador(a): Prof. Dr. Augusto Costa
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Exatas e Naturais, Programa de Pós-Graduação em Matemática em Rede Nacional, Belém, 2021.

1. Equações Diofantinas Lineares. 2. Máximo Divisor Comum. 3. Aritmética. 4. Teoria dos Números. I. Título.

CDD 372.13

Andrey Uchôa Fernandes

Um breve comentário sobre números inteiros - Equações Diofantinas e Aplicações

Dissertação apresentada, como requisito parcial, para obtenção do título de Mestre em Matemática do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, sob orientação do Prof. Dr. Augusto César dos Reis Costa
Resultado: Aprovado

Brasil, 22 de Abril de 2021:

BANCA EXAMINADORA

Prof. Dr. Augusto César dos Reis Costa. (UFPA)
Orientador

Andréia Gomes Pinheiro

Prof. Dra. Andréia Gomes Pinheiro. (IFPA)

Prof. Dr. Geraldo Mendes de Araújo. (UFPA)

Prof. Dr. Sebastião Martins Siqueira Cordeiro.(UFPA)

Brasil
2021

Este trabalho é dedicado a minha mãe Danielle Angelica Uchôa Lima que, fez bem mais que a sua obrigação.

Agradecimentos

Quero, primeiramente, a agradecer a Deus, pela força que me foi dada, saúde, minha e dos meus queridos. À minha família, por sempre me apoiar no caminho da educação. Quero agradecer à minha esposa, Romena Andréia Charchar Campos Marques, sou eternamente grato por ela estar sempre ao meu lado, apoiando-me.

Agradeço ao meu orientador, prof. Dr. Augusto César dos Reis Costa, pelas contribuições que tornaram este trabalho melhor a cada nova sugestão.

A Universidade Federal do Pará devo agradecer, por sempre receber novos estudantes com braços abertos, sempre com o propósito de tornar cada discente um profissional melhor, criando programas que melhoram a qualidade dos profissionais nas mais diversas áreas, e mais específicamente, nessa qualificação de professores de Matemática.

Agradecer também aos amigos que a educação me proporcionou, principalmente, Mestre Márcio Pinheiro, a pessoa que me deu o primeiro impulso para estar aqui, concluindo este mestrado. Agradecer ao grande amigo Mestre Henrique Maia, sem a sua parceria e conhecimento, não sei se conseguiria chegar ao fim, devido aos percalços no caminho do mestrado.

E o meu principal agradecimento vai para minha mãe, Danielle Angélica Uchôa Lima, sem ela, nada teria acontecido. Muito obrigado mãe, te amo muito.

"Ainda que eu andasse pelo vale da sombra da morte,
não temeria mal algum, porque tu estás comigo;
a tua vara e o teu cajado me consolam.
(Bíblia Sagrada, Salmos 23:4)

Resumo

Este trabalho é voltado para alunos e professores que atuam no ensino básico. Tem como objetivo comentar alguns tópicos do conjunto dos números inteiros e algumas de suas aplicações, com o foco em equações diofantinas linerares. A motivação de escolher esse tema é que o conteúdo de números inteiros é lecionado no ensino básico, entretanto alguns assuntos que os cercam, são deixados de lado, assim também como algumas propriedades e demonstrações que são acessíveis aos alunos, e são deixadas de lado. Este trabalho tem o intuito de ajudar a sanar essas lacunas que são muito requisitadas quando falamos de provas de olimpíadas de matemática e concursos militares. Neste trabalho serão comentados alguns tópicos de números inteiros e após serão resolvidos e comentados alguns problemas corriqueiros envolvendo às equações diofantinas lineares.

Palavras-chave: Teoria dos números. Aritmética. Equações diofantinas lineares. Ensino da matemática.

Abstract

This work is aims to students and teachers who work in basic education. It aims to comment on some topics in the set of integers and some of their applications, with a focus on linear Diophantine equations. The motivation for choosing this theme is that the content of whole numbers is taught in basic education, however some subjects that surround them are left out, as well as some properties and demonstrations that are accessible to students, and for unknow reason are not taught. This work is intended to fill those gaps that are very requested when we talk about olympics mathematics tests and military tests. In this paper, some integer topics will be commented and then some common problems involving linear Diophantine equations will be solved and commented.

Keywords: Number theory. Arithmetic. Diophantine linear equations. Mathematics teaching.

Sumário

Lista de ilustrações

Introdução

Dentre as diversas funções que um professor tem, uma das que mais se destaca é a de dar sentido ao ensino, o porquê daquilo ser ensinado, e a de um professor de matemática não é diferente, deve-se esclarecer aos alunos quanto às expressões algébricas, gráficos, tabelas e etc.

A ideia de escolher as equações diofantinas lineares como tema da dissertação, não se deu de uma hora para a outra. A primeira vez que estudei esta teoria foi na minha graduação, em seguida, na minha pós-graduação, me aprofundei um pouco mais neste assunto. Passado o tempo, comecei a lecionar para turmas de olimpíadas e turmas preparatórias para concursos militares e constatei que este assunto não deveria ser ministrado exclusivamente no ensino superior, mas também no ensino básico. Contudo, não é comum ser ensinado nele, a não ser nestas turmas específicas, foi com o propósito de criar um material que ajude os alunos que estão iniciando em turmas de olimpíadas e preparatórias para concursos militares que foi elaborada esta dissertação.

Serão apresentadas algumas definições acerca do conjunto dos números inteiros, tais como suas propriedades, proposições, lemas, teoremas e consequências. Assim como também será comentado, brevemente, sobre divisibilidade, definição e propriedades (demonstradas, visando a compreensão do aluno) de uma forma elegante e clara, expondo os principais tópicos de modo que o aluno que se prepara para as provas de olimpíadas e de concursos militares, possa usar este material como apoio.

O seguinte trabalho tem como objetivo a estruturação deste material, para que o mesmo seja visto pelo aluno como algo interessante e relevante, e assim o use para estudar e compreender melhor os assuntos que as equações diofantinas se baseiam. Visto que essas equações possibilitam vários caminhos distintos para resolução dos problemas, serão apresentados diferentes métodos aplicados em alguns problemas, junto com a teoria por trás deles.

No primeiro capítulo, vai ser um breve comentário histórico sobre a construção do conjunto dos números inteiros, destacando a história e descobertas matemáticas de Diofanto de Alexandria (250a.c - 350a.c), o matemático que muito ajudou na construção algébrica, e nos problemas envolvendo aritmética. Pouco se sabe da vida deste matemático, contudo, se tem profundo conhecimento da sua obra "Arithmética", na qual são citados vários problemas matemáticos, dentre as descobertas dele. Sendo que uma delas que será norte deste trabalho, que são as Equações diofantinas lineares (a tendência metodológica História da matemática, é uma forma bem interessante de começar alguns assuntos), em seguida será exposto algumas propriedades do conjunto dos números inteiros, como ele

se organiza e suas proposições. Após, será explicado sobre quem são os números primos e alguns de seus principais tópicos e definições. Posteriormente, será exposto o assunto Máximo Divisor Comum, citando observações, teoremas, lemas e propriedades e suas consequências aritméticas. Finalizando o capítulo com o Mínimo Múltiplo Comum.

É válido comentar também, que é possível resolver muitos problemas de equações diofantinas por congruência aritmética, mas neste trabalho a preferência não será ela, visto que é um tópico um pouco mais avançado, apesar de ser um assunto que também é visto no ensino militar. O foco do trabalho, de modo geral, é solucionar alguns problemas de equações diofantinas lineares com a matemática mais básica possível. No segundo capítulo, que versa sobre as equações diofantinas, expondo a definição, sua condição de existência, assim como suas soluções se dão, terminando o trabalho com alguns problemas clássicos de equações diofantinas lineares. Nesta parte do trabalho serão resolvidas cada questão de uma forma diferente da outra, para que o leitor saiba que existem diversos cominhos a se seguir para chegar no resultado devido, e o próprio possa decidir qual ache mais interessante, ou até mesmo, optar por resolver uma questão por algum outro método que foi usado na questão, como forma de estudo.

Este trabalho é destinado para os estudantes dos anos finais do ensino fundamental II, ao ensino médio (principalmente aos alunos que participam das turmas de olimpíadas de matemática e a alunos que estão em turmas preparatória para concursos militares). Este material também pode servir de auxílio para alunos da graduação, pois que ele é visto em teoria dos números. O objetivo é sempre ajudar os discentes que procuram auxílio no momento do estudo.

1 Um breve comentário sobre Números Inteiros

1.1 Resumo Histórico

A construção do conjunto dos números inteiros não se deu de forma rápida ou fácil, esses números só tiveram sua organização e aceitação da maioria dos grupos de matemáticos já na idade contemporânea.

Segundo Sá e Anjos a trajetória dos números pode ser dívidida em duas categorias: Uma que tem sua origem por motivação externa ou das atividades de contagem e medida e outra que tem origem interna ou das necessidades da própria matemática.

O conjunto chamado de inteiro, representado pela letra $\mathbb{Z}$ (Zahlen: números, em alemão), formado pelos números naturais e seus respectivos opostos, sendo escrito da seguinte forma:

$$\mathbb{Z} = \{..., -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ ...\}.$$

Voltando há milhares de anos, nos primórdios da humanidade, a necessidade de contar já se fazia necessária, agrupar pedras, riscos em ossos, entalhes na madeira e marcas em cavernas mostram tal necessidade.

Com a não existência formal dos números, várias formas de representar foram criadas, como por exemplo: Um pastor de ovelhas que sai pra passear com os seus animais, mas para não voltar com menos ovelhas que saiu, fazia uma espécie de bijeção com pedrinhas, associando cada pedrinha a uma ovelha, assim voltando para casa e verificando se a quantidade (embora não existisse esse conceito bem definido) de pedrinhas formava pares com as ovelhas. Curiosamente a palavra Calculus significa pedras, ou seja, as pedras que eles utilizavam para contar ovelhas. De outro modo, para uma quantidade muito grande de ovelhas seria muito complicado a utilização de pedrinhas, surgindo então a necessidade de fazer agrupamentos, ou seja, a noção primitiva de Conjunto.

E assim, diversas outras formas criativas de contagens foram surigindo, primitivas, mas que funcionavam para as necessidades dos habitantes da época. Outro método de contagem, muito comum, era riscar ossos para representação de animais mortos em uma caçada, por exemplo.

A figura 1 mostra um osso talhado descoberto por volta de 1950 que foi datado do período Paleolítico Superior da história humana, aproximadamente 20.000-25.000 anos atrás. O osso, provavelmente a fíbula de um babuíno, gato grande ou outro grande mamífero, feito vários riscos representando quantidades.

Figura 1 – Riscos em ossos representando quantidades.

Fonte: https://www.maa.org/ Acessado: 22:05 08/04/2021.

Para Aristóteles, todo homem deseja naturalmente saber, a partir daí, conjecturou que é inato do ser humano a necessidade de descobrir padrões e tentar organiza-los, talvez dessa necessidade tenha nascido a matemática, com os primeiros conceitos de quantidades, números e organização.

Diversas civilizações criaram suas representações para quantidades, como os romanos, egípcios, astecas e várias outras, destacando-se os hindus e os árabes com a primeira noção dos chamados algarismos hindo-arábicos, que possuem esse nome por terem sido criados pelos hindus e divulgados pelos arábes, e, por sua facilidade para representar grandes quantidades, em um pequeno espaço, são os mais conhecidos e utilizados pelas sociedades ao longo do tempo, perdurando até a atualidade, sendo esses:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Esses algarismos podem informar infinitas quantidades com suas combinações organizados num sistema numérico posicional, veja nesses exemplos:

$$234$$

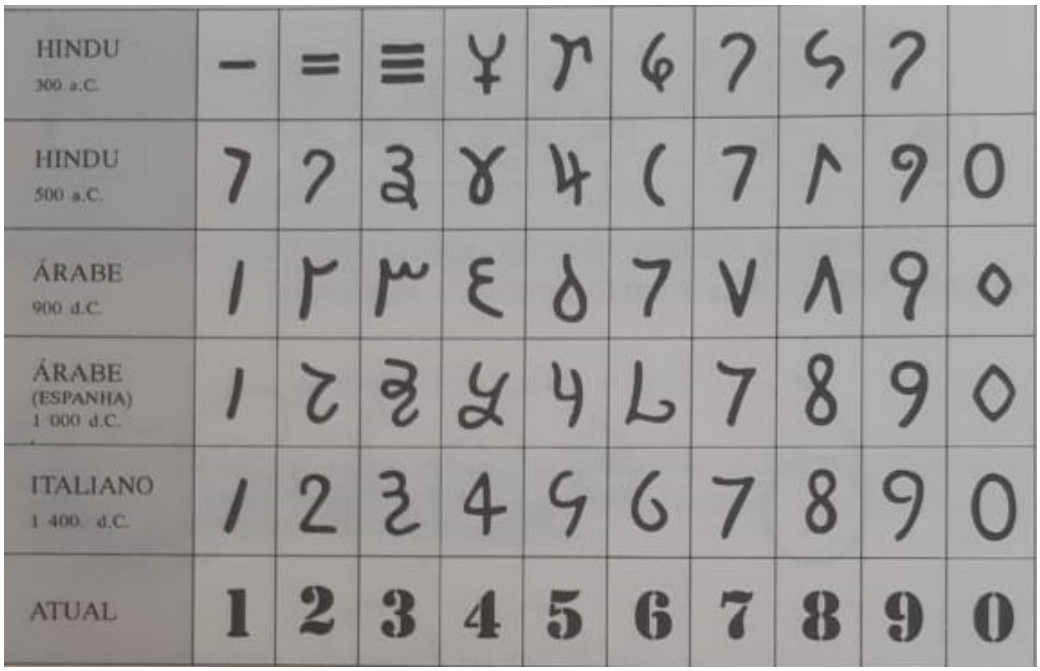
$$243$$

$$432.$$

Perceba que os mesmos algarismos foram utilizados na formação de 3 números, entretanto como estes algarismos estão em posições diferente, os números formados são

diferentes entre sí. Outra curiosidade é que tais algarismos não nasceram no formato que utilizamos hoje em dia, houve uma evolução na escrita destes, conforme mostra a Figura 2.

Figura 2 – Figura Construção dos algarismos Hindus-Arábicos.



Fonte: Centurión, Marilia. "Conteúdo e metodologia da matemática: números e operações."São Paulo: Scipione (1994).

No desenvolvimento da civilização, é perceptível que o uso dos números positivos acaba se limitando a certos problemas, sendo necessário criar outro sistema numérico, ou adaptar o já existente, para resolver diversas situações que podem ocorrer. Podemos encontrar relatos que a origem dos números inteiros não se deu somente a partir de uma única civilização, mas sim em diversos povos, como os egípcios, chineses hindus e outros, que encontraram maneiras diferentes de representar os números negativos.

Um exemplo da necessidade desses números é: Um vendedor A de certo produto, tem que ter produtos em sua loja para comercializar e tirar o seu sustento, entretanto não possui condições de adquirir tais produtos para abrir, este então pede emprestado para o vendedor B, com a promessa de assim que fizer suas vendas pagará sua dívida com o vendedor B e com a esperança de sobrar uma pouco mais para sí, e poder sustentar sua família.

Ora, quando o vendedor A abre sua loja, já está com um prejuízo, e precisa com suas vendas quitar o prejuízo e a partir daí sim, conseguir algo a mais para o seu sustento. No momento da organização dos dados do que precisa vender para quitar o que deve, este vendedor pode representar a sua dívida de forma mais simples com os números negativos.

Também na construção da noção primitiva dos números inteiros, problemas ligados

ao dia a dia dos matemáticos chineses conduziria-os a sistemas de equações lineares, que era escrito na forma de matriz dos coeficientes. A solução era dada pelo que nós chamamos hoje de: *tranformações de matrizes*. É nestas matrizes que encontramos pela primeira vez na história da matemática a presença dos números negativo.

No entanto, de acordo com (FOSSA; ANJOS, 2007) durante os primeiro mil anos da era cristã os chineses não concebiam o número negativo como entidades matemática independentes.

O números Hindu-Arábicos são posicionais, onde cada posição representa algo, da direita para a esquerda temos as classes numéricas, elas são: classe de unidade, classe de milhar, classe de milhão, classe de bilhão e assim por diante, e cada uma dessas classes são subdivididas em outras 3, ordens, a primeira (da direita para a esquerda) é a ordem das unidades, a segunda das dezenas e a terceira das centenas.

Exemplo de tabela de classes numéricas

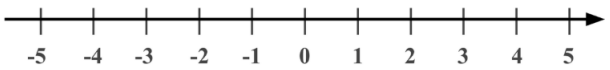
3ª Classe : Milhão			**2ª Classe: Milhar**			**1ª Classe: Unidades**		
9ª Ordem	8ª Ordem	7ª Ordem	6ª Ordem	5ª Ordem	4ª Ordem	3ª Ordem	2ª Ordem	1ª Ordem
7	4	3	3	8	5	2	1	1

O número acima possui: Sete centenas de milhões, quatro dezenas de milhões, três unidades de milhões, três centenas de milhares, oito dezenas de milhares, cinco unidades de milhares, duas centenas, uma dezena e uma unidade. Lê-se: setecentos e quarenta e três milhões, trezentos e oitenta e cinco mil e duzentos e onze.

Segundo (BERLINGHOFF; GOUVÊA, 2008) a primeira civilização a desenvolver o uso do zero foi a civilização Hindu, que sentiu a necessidade de usá-lo quando se encontrava com a seguinte situação: O número 507, possui 5 centenas, ? dezenas e 7 unidades. Essa representação explicando a ausência numérica da casa das dezenas motivou o "descobrimento" deste número, que representa o vazio, a ausência de números.

Os números inteiros também podem estar organizados em uma reta numérica, como sugeriu o mátemático Colin McLaurin (1698 - 1756) para organizá-los de alguma forma, conforme ilustra a Figura 3.

Figura 3 – Números Inteiros ($\mathbb{Z}$).



A ideia básica é que o zero está no centro da reta numérica e quanto mais a direita está um número, maior ele é.

O conceito de número inteiro é quase tão antigo quanto o de número natural, visto

que esses números eram utilizados para resolver problemas de contagens e principalmente no desenvolvimento de atividades mercantis que aconteciam na Europa, na idade média, entretanto temos que considerar esses conceitos eram bem primitivos.

Nesse contexto surgiu a figura de Diofanto de Alexandria (250 a.c - 350 a.c), que comentarei em seguida um pouco mais sobre tal nobre matemático, mas na história da construção dos números negativos, também teve sua contribuição. Embora Diofanto tenha dado várias contribuições à algebra, ele não fez sequer referência aos números negativos.

No entanto, no começo do Livro I da sua "Arithmética", que consiste em uma coleção de 150 problemas, ele apresentou uma declaração muito importante a respeito do que hoje é a multiplicação dos números negativos afirmando que o que está em falta multiplicado pelo que falta resulta em algo positivo; enquanto que o que está em falta multiplicado pelo que é positivo resulta em algo que está em falta.

Mesmo tendo um enfoque prático, Diofanto sinaliza a necessidade da criação de um novo "tipo" de número ainda que na prática diária da época eles não fossem tão importantes, conforme reforça Bombelli:

> Mais por mais dá mais; menos por menos dá mais; mais por menos dá menos; menos por mais dá menos; mais 8 por mais 8, dá 64; menos 5 por menos 6, dá mais 30; menos 4 por mais 5, dá menos 20; mais 5 por menos 4, dá menos 20. (BOMBELLI, 1572)

Contudo, os números inteiros não eram bem vistos por matemáticos desde a antiguidade, passando pela idade média, idade moderna e começando a serem mais estudados e aceitos na idade conteporânea.

De acordo com Boyer e Eves,

> Um matemático Hindu muito notável, conhecido com Bhaskara (1114 - 1185) em um de seus livros resolve uma equação do segundo grau e encontra duas raízes 50 e -5 como solução de um problema. Para o segundo valor ele considerou inadequado devido as pessoas ainda não aceitarem soluções negativas. Bahskara também afirmava que as raízes negativas não podiam existir porque um número negativo não é um quadrado. (BOYER, 1996)

Michael Stifel (1487 - 1567) chamava os números inteiros de Números Absurdos, já Girolamo Cardano (1501 - 1576) os denominava de Números Falsos, demonstrando assim a rejeição desses números pelos matemáticos da época.

Da noção intuitiva do números inteiros até os conceito mais elaborados, muito bem definidos, nós tivemos uma período secular. Só no final do século XIX, que tivemos a transição finalizada, que a noção de números inteiros passou a ser baseada em conceitos

da teoria dos conjuntos.

O matemático alemão Edmund Landau (1877 - 1938), ilustrado na Figura 4, um dos matemáticos que ajudou a desenvolver o conceito dos conjuntos números inteiros e o batizou com a letra $\mathbb{Z}$ que é a primeira letra da palavra, número, em alemão. Um grupo de matemáticos franceses chamados: Grupo Bourbaki (1938) gostaram da ideia de Landau e ajudaram a dinfundi-la.

Figura 4 – Edmund Landau.

Fonte: https://www.spm.pt/ Acessado: 23:19 02/03/2021.

Segundo (SÁ; ANJOS,), Franois Viète (1540 - 1630), é conhecido como um dos introdutores dos simbolos "+", "−"e "=", entretanto estes simbolos referiam-se apenas à operação de subtração entre números "verdadeiros", isto é, positivos. Para Viète, os números negativos eram desprovidos do significado intuitivo e físico, era do tipo de que em vez de acrescente -3, diria diminua 3. Mas, Viète acabou contribuindo para o amadurecimento dos números relativos, com a inserção de uma nova notação na matemática que passou a ser abundantemente utilizada pelos matemáticos no futuro.

O meu objetivo com este trabalho é fazer um material de apoio, para que os discentes que irão estudar o assunto de equações diofantinas lineares, consigam se basear por esta dissertação, e para que cheguemos no assunto de equações diofantinas, é necessário que o discente tenha uma base, não só histórica, como também no que diz respeito ao conjunto dos números inteiros e suas operações (Adição e Multiplicação).

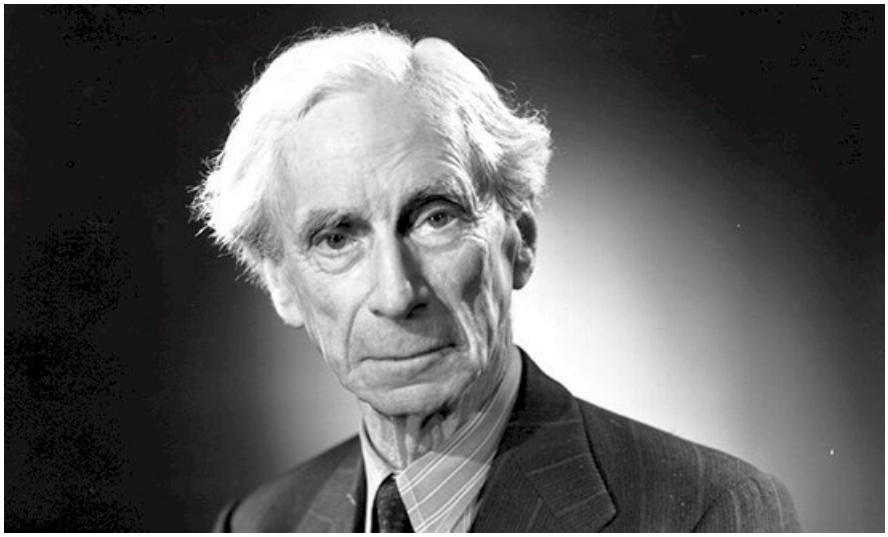
$$\mathbb{Z} = \{..., -6, -4 - 3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ ...\}.$$

Temos também que, em $\mathbb{Z}$ há um subconjunto do números naturais:

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, ...\}.$$

Outro matemático que contribuiu com uma teoria dos números inteiros como a extensão dos números ordinais foi B. Russel, representado na Figura 5, que propôs uma definição de número inteiro baseada na relação de ordem. Caracterizou a idéia de ordem como uma relação assimética e transitiva e definiu os números inteiro como relações assimétricas entre números naturais.

Figura 5 – Bertrand Russel.



Fonte: http://editoraunesp.com.br/ Acessado: 23:32 02/03/2021.

De acordo com Gonzales (1990, *apud* (SÁ; ANJOS,)), a teoria de Russeal também se relacionou com a teoria de Dedekind, pois para este um número inteiro era uma classe de equivalência de pares ordenados de números naturais que coincida com o grafo da relação proposta por Russeal.

A minha abordagem neste trabalho é citar uma lista com algumas propriedades básicas do conjunto dos números inteiros e alguns dos seus conceitos que o tornaram mais "elegante", e para o definir e organizá-lo junto com a suas propriedades, foi usado os Aximoas desenvolvidos por Giuseppe Peano (1858 - 1932) que caracterizou o conjunto dos números naturais e serviu como base para obtermos os conjunto do inteiros.

1.1.1 A matemática de Diofanto

Diofando de Alexandria, foi um dos mais importantes matemáticos que viveu no Egito no século III a.C, muitas vezes considerado como "O pai da Algebra", Diofanto está para Aritmética, assim como Ptolomeu está para a Astronomia e Euclides para a Geometria.

Devido a sua fama, algumas histórias são contadas, como o enigma que teria sido gravado no túmulo do matemático por um amigo, Metrodorus, e cujo resultado revela a idade desse matemático:

"Viajante! Aqui estão as cinzas de Diofanto. É milagroso que os números possam medir a extensão da sua vida.

Um sexto dela foi uma bela infância.

Depois de 1/12 da sua vida, a sua barba cresceu.

Um sétimo da sua vida passou-se num casamento sem filhos.

Mas, cinco anos após isso, nasceu o seu primeiro filho.

Que viveu uma vida feliz durante apenas metade do tempo de vida do seu pai.

E, em profundo pesar, o pobre velho terminou os seus dias na Terra, quatro anos após perder o seu filho."

... resultando em 84 anos.

Dentre grandes descobertas de Diofantino, cujo busto está ilustrado na Figura 6, posso destacar uma, que foi provada tempos depois por Lagrange - Joseph Louis Lagrange que dizia: *"todo número inteiro positivo pode ser escrito como uma soma de no máximo quatro quadrados de outros números inteiros positivos"*. Como no exemplo:

$22 = 2^2 + 3^2 + 3^2$

$32 = 4^2 + 4^2$

$16 = \frac{256}{24} + \frac{144}{25} = (\frac{16}{5})^2 + (\frac{12}{5})^2$.

Figura 6 – Diofanto de Alexandria.

Fonte: http://www.repositorio.ufc.br/ Acessado: 19:12 09/04/2021.

Grande parte da sua fama também é advinda da criação do seu livro, batizado de *Arithmetica*, conforme ilustra a Figura 7, no qual são citados por volta de 150 problemas matemáticos e resolvidos, de forma engenhosa pelo seu criador, já começando a dar as primeiras noções algébricas na resolução desses problemas, que possuiam geralmente so-

luções interias, e que foram batizados de Equações Diofantinas, e estas serão as equações que serão geradas e resolvidas a partir dos problemas que irei trabalhar mais afundo no próximom capítulo.

Figura 7 – Frontispício da “Arithmetica De Diofanto", publicado em Toulouse, Fr. em 1620.

Fonte: http://clubes.obmep.org.br/ Acessado: 00:27 02/11/2020.

Acredita-se que sua obra tenha sido achada e perdida várias vezes, chegando na Europa por volta do início do século 17, na fuga do Império Bizantino de Constantinopla [Istanbul]. Sua primeira tradução para o latim, mais famosa foi feita por Barchet em 1621.

1.2 Propriedades dos Números Inteiros

As operações de adição e multiplicação em $\mathbb{Z}$ possuem as seguintes propriedades:

1. 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* $a.b = a'.b'$.

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

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

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

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

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

7. Fechamento:
   O conjunto $\mathbb{Z}$ é fechado para a adição e para a multiplicação, ou seja, para todos a, $b \in \mathbb{Z}$, tem-se que $a + b \in \mathbb{Z}$ e $a.b \in \mathbb{Z}$.

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

   I. $a = b$;

   II. $b - a \in \mathbb{N}$;

   III. $(-b - a) = a - b \in \mathbb{N}$.

   Diremos que a é menor do que b, simbolizado por $a < b$, toda vez que a propriedades (II) acima for verificada.

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

   i. $a = b$;

   ii. $a < b$;

   iii. $b < a$.

9. Princípio da Boa Ordenação:

   Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Proposição 1.2.1. $a.0 = 0$ para todo $a \in \mathbb{Z}$.

Demonstração. Temos pelas Propriedades 4 e 6 que

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

Somando $-(a.0)$ aos extremos da igualdade, pelas Propriedades 2, 3, 4 e 5, obtemos:

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

□

Proposição 1.2.2. A adição é compatível e cancelativa com respeito à igualdade:

$$\forall a,\ b,\ c \in \mathbb{Z},\ a = b \ \Leftrightarrow a + c = b + c.$$

Demonstração. A implicação $a = b \rightarrow a + c = b + c$ é consequência do fato de a adição ser bem definida, pela propriedade 1.
Suponha agora que $a + c = b + c$. Somando $(-c)$ a ambos os lados, obtemos $a = b$. □

1.3 Divisibilidade

Definição 1.3.1. Dados dois números naturais a e b com $a \neq 0$, diremos que a *divide* b, escrevendo $a \mid b$, quando existir uma $c \in \mathbb{Z}$ tal que $b = a.c$. Neste caso, diremos também que a é um divisor ou um fator de b, ou ainda, que b é uma múltiplo de a.

A notação $a \mid b$ diz que b é um múltiplo de a e não uma operação matemática em $\mathbb{Z}$. Quando temos a negação dessa notação: $a \nmid b$ temos que b não é um múltiplo de a. ou seja, não existe um $c \in \mathbb{Z}$ tal que $b = a.c$.

Exemplo 1.3.1. Pela *definição* é fácil ver que:

$$\pm 1 \mid 0,\ \pm 2 \mid 0,\ \pm 3 \mid 0 \ ...$$

$$\pm 1 \mid 8 \ \pm 2 \mid 8 \ \pm 4 \mid 8 \ \pm 8 \mid 8;$$

$$\pm 0 \nmid 8 \ \pm 3 \nmid 8 \ \pm 5 \nmid 8 \ \pm 6 \nmid 8 \ \pm 7 \nmid 8...$$

1.3.1 Propriedades

Sejam $a,\ b,\ c \in \mathbb{Z}$. Tem-se que

1. $1 \mid a,\ a \mid \ a \ e \ a \mid 0$;
2. a divide b se, e somente se, $|a|$ divide $|b|$;
3. se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. (1) Isto decorre das igualdades $a = a.1,\ a = 1.0 \ e \ 0 = a.0$.

□

Demonstração. (2) ($\Leftarrow$) Inicialmente, temos que $a \mid |a|$, para todo $a \neq 0$.

Supondo que $|a| \mid b$ ou $|a| \mid (-b)$, temos:

i. Se $|a| \mid b$, como $a \mid |a|$, por transitividade, segue que $a \mid b$.

ii. Se $|a| \mid (-b)$ $(\rightarrow)$ $|a| \mid b$ *ou* $|a| \mid (-1)$.

- $|a| \mid b$, pelo item 1., nada há a mostrar.
- $|a| \mid (-1)$, então $a = 1$ ou $a = -1$, em ambos os casos $a \mid b$, para todo b inteiro.

Portanto, se $|a| \mid |b|$, então $a|b$. Logo $a \mid b(\rightarrow)|a| \mid |b|$.

Temos que $|a| \mid a$, para todo $a \neq 0$ *e* $b \mid |b|$, para todo $b \neq 0$.

De $|a| \mid a$, como por hipótese $a \mid b$, $|a| \mid b$ e, novamente por transitividade, $|a| \mid |b|$. □

Demonstração. (3) $a \mid b$ e $b \mid c$ implica que existe $f,\ g \in \mathbb{Z}$, tais que $b = f.a$ e $c = g.b$. Suponhamos que o valor de b da primeira equação na outra, obtemos:

$$c = g.b = g.(f.a) = (g.f).a,$$

o que nos mostra que $a \mid c$. □

1.4 Números Primos

Definição 1.4.1. Diz-se que um número inteiro p é primo, se e somente se, p satisfaz as seguintes condições:

i. $p \neq 0$ e $p \neq \pm 1$.

ii. Os únicos divisores de p são -1, 1, p e $-p$.

Todo número pode ser partido em produtos de seus primos constituintes, dos primos formamos os demais números, e desses, construímos toda a matemática e desta temos toda a ciência.

O meu objetivo neste trabalho acadêmico não é provar todas a propriedades dos números primos, advindas, ou não, de lemas, corolários ou teoremas, mas sim, citar, comentar e, até mesmo, demonstrar as principais, para desenvolver o assunto em foco, com objetividade e lastro matemático, que são as equações diofantinas lineares.

Os números primos são incríveis, parece até que uma áura de mistérios ainda os rodeiam, tais números são tão especiais que fazem parte da matemática básica e superior, e até hoje ainda não se consegue descobrir uma expressão que consiga identificá-los, entretanto já se sabem algumas informações sobre esses números.

Uma das primeiras perguntas sobre eles é: Será que eles são finitos ou infinitos?

Um dos primeiros a responder tal questionamento foi Euclides de Alexandria (300 A.C), partindo da hipótese:

Demonstração. Vamos supor que a quantidade de números primos é finita.

Sendo o conjunto:

$$A = \{\ 2, 3, 5, ...p_n\}\ .$$

O conjunto dos n primeiros números primos, com p_n, o maior e últimos deles.

Além disso, podemos afirmar que existe um Q, de modo que:

$$Q = (2.3.5.....p_n) + 1 > p_n.$$

Devido a parcela 1, podemos concluir que:

$2 \nmid$ Q;

$3 \nmid$ Q;

$5 \nmid$ Q;

...

p $\nmid$ Q.

Isso implica $1 \mid Q$ e $Q \mid Q$ portanto Q é primo e maior que p_n. Contradição, visto que p_n era o maior primo, e encontramos Q que é maior que p_n.

Assim concluímos que o conjunto do números primos é infinito.

□

1.4.1 Propriedades

1. Se p é um primo tal que $p \mid a.b$, então $p \mid a$ ou $p \mid b$.

2. Se p é um primo tal que $p \mid a_1.a_2.\ ...\ a_n$, então existe um índice k com $1 \geq k \geq n$, tal que $p \mid a_k$.

3. Se os inteiros $p, q_1, q_2,\ ...\ q_n$ são todos números primos e se $p \mid q_1.q_2.\ ...\ .q_n$, então existe um índice k, com $1 \leq k \leq n$, tal que $p = a_k$.

4. Todo inteiro composto possui um divisor primo.

1.4.2 Teorema Funadamental da Aritmética.

Definição 1.4.2. Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado número primo.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

1. Se $p \mid q$, então $p = q$.

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

2. Se $p \nmid a$, então $(p, a) = 1$ [1].

   De fato, se $(p, a) = d$,[2]. temos que $d \mid p$ e $d \mid a$. 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 número natural n_2 tal que

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

   Assim temos como exemplos, $2, 3, 5, 7$ *e* 13 são números primos e $4, 6, 8, 9$ *e* 10 são números compostos.

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, logo, todos os números inteiros não nulos, conforme demonstrartei no *Teorema fundamental da Aritmética.*

Corolário 1.4.1. Se $p, p_1, p_2, \ \ldots\ , p_n$, são números primos e, se $p \mid p_1.p_2.\ \ldots\ p_n$, então $p = p_i$ para algum
$i = 1, 2, \ \ldots\ n$.

Teorema 1.4.1. 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.

[1] $(p, a) = 1$. Lê-se: MDC entre p e a é igual a 1
[2] $(p, a) = d$. Lê-se: MDC entre p e a é igual a d

Demonstração. Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente o 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 na temos que 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 $p_1, p_2, ..., p_2$ e $q_1, q_2, ..., q_s$ tais que $n_1 = p_1.p_2. \ ... \ .p_r$ e $n_2 = q_1.q_2. \ ... \ .q_s$. Portanto, $n = p_1. \ .p_2. \ ... \ .q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1.p_2. \ ... \ .p_r = q_1.q_2. \ ... \ .q_s$, onde os p_i e os q_j são primos. Como $p_1 \mid q_1.q_2. \ ... \ .q_s$, pelo corolário há pouco citado, temos que $p_1 = q_j$ para algum j, que após o reordamento de $q_1, q_2, \ ... \ , q_s$, podemos supor que seja q_1. Portanto,

$$p_2.p_3. \ ... \ .p_r = q_2.q_3. \ ... \ .q_s.$$

Como $p_2.p_3. \ ... \ .p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

□

Teorema 1.4.2. Unicidade da decomposição de um número primo em fatores primos:

A menos da ordem dos fatores, a decomposição de um inteiro positivo $n > 1$ como produto de fatores primos é única.

Demonstração. Suponhamos que n admita duas decompsições como produto de fatores primos:

$N = p_1.p_2. \ ... \ .p_r = q_1.q_2. \ ... \ q_s (r \leq s)$ onde p_i e q_j são inteiros primos e $p_1 \leq p_2 \ ... \leq p_r, \ q_1 \leq q_2 \ ... \leq q_s$.

Como $p_1 \mid q_1.q_2. \ ... \ q_s$ então $\in k (1 \leq k \leq s)$ tal que $p_1 = q_k$.

Da mesma forma $p_2 = q_h, \ p_3 = q_m, \ ...$, e assim por diante.

Se $r < s$, depois de r cancelamentos temos: $1 = q_{r+1}.q_{r+2}. \ ... \ q_s$. Absurdo, pois $q_j > 1$.

Assim $r = s$ e cada p_i, é igual a um q_j, ou seja, as decomposições são identicas, a menos da ordem dos fatores. Deste modo, qualquer inteiro $n > 1$ admite somente uma representação da forma: $n = p_1^{k_1}.p_2^{k_2}. \ ... \ p_r^{k_r}$, onde, para $i = 1, 2, 3, ..., r$, k_i é um inteiro positivo e cada p_i é um primo, com $p_1 < p_2 < \ ... \ < p_r$, denominada decomposição canônica do inteiro positivo n.

□

1.4.3 Crivo de Eratóstenes.

O crivo de Eratóstenes é um algorítmo que nos ajuda a encontrar uma lista de números primos, como ja dito anteriormente, não existe um padrão na organização dos números primos, então esse crivo é uma ferramenta que ajuda a encontra alguns deles.

Primeiramente é colocado os n ($n \geq 2$) números naturais em uma tabela, em sua ordem natural, e em seguida, eliminam-se todos os inteiros compostos que são múltiplos de dos primos p tais que $p\sqrt{n}$, isto é $2p,\ 3p,\ 4p,\ \ldots$.

Exemplo 1.4.1. Construir a tabela de todos os primos menores que 100.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Perceba que o 1 não aparece na lista, pois não é primo, em seguida o primeiro número primo que temos é o 2, o que faz nos eliminar todos o seus múltiplos, maiores que ele. Após, temos o número 3, assim elmininando todos os seus múltiplos maiores. Fazendo a mesma coisa com o 5, 7. Quando chegamos no 11 que é maior que $\sqrt{100}$ temos todos os números compostos eliminados, sobrando assim: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97 que são os primos menores que 100 nesta lista.

1.4.4 Primos Gêmeos

Sendo a e b dois inteiros positivos, denomina-se a e b primos gêmeos se os dois são primos, positivos, ímpares e consecutivos. Por exemplo, são pares de primos gêmeos: 3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31. Até hoje não é sabido se existe um número infito de pares de primos gêmeos.

Um fato interessante é a existência de apenas um terno de inteiros positivos ìmpares e consecutivos que são todos primos: 3, 5 e 7.

1.5 Máximo Divisor Comum.

Definição 1.5.1. Sejam a e b dois inteiros simultaneamente nulos ($a \neq 0$ *ou* $b \neq 0$). O inteiro positivo d é o máximo divisor comum de a e b se:

i. $d \mid a$ e $d \mid b$.

ii. $c \mid a$ e $c \mid b \Rightarrow c \mid d$.

Nota-se que a condição (i) garante que d é um divisor comum de a e b e a condição (ii) afirma que d é o maior dentre todos os divisores comuns de a e b. Uma outra notação bastante comum para o MDC entre a e b é (a, b).

Observação 1.5.1.

- $(a, b) = (b, a)$;
- $(0, 0)$ não existe;
- $(a, 1) = 1$, para qualquer inteiro a;
- se $a \neq 0$, então $(a, 0) = |a|$;
- se $a \mid b$, então $(a, b) = |a|$.

1.5.1 Existência e Unicidade de MDC

Sendo a e b dois inteiros não simultaneamente nulos ($a \neq 0$ ou $b \neq 0$), então existe e é único (a, b). Afirma-se também que existem os inteiros x e y tais que $(a, b) = a \cdot x + b \cdot y$, isto é o (a, b) é uma combinação linear entre os valores de a e b.

1.5.2 Inteiros Primos entre si

Sendo a e b dois inteiros que não são simultamente nulos ($a \neq b$) ou ($b \neq 0$), pode-se afirmar que a e b são primos entre sí se e somente se o $(a, b) = 1$. Concluí-se, portanto, que dois inteiros a e b primos entre si somente admitem como divisores os inteiros 1 e -1.

Lema 1.5.1. Lema de Euclides

Sejam $a,\ e\ b,\ n \in \mathbb{N}$ com $a < n \cdot a < b$. Se existe $(a, b - n \cdot a)$, então (a, b) existe e

$$(a, b) = (a, b - n \cdot a).$$

Demonstração. Seja $d = (a, b - n \cdot a)$. Como $d \mid a$ e $d \mid (b - n \cdot a)$, segue que d divide $b = b - n \cdot a + n \cdot a$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b; logo, c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c \mid d$. Isso prova que $d = (a, b)$.

□

Observação 1.5.2. Com a mesma idéia usada para provar Lema de Euclides, pode-se provar que, para todos $a,\ b,\ n \in \mathbb{N}$,

$$(a, b) = (a, b + n \cdot a),$$

ou que, se $n \cdot a > b$, então

$$(a, b) = (a, n \cdot a - b).$$

Teorema 1.5.1 (Teorema de Bachét-Bezout)**.** Se $d = (a, b)$, então existem inteiros x e y tais que $d = a \cdot x + b \cdot y$

Demonstração. 1° Caso

$a = b = 0$. Neste caso, basta ver que $x = 0$ e $y = 0$ são soluções inteiras da equação $0 \cdot x + 0 \cdot y = (0, 0)$.

2° Caso

$a \neq 0$ ou $b \neq 0$. Neste caso, considere o conjunto

$$I(a, b) = a \cdot x + b \cdot y;\ x, y \in \mathbb{Z}.$$

Observe que $I(a, b)$ é formado por números inteiros, pois como $a, b, x, y \in \mathbb{Z}$, então $a \cdot x + b \cdot y \in \mathbb{Z}$.

Além disso, $I(a, b)$ é formado por números inteiros, pois tomando o mesmo sinal de b vamos ter que $a \cdot x$ e $b \cdot y$ sejam maiores ou iguais a zero, e pelo menos um deles é positivo, pois um deles é maior que zero. Logo $a \cdot x + b \cdot y \geq 0$ e $a \cdot x + b \cdot y \in I(a, b)$

Seja $d = a \cdot x_0 + b \cdot y_0 \in I(a, b)$ o menor inteiro positivo do conjunto $I(a, b)$.

Agora vamos provar que d divide todos os elementos do conjunto $I(a, b)$. Seja $m = a \cdot x + b \cdot y \in I(a, b)$ um elemento qualquer de $I(a, b)$. E sejam q e r o quociente e o resto da divisão de m por d, isto é quando dividimos m por d obtemos quociente q e resto r ou seja,

$$m = d \cdot q + r,\ q \in \mathbb{Z},\ r \in \mathbb{Z},\ 0 \leq r < d.$$

Daí, temos

$r = m - d \cdot q$

$= (a \cdot x + b \cdot y) - (a \cdot x_0 + b \cdot y_0) \cdot q$

$= a(x - x_0 \cdot q) + b(y - y_0) \cdot q$

como $x - x_0 \cdot q$ e $y - y_0 \cdot q$ são inteiros e

$r = a(x - x_0 \cdot q) + b(y - y_0 \cdot q)$

então $\in I(a, b)$.

Observe que r não pode ser maior que zero, pois como $0 \geq r \geq d$, então r seria um inteiro positivo do conjunto $I(a, b)$ menor do que d. Absurdo, pois já tomamos d como sendo o menor inteiro positivo de $I(a, b)$.

Como $r \geq 0$ e r não pode ser positivo , então $r = 0$. Logo temos $m = d \cdot q$, ou seja, $d \mid m$. Como m foi um elemento qualquer de $I(a, b)$, então isto prova que d divide todos os elementos do conjunto $I(a, b)$. Observe que a e b são da forma $a = a \cdot 1 + b \cdot 0$ e $b = a \cdot 0 + b \cdot 1$, logo temos que $a, b \in I(a, b)$. Como d divide todos os elementos do conjunto I(a,b), e $a, b \in I(a, b)$, então $d \mid a$ e $d \mid b$, ou seja d é divisor comum de a e b, logo $d \leq (a, b)$. Por outro lado, como $(a, b) \mid a$ e $(a, b) \mid b$, então (a, b) também divide $a \cdot x_0$ e $b \cdot y_0$, como $d = a \cdot x_0 + b \cdot y_0$, então $(a, b) \mid d$.

Como $0 \leq d \leq (a, b)$ e $(a, b) \mid d$, então $(a, b) \leq d$ juntando com $d \leq (a, b)$, obtemos $d = (a, b)$, e como $d = ax_0 + b \cdot y_0$, então

$$a \cdot x_0 + b \cdot y_0 = (a, b).$$

Ou seja provamos que existem inteiros $x = x_0$ e $y = y_0$ que resolvem a equação

$$a \cdot x + b \cdot y = (a, b).$$

Como queriamos demonstrar.

□

Teorema 1.5.2. Sejam a e b dois inteiros não simultaneamente nulos ($a \neq b$) ou ($b \neq 0$). Os inteiros a e b são primos entre si se e somente se existem inteiros x e y tais que $a \cdot x + b \cdot y = 1$.

Demonstração. ($\Rightarrow$) De 1.5.1 temos que se a e b são primos entre sí, então $(a, b) = 1$, consequentemente existem x e y tais que $a \cdot x + b \cdot y = 1$.

($\Leftarrow$) Se existem inteiros x e y, tais que $a \cdot x + b \cdot y = 1$ e $(a, b) = d$, então $d \mid a$ e $d \mid b$. Logo, $d \mid (a \cdot x + b \cdot y)$ e como $d \mid 1$, resulta em $d = 1$, ou seja, $(a, b) = 1$.

□

1.5.3 Propriedades

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

   Demonstração. Desde que $d = (a, b)$ suponhamos que existe um $c > 1$, com $c \in \mathbb{Z}$ tal que $c \mid \frac{a}{d}$ e $c \mid \frac{b}{d}$, assim $c \mid a$ e $c \mid b$. Isso seria uma contradição com a hipótese, poís $(a, b) = d \cdot c$

   □

2. Se $a \mid b$ e se $(b, c) = 1$ então o $(a, c) = 1$.

   Demonstração. Suponhamos que $(a, c) = d > 1$, então teremos um $d \in \mathbb{Z}$ tal que $d \mid a$ e $d \mid c$. Por hipótese, temos que $a \mid b$, assim, por transitividade $d \mid b$. Uma contradição com a hipótese, poís se $d \mid c$ e $d \mid b$ teriamos $(b, c) > 1$, Portanto $(a, c) = 1$

   □

3. Se $a \mid c$, se o $b \mid c$ e se o $(a, b) = 1$, então $a \cdot b \mid c$.

   Demonstração. Com efeito, como $a \mid c$ existe um $q \in \mathbb{Z}$ tal que $c = a \cdot q$ de outro lado, como $(a, b) = 1$ e $b \mid c$, concluímos que $b \mid q$ ou seja, existe um $p \in \mathbb{Z}$ de modo que $q = b \cdot p$. Assim, $c = a \cdot b \cdot p$. Logo $a \cdot b \mid c$.

   □

4. Se $(a, b) = 1 = (a, c)$, então o $(a, b \cdot c) = 1$.

   Demonstração. Como $(a, b) = 1$, então existem inteiros n e m tais que

   $$a \cdot n + b \cdot m = 1.$$

   Multiplicando por c, obtemos

   $$a(c \cdot n) + b \cdot c(m) = c.$$

   Agora seja $d = (a, b \cdot c)$

   Então $d \mid a$ e $d \mid b \cdot c$.

   Portanto d divide a combinação linear entre a e $b \cdot c$, em particular

$$d \mid [a(c \cdot n) + b \cdot c(m)].$$

E como isso é válido.

Então $d \mid c$

$d \mid [a(c \cdot n) + b \cdot c(m)]$, mas $a(c \cdot n) + b \cdot c(m) = c$, portanto $d \mid c$

E como $d \mid a$, e $d \mid c$

Então $d \mid (a, c)$

Mas como $(a, c) = 1$, então $d \mid 1$.

Portanto $d = 1$.

□

5. Se o $(a, b \cdot c) = 1$, então $(a, b) = 1 = (a, c)$.

Demonstração. Se $(a, b \cdot c) = 1$, então

$$\begin{aligned} a \cdot x + b \cdot c \cdot y = 1 \Rightarrow 1 &= a \cdot x + b \cdot (c \cdot y) = a \cdot x + c \cdot (b \cdot y) \\ &\Rightarrow (a, b) = 1 = (a, c). \end{aligned}$$

□

6. Se $a \mid b \cdot c$ e se o $(a, b) = 1$, então $a \mid c$.

Demonstração. Com efeito, se $a \mid b \cdot c$ então $b \cdot c = k \cdot a$. Também, se $(a, b) = 1$ então

$$\begin{aligned} a \cdot x + b \cdot y = 1 &\Rightarrow a \cdot c \cdot x + b \cdot c \cdot y = c \\ &\Rightarrow a \cdot c \cdot x + k \cdot a \cdot y = c \\ &\Rightarrow a \cdot (c \cdot x + k \cdot y) = c \\ &\Rightarrow a \mid c. \end{aligned}$$

□

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

Demonstração. Se $d = (a, b, c)$ então $a \cdot x + b \cdot y + c \cdot z = d$.

Se $(a, b) = d'$ então existem inteiros m e n tais que $a \cdot m + b \cdot n = d'$ e d' é o menor valor que podemos obter em uma combinação linear de a e b deve ser múltiplo de d'. Logo: $a \cdot x + b \cdot y = d'k$.

Assim: $d = a \cdot x + b \cdot y + c \cdot z = d' \cdot (k) + c \cdot z \Rightarrow d = (d', c) = ((a, b), c)$.

□

1.5.4 Cálculo de MDC a partir das Fatorações Canônicas

A partir da idéia do cálculo do MDC de alguns números inteiros, por meio da fatoração, pode-se tomar como base para esse cálculo todos dos fatores primos existentes nas fatorações canônicas dos inteiros elevados aos respectivos menores expoentes.

Por exemplo, para calcular o MDC de $2^3 \cdot 3 \cdot 5^4 \cdot 7^3$ e $2^2 \cdot 3^2 \cdot 5^4 \cdot 11$, observaremos então quais são os fatores primos existentes nesses inteiros, ou seja $2,\ 3,\ 5,\ 7,\ e\ 11$ e em seguida adotar os menores expoentes destes números inteiros. Finalmente, teremos que $(2^3 \cdot 3 \cdot 5^4 \cdot 7^3,\ 2^2 \cdot 3^2 \cdot 5^4 \cdot 11) = 2^2 \cdot 3 \cdot 5^4$.

Definição 1.5.2. Sejam $d = (a, b)$, $a = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}...$ e $b = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3}...$, temos que $d = 2^{min(\alpha_1,\beta_1)} \cdot 3^{min(\alpha_1,\beta_1)} \cdot 5^{min(\alpha_1,\beta_1)}...$

1.5.5 Algoritmo de Euclides

Demonstração. Seja d o maior divisor comum de a e b. Admitindo, sem perda de generalidade: $a > b$ teremos: $a = d \cdot k_1$

$$k_1 > k_2.$$

$b = d \cdot k_2$. Daí: $a - b = d \cdot k_1 - d \cdot k_2$ Assim,

$$a - b = d(k_1 - k_2).$$

Permitindo assim concluir que d é divisor de $a - b$.

Dessa sentença temos: $d \mid a$ e $d \mid b \Rightarrow$ d$\mid a - b$. $(\star)$

Por outro lado, Seja r o maior divisor comum de a e $a - b$ temos: $a = r \cdot \lambda_1$ $(\lambda_1 > \lambda_2)$ $a - b = r \cdot \lambda_2 \Rightarrow$ r$\cdot\lambda_1 - b = r \cdot \lambda_1 \Rightarrow$ r$\cdot\lambda_1 - r \cdot \lambda_1 = b \Rightarrow r \underbrace{(\lambda_1 - \lambda_1)}_{>0} = b$.

Permitindo-se concluir que r é divisor de b. Então $r \mid a\ e\ r \mid a - b \Rightarrow r \mid b$. $(\star\star)$

De $(\star)$ e $(\star\star)$ tem-se

$$x \mid a\ e\ x \mid b \Longleftrightarrow x \mid a\ e\ x \mid a - b.$$

De fato, suponhamos que $d = (a, b)$ e $x = (a, a-b)$. Mostraremos agora que $x = d$.

(α) Considere que $d = (a, b)$, ou seja,

$$d = x.$$

(β) Também, sendo $x = (a, a - b)$, temos:

i. Uma vez que x é o maior divisor de a e de $a - b$ então, podemos concluir que, $x \mid a$ e $x \mid a - b$, portanto

$$x \mid b.$$

ii. De (α), d é o maior divisor de a e o maior divisor de b.

iii. Como x é o maior divisor de a, d é o maior divisor de a, d é o maior divisor de b e $x \mid b$, concluímos que

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

Portanto

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

□

Exemplo 1.5.1. Calcule $(12, 8)$.

Da relação acima podemos resolver esse problema muito rapidamente:

$(12, 8) =(12, \underbrace{4}_{12-8}) = (8,4) = (4,4) =1.$

Exemplo 1.5.2. Calcule $(243, 37)$.

Neste exemplo, para não ficar muito extenso, irei subtrair o b do a quantas vezes forem possíveis, para isso basta fazer a divisão do a por b e usarmos o resto.

$$(243, 37) = (37, \underbrace{21}_{243-6\cdot 37}) = (21, 16) = (16, 5) = (5, \underbrace{1}_{16-3\cdot 5}) = (1, 1) = 1.$$

A partir desse processo criou-se um método de cálculo de MDC chamado: Jogo da velha. Particularmente eu gosto de chama-lo de jogo dos restos.

Quoc.	6	1	1	3	5
243	37	21	16	5	$1 \Rightarrow MDC$
Rest.	21	16	5	1	0

Note que é feita a divisão dos elementos da segunda linha $(234 : 37)$, o quociente desta divisão será levado para linha de cima, e o resto para a linha de baixo, em seguida

este resto irá para a segunda linha e o processo será refeito $(37 : 21)$..., até se obter o resto zero. A partir daí, o resto que tivermos antes do zero será o MDC.

A priori pode-se pensar que a linha dos quociente não será relevante, visto que somente os restos serão utilizados, entretanto para o assunto abordado neste trabalho será importante estes quocientes, visto que podemos escrever esse MDC como uma espécie de combinação linear dos números que pediu-se o MDC.

Note que, do exemplo anterior pode-se escrever:

i . $21 = 243 - 37 \cdot 6$

ii . $16 = 37 - 21 \cdot 1$

iii . $5 = 21 - 161$

iv . $1 = 16 - 53$

Substituindo $[iii]$ em $[iv]$ teremos:

$1 = 16 - (21 - 16 \cdot 1)3 \;\Rightarrow\; 1 = 16 \cdot 4 - 21 \cdot 3$

Agora substituindo [ii] nesta nova equação:

$1 = (37 - 21 \cdot 1)4 - 21 \cdot 3 \;\Rightarrow\; 1 = 37 \cdot 4 - 217$

Por fim, substituindo [i] nesta equação, podemos escrever:

$1 = 37 \cdot 4 - (243 - 37 \cdot 6)7$

Portanto

$1 = 243 \cdot (-7) + 37 \cdot 46.$

É sempre bom reforçar que não é necessário efetuar as multiplicações neste método, visto que o objetivo é escrever o MDC como uma soma de produtos.

Perceba que encontramos uma expressão numérica que indica o MDC com os números que nos foram dados para determinar o MDC entre eles, e existe uma teorema que garante que o MDC sempre poderá ser escrito desta forma, e ele foi citado e demonstrado acima 1.5.1. Para a resolução de problemas envolvendo Equações diofantinas lineares (que é um dos focos deste trabalho) tal relação servirá de ajuda na resolução de muitos outros problemas.

1.6 Mínimo Múltiplo Comum.

Definição 1.6.1. Sendo a e b dois inteiros diferentes de zero ($a \neq 0$ *e* $b \neq 0$) define-se mínimo múltiplo comum de a e b o inteiro positivo m ($m > 0$ satisfaz às seguintes

condições:

i. $a \mid b$ e $b \mid m$;

ii. se $a \mid c$ e se $b \mid c$, com $c > 0$, então $m \leq c$.

Observa-se que a condição (i) garante que m é múltiplo comum de a e b e a condição (ii) afirma que m é o menor dentre todos os múltiplos comuns de a e b. Por $[a,\ b]$ indica-se o mínimo múltiplo comum de a e b.

Como o produto ab é um dos múltiplos comuns de a e b, temos que: $[a,\ b] \leq |ab|$.

Nota-se também que , se $a \mid b$, então $[a,\ b] = |b|$.

1.6.1 Cálculo de MMC a partir das Fatorações Canônicas

A partir da idéia do cálculo do MMC de alguns números inteiros, por meio da fatoração, pode-se tomar como base para esse cálculo todos dos fatores primos existentes nas fatorações canônicas dos inteiros elevados aos respectivos maiores expoentes.

Por exemplo, para calcular o MMC de $2^3 \cdot 3 \cdot 5^4 \cdot 7^3$ e $2^2 \cdot 3^2 \cdot 5^4 \cdot 11$, observaremos então quais são os fatores primos existentes nesses inteiros, ou seja $2,\ 3,\ 5,\ 7,\ e\ 11$ e em seguida adotar os maiores expoentes destes números inteiros. Finalmente, teremos que $[2^3 \cdot 3 \cdot 5^4 \cdot 7^3,\ 2^2 \cdot 3^2 \cdot 5^4 \cdot 11] = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7^3 \cdot 11$.

Definição 1.6.2. Sejam $m = [a, b]$, $a = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3}...$ e $b = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3}...$, temos que $m = 2^{max(\alpha_1,\beta_1)} \cdot 3^{max(\alpha_1,\beta_1)} \cdot 5^{max(\alpha_1,\beta_1)}...$

Proposição 1.6.1. Dados dois números naturais a e b, temos que $[a, b] \cdot (a, b) = a \cdot b$

Demonstração. Seja $(a, b) = d$ e $[a, b] = m$.

Como $a|a \cdot \frac{b}{d}$ e $b|b \cdot \frac{a}{d}$, segue-se que $\frac{a \cdot b}{d}$ é múltiplo comum de a e b.

Portanto, existe um inteiro positivo k tal que $\frac{a \cdot b}{d} = m \cdot k, k \in \mathbb{N}$, o que implica: $\frac{a}{d} = \frac{m}{b} \cdot k$ e $\frac{b}{d} = \frac{m}{a} \cdot k$, isto é, k é divisor comum dos inteiros $\frac{a}{d}$ e $\frac{b}{d}$. Mas $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre sí, de modo que $k = 1$. Assim sendo, temos $\frac{a \cdot b}{d} = m$ ou $a \cdot b = d \cdot m$, isto é $a \cdot b = (a, b).[a, b]$.

□

2 Equações Diofantinas Lineares e Aplicações

Deste capítulo irei apresentar um pouco sobre alguns dos principais tópicos que cercam as equações diofantinas lineras, tais como: definições, condição de existência e suas soluções. Em seguida resolverei alguns problemas clássicos deste assunto, sempre tentando usar a matemática mais básica possível para que seja compreendida de forma clara para o aluno.

2.1 Equações Diofantinas Linerares

Definição 2.1.1. Uma equação Diofantina linear com duas variáveis é toda resolução de problema que recai em uma equação cuja o formato é:

$$a \cdot X - b \cdot Y = c,$$

ou, ainda, do tipo

$$a \cdot X + b \cdot Y = c,$$

com $a,\ b,\ c \in \mathbb{N}$.

Não é sempre que as equações diofantinas possuem solução. Por exemplo:

$$2 \cdot X + 4 \cdot Y = 5.$$

Esta equação não possui solução x_0, y_0 inteiros, e é fácil perceber isto, poís $2 \cdot X$ é um número par e $4 \cdot Y$ támbém é um número par, e a soma de dois números pares não tem como resultar em um ímpar. Logo é muito natural perguntar-se quando as equações diofantinas linerares possuem soluções inteiras.

2.1.1 Condição de Existência de Solução

A equação diofantina linear $a \cdot X + b \cdot Y = c$ tem solução se e somente se $(a, b) \mid c$.

Demonstração. ($\Rightarrow$) Suponhamos que $a \cdot X + b \cdot Y = c$ tem solução, isto é que existem inteiros x_0, y_0 tais que $a \cdot X_0 + b \cdot Y_0 = c$. Por ser $(a, b) = d$, existem r e s tais que $a = d \cdot r$ e $b = d \cdot s$, e temos: $c = a \cdot X_0 + b \cdot Y_0 = d \cdot r \cdot X_0 + d \cdot s \cdot Y_0 = d(r \cdot X_0 + s \cdot Y_0)$, e como $r \cdot X_0 + s \cdot Y_0$ é um inteiro, segue-se que $d \mid c$.

($\Leftarrow$) Suponhamos que $d \mid c$, isto é, que $c = d \cdot t$, onde $t \in \mathbb{Z}$.

Por $(a, b) = d$, existem inteiros X_0 e Y_0 tais que $d = a \cdot X_0 + b \cdot Y_0$, o que implica: $c = d \cdot t = (a \cdot X_0 + b \cdot Y_0)t = a(t \cdot X_0) + b(t \cdot Y_0)$, isto é, o par de inteiros: $x = t \cdot X_0 = (\frac{c}{d}) \cdot X_0$, $y = t \cdot Y_0 = (\frac{c}{d}) \cdot Y_0$, é uma solução da equação $a \cdot X + b \cdot Y = c$.

□

2.1.2 Soluções parametrizadas de uma Equação Diofantina Linear

Seja x_0 e y_0 uma solução da equação $a \cdot X + b \cdot Y = c$, onde $(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são:

$$x = x_0 + t \cdot b, \qquad y = y_0 - t \cdot a; \qquad t \in \mathbb{Z}.$$

Demonstração. Suponhamos que o parde inteiros x_0, y_0 é solução particular da equação $a \cdot X + b \cdot Y = c$, e seja x, y uma solução qualquer desta equação. Então temos:

$$a \cdot x_0 + b_0 = c = a \cdot x + b \cdot y \Rightarrow$$

$a(x - x_0) = b(y_0 - y) \qquad (\star)$

Como $(a, b) = 1$, segue que $b \mid (x - x_0)$.

Logo $x - x_0 = t \cdot b$, $t \in \mathbb{Z}$. $\qquad (\star\star)$

Substituindo a expressão $(\star\star)$ em $(\star)$, segue que:

$$y = y_0 - t \cdot a.$$

□

2.2 Algumas aplicações envolvendo Equações Diofantinas Lineares

Neste tópico resolverei alguns problemas clássicos de equações diofantinas lineares com duas incógnitas, desde os problemas mais básicos até os problemas mais elaborados. Em nenhum momento deixarei fixo algum método específico de resolução de problemas, essas questões que envolvem este tipo de equações muitas vezes possuem mais de um método de resolução, então tentarei resolver as questões sempre de alguma forma que eu acredite que seja mais fácil de enxergar, o que não impede do leitor que esteja usando esse material como apoio possa tentar resolver a mesma questão por outro método.

01. Resolva as Equações:

a) $14X + 22Y = 50$.

Resolução:

Primeiramente, note que podemos simplicar a equação por 2. Assim teremos:

$$7x + 11y = 25$$

Daí, verifico que $(7, 11) = 1 \mid 25$, logo esta equação possui soluções inteiras. Agora preciso apenas de um par x, y que seja solução deste problema para montar as duas equações paramétricas que me informam todas as soluções deste problema. Verifico que $13, -6$ é uma solução deste problema, e ainda:

$$7 \cdot (13) + 11 \cdot (-6) = 25$$
$$(24) \qquad (-13)$$
$$(35) \qquad (-20)$$
$$(46) \qquad (-27)$$
$$\ldots$$
$$x = 13 + 11k \qquad y = -6 - 7k \qquad \text{com } k \in \mathbb{Z}.$$

Verifico também que as possíveis soluções de x aumentam de 11 em 11, já as de y diminuem de 7 em 7.

Logo, a solução da equação é:

$$\begin{cases} x = 13 + 11k \\ y = -6 - 7k \end{cases} .$$

Observe que os valores que multiplicam k são os coeficientes da equação diofantina linear simplicificada, justificado em 3.3.2.2 .

b) $90X - 29Y = 22$.

Resolução: De fato, inicialmente, dividiremos ambos os membros da igualdade por 2, assim:

$$[90x - 28y = 22] : 2$$
$$45x - 14y = 11.$$

Como $(45, 14) = 1$, concluímos que existe solução para a equação:
$x = \dfrac{11 - 14y_0}{45}$ $(\star) \Rightarrow y = \dfrac{-11 + 3.x}{14} + 3.x \in \mathbb{Z}$.
Por outro lado temos também que: $x = -1 + 14t$ $(\star\star)$

Substituindo $(\star\star)$ em $(\star)$ teremos.

$$y = \frac{-11 + 45.(-1 + 14t)}{14} \Rightarrow y = \frac{-11 - 45 + 4.14t}{14}$$
$$\Rightarrow y = \frac{-56 + 45.14t}{14}$$
$$\Rightarrow y = -4 + 45t.$$

Logo, a solução da equação é:

$$\begin{cases} y = -4 + 45t \\ x = -1 + 14t \end{cases} .$$

.

02. (OBM-98) No planeta Z todos os habitantes possuem 3 pernas e cada carro possui 5 rodas. Em uma pequena cidade desse planeta, existem ao todo 97 pernas e rodas. Então podemos afirmar:

a) É possível que existam 19 carros nessa cidade.

b) Existem no máximo 16 carros nessa cidade.

c) Essa cidade têm 9 habitantes e 14 carros.

d) Essa cidade possui no máximo 17 carros.

e) Nessa cidade existem mais carros do que pessoas.

Resolução:

Note que, chamando de x a quantidade de carro e y a quantidade de pessoas nesta cidade, podemos escrever:

$$5x + 3y = 97.$$

Tendo que como valores de x e y números inteiros, temos uma equação diofantina.

Como $(3, 5) = 1$ e $1 \mid 97$, temos soluções inteiras para a equação.

[1] Pelo algorítmo de MDC teremos:

Quoc.	1	1	
5	3	2	$1 \Rightarrow MDC$
Rest.	2	1	

[1] Perceba que é simples pensar em dois valores para serem solução trivial deste problema e criar o par de equações que informam as soluções, entretanto esse trabalho tem o intuito de mostrar para o leitor as diferentes formas de resolução.

Logo:

$5 = 1 \cdot 3 + 2 \Rightarrow 5 - 1 \cdot 3 = 2 \quad$ (I)

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

Substituindo (I) em (II)

$3 - 1(5 - 1 \cdot 3) = 1 \Rightarrow 3 - 5 + 1 \cdot 3 = 1 \Rightarrow 5(-1) + 3(2) = 1.$

Multiplicando os dois membros da igualdade por 97.

$$5 \cdot (-97) + 3 \cdot (194) = 97.$$

Portanto teremos como equações paramétricas:

$x = -97 + 3t$ e $y = 194 - 5t$ com $t \in \mathbb{Z}$.

Para que os valores dos possíveis números de carros sejam positivos teremos

$$x > 0$$

$$-97 + 3t > 0$$

$$3t > 97$$

$$t > 32,333...$$

Com $x = -97 + 3t$ e $y = 194 - 5t$

k	x	y
33	2	29
34	5	24
35	8	19
36	11	14
37	14	9
38	17	4
39	20	-1 (???)

Assim, essa cidade possui, no máximo 17 carros. *(Letra d)*

03. (ENQ - 2019.1)[2]

a) Determine o menor número natural c para qual a equação

$$5X + 7Y = c$$

[2] Esta questão veio no meu primeiro Exame Nacional de Qualificação e deixou muitos amigos atordoados. Não poderia faltar neste trabalho.

tenha exatamente 4 soluções em $\mathbb{N} \cup \{0\}$.

Resolução:

De modo geral, nesses tipos de problema que envolvem uma constante, faremos um passo inicial, para uma equação diofantina seja igual a 1, em seguida multplicaremos a equação por essa constante constante e por fim analisáremos o intervalo de soluções.

Logo, teremos:

$$5x + 7y = 1.$$

É fácil ver que, $(-4, 3)$ é solução desta equação, logo

$$5(-4) + 7(3) = 1 \Rightarrow 5(-4c) + 7(3c) = c.$$

Tendo assim $x_0 = 4c$ e $y_0 = 3c$, portanto $x = -4c + 7t$ e $y = 3c - 5t$, com $t \in \mathbb{Z}$.

Pelo enunciado da questão temos que $x \geq 0 \Rightarrow -4c + 7t \geq 0 \Rightarrow t \geq \frac{4}{7}c$. $(\star)$

Por outro lado, tem-se que $y \geq 0 \Rightarrow 3c - 5t \geq 0 \Rightarrow t \leq \frac{3}{5}c$. $(\star\star)$.

Com efeito, temos que as soluções destes problemas pertencem ao conjunto dos números naturais, e mais, temos 4 soluções para este problema, ou seja, 4 valores diferentes para t. Note que no mínimo a diferença entre a solução de x e y é igual a 3, poís pode ser que os quatro números estejam em sequência, assim teremos

$$\frac{3}{5}c - \frac{4}{7}c \geq 3 \Rightarrow c \geq 105.$$

Além disso, de $(\star)$ e $(\star\star)$ temos a desigualdade

$$\frac{3}{5}c \geq t \geq \frac{4}{7}c \quad \Rightarrow 63 \geq t \geq 60.$$

Concluindo os valores de t serão 60, 61, 62 e 63.

b) Determine, explicitamente, as 4 soluções obtidas no item (a).

Resolução:

Com efeito, sendo $x = -4c + 7t$ e $y = 3c - 5t$ e admitindo o valor $c = 105$ e os valores $t = 60,\ 61,\ 62\ e\ 63$ descobertos do item anterior, temos as soluções:

$(0, 15);\ (7, 10);\ (14, 5)\ e\ (21, 0)$.

04. Numa criação de coelhos e galinhas , contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?

Resolução:

Com efeito, chamaremos de de x o número de coelhos e y o número de galinhas, logo teremos a equação:

$$4x + 2y = 400 \Rightarrow 2x+y=200.$$

Como $(2, 1) \mid 200$ temos solução para este problema.

É facil ver que, uma solução possível para esse problema é $x_0 = 100$ e $y_0 = 0$, obentedo as paramétricas $x = 100 + t$ e $y = -2t$, com $t \in \mathbb{Z}$, sendo $x \geq 0$ e $y \geq 0$.

Contruindo uma tabela com algumas soluções possíveis.

x	y	t
100	0	0
99	2	-1
98	4	-2
...	...	...
50	100	-50
49	102	-51
...	...	...
0	200	-100

Por outro lado, o problema deseja que a diferença da quantidade de animais seja a menor possível, logo irei verificar qual o valor de t para que a quantidade de coelhos e galinhas sejam iguais.

$$x = y$$
$$\Rightarrow 100 + t = -2t$$
$$\Rightarrow t = -33,333...$$

Para $t = -33$ teremos o número de coelhos $x = 67$ e o número de galinhas $y = 66$. Assim obtendo uma diferença igual a 1. Note que se adotarmos $t = 34$ teremos $x = 66$ e $y = 68$, fazendo com a diferença não seja a menor possível.

05. (OBM - 99) Quantos são os pares (x, y) de inteiros positivos que satisfazem a equação $2x + 3y = 101$?

a) 13

b) 14

c) 15

d) 16

e) 17

Resolução:

Com efeito, nestes problemas, de modo geral, precisamos encontrar uma solução possível (x_0, y_0) para encontrar uma equação paramétrica que me informa todas as soluções inteiras da questão.

É fácil ver que $x_0 = 1$ e $y_0 = 33$ é uma solução possível desta equação. Logo,

$x = 1 + 3k$ e $y = 33 - 2k$, com $k \in \mathbb{Z}$.

Pelas condições do problema temos $x > 0$ e $y > 0$ então,

$$\begin{gathered} 1 + 3k > 0 \\ \Rightarrow 3k > -1 \\ \Rightarrow k > -\tfrac{1}{3} \\ \Rightarrow k \geq 0. \end{gathered}$$

Temos também,

$$\begin{gathered} 33 - 2k > 0 \\ \Rightarrow -2k > -33 \\ \Rightarrow k < \tfrac{33}{2} \\ \Rightarrow k \leq 16 \\ \text{Logo,} \quad 0 \leq k \leq 16. \end{gathered}$$

Assim, este problema possuirá 17 soluções para que (x, y) sejam inteiros positivos. (Letra e)

06. (Colégio Naval - 2018) Seja A o conjunto formado pelos pares (x, y), onde x e y são inteiros positivos tais que $2x + 3y = 2018$. Sendo assim, é correto afirmar que a quantidade de elementos do conjunto A é:

a) 256

b) 336

c) 512

d) 640

e) 720

Resolução:

O menor valor positivo pra y é 2, quando $x = 1006$.

Portanto, temos as soluções paramétricas?

$$x = 1006 - 3t$$

$$y = 2 + 2t$$

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

Daí,

$$1006 - 3t > 0$$

$$1006 > 3t$$

$$t < 1006/3$$

$$t < 335,33$$

$$t = 335 \text{ (máx)}.$$

Também,

$$2 + 2t > 0$$

$$t > -1$$

$$t = 0 \text{ (mín)}.$$

Logo, há 336 soluções inteiras positivas. (Letra B)

07. (Olimpíadas do Rio Grande do Norte - 95)(Adaptada) Um caixa automática de um banco só trabalha com notas de 5 e de 10 reais. Um usuário deseja fazer um saque de 100 reais. De quantas maneiras distintas a caixa eletrônica poderá fazer o pagamento?

Resolução:

De fato, de acordo com os dados do enunciado, podemos considerar a seguinte equação diofantina:

$$5x + 10y = 100.$$

Que é equivalente a

$$x + 2y = 20.$$

Note que $x_0 = 0$ e $y_0 = 10$ são soluções triviais.

Deste modo, temos a seguinte equação paramétrica

$$x = 0 + 2t \text{ e } y = 10 - t.$$

Como

$$x \geq 0 \text{ e } y \geq 0,$$
$$2t \geq 0 \text{ e } 10 - t \geq 0$$
$$t \geq 0 \text{ e } t \leq 10.$$

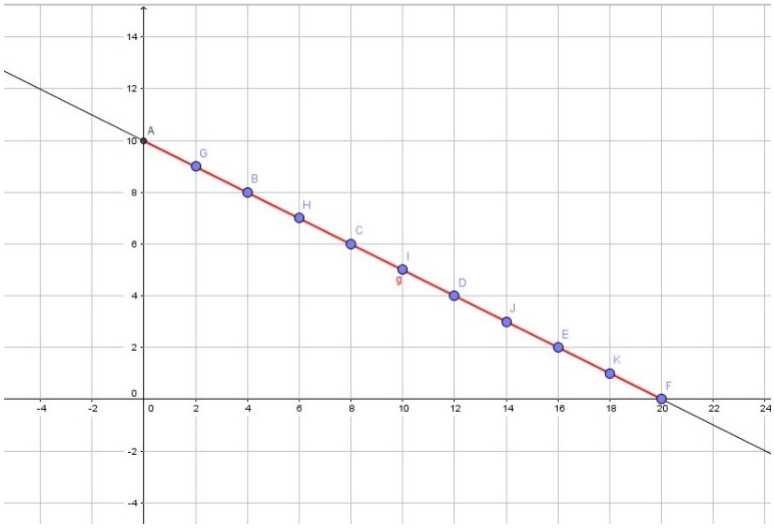
Deste modo,

$$0 \leq t \leq 10.$$

Logo, há 11 soluções possíveis.

Uma outra forma interessante de análisar e representar as soluções possíveis que o problema traz, é a exposição geométrica destes pares ordenados no plano cartesiano. A equação diofantina linear é representada por uma linha reta no sistema de coordenadas cartesianas, e a solução deste problema são alguns pontos pertencentes a reta. A Figura 8 apresenta estes pontos (A, B, C, D, E, F, G, H, I, J e K).

Figura 8 – Representação no plano cartesiano das soluções possíveis.



Fonte: Software de ensino GeoGebra.

Considerações Finais

Construir este trabalho foi de grande relevância pra mim, pois com ele, lancei uma proposta de um material que possa ser usado no ensino de equações diofantinas lineares, para alunos dos anos finais do fundamental 2 e do ensino médio. Acredito que possa ser utilizado como apoio por alunos e professores, para obterem um norte de como esta matéria é cobrada nas provas de olimpíadas e concursos militares, onde esse assunto é mais recorrente.

Conhecer os fatos históricos na construção e formalização do conjunto dos números inteiros, acredito que seja uma forma interessante de iniciar um conteúdo, a história da matemática é uma metodologia interessante para o início de diversos assuntos. E ao fim é possível concluir que esse conjunto numérico, apesar de parecer simples entender a sua base, é algo que demorou séculos para se oficializar.

Compreender a definição básica do conjunto dos números inteiros é algo bem corriqueiro, entranto as consequências que esse conjunto traz, é algo muito amplo, e muitas vezes complexo, que podem ser aplicadas nas formas mais diversas. Nesse trabalho tento esplanar alguns conceitos advindos deste conjunto e busco uma aplicação na resolução de problemas que o envolve.

Ao final desse trabalho propus algumas formas de como resolver certos problemas clássicos que circundam as equações diofantinas lineares com duas incógnitas, sempre tentando resolvê-las de formas diferentes e usando conceitos básicos de matemática. Com a pequena experiência com as olimpíadas de matemática que tenho, percebi que os métodos de resolução de um mesmo problema podem ser os mais variádos possíveis, e cada um desses métodos podem agradar estudantes diferentes. Assim sendo, optei por diversificar os métodos de resoluções.

Meu intuito na construção desse trabalho, não foi esgotar o conhecimento do assunto número inteiros, muito pelo contrário, foi dar uma pequena base de como começar a estudá-lo com um olhar um pouco mais aprofundado, em relação ao ensino básico tradicional, para que a partir daí o próprio aluno, baseado neste material, busque outras fontes para conhecer o conjunto dos números inteiro cada vez mais. E ainda, dei preferência por não resolver as equações por congruência aritmética (um outro método de resolução), visto que também não é um conhecimento usual nestas séries. Sempre optei pelo uso de uma matemática mais acessível na resolução da questões que propus. Ratificando que, acredito que após o estudo e compreesão deste material, o aluno estará apto a aprender e aprofundar um pouco mais sobre equações diofantinas, não só lineares ou com apenas duas incógnitas, mas abrir um leque de questões e métodos de resoluções diferentes.

Referências

BERLINGHOFF, W. P.; GOUVÊA, F. Q. *A matemática através dos tempos: um guia fácil e prático para professores e entusiastas*. [S.l.]: Editora Blucher, 2008. Citado na página 16.

BOMBELLI, R. *LÁlgebra*. [S.l.]: 1966, 1572. Citado na página 17.

BOYER, C. B. *História da Matemática.(2ª edição)*. [S.l.: s.n.], 1996. Citado na página 17.

EVES, H. W. *Introdução à história da matemática*. [S.l.]: Unicamp, 2004. Nenhuma citação no texto.

FOSSA, J. A.; ANJOS, M. F. dos. Sobre a incompatibilidade dos números negativos com o conceito grego de rithmós. *Revista Brasileira de História da Matemática*, v. 7, n. 14, p. 163–171, 2007. Citado na página 16.

FREITAS, C. W. A. Equações diofantinas. 2015. Nenhuma citação no texto.

HEFEZ, A. *Elementos de aritmética*. [S.l.]: Sociedade Brasileira de Matemática, 2006. Nenhuma citação no texto.

HEFEZ, A. *Aritmética: Coleçao PROFMAT, 2ª Ediçao*. [S.l.: s.n.], 2016. Nenhuma citação no texto.

MAIA, L. F. Equações diofantinas. 2018. Nenhuma citação no texto.

MARI, J. G.; BUSTOS, D. I. et al. Los números enteros. *Síntesis*, 1990. Nenhuma citação no texto.

OLIVEIRA, M. R. d.; PINHEIRO, M. R. d. R. *Coleção Elementos da Matemática 1: Conjuntos, Funções e Aritmética*. [S.l.]: GTR, 2010. Nenhuma citação no texto.

STRUIK, D. J. *História concisa das matemáticas*. [S.l.]: Gradiva Lisboa, 1992. Nenhuma citação no texto.

SÁ, P. F. d.; ANJOS, L. J. S. D. Aspectos históricos da construção dos números negativos. Citado 2 vezes nas páginas 18 e 19.

TEX2, E. abn. Modelo canônico de trabalho acadêmico com abntex2. 2018. Nenhuma citação no texto.