UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

CARLOS WAGNER ALMEIDA FREITAS

EQUAÇÕES DIOFANTINAS

FORTALEZA

2015

CARLOS WAGNER ALMEIDA FREITAS

EQUAÇÕES DIOFANTINAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de Concentração: Equações Diofantinas.

Orientador: Prof. Dr. José Robério Rogério

FORTALEZA

2015

CARLOS WAGNER ALMEIDA FREITAS

EQUAÇÕES DIOFANINAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 30 / 03 / 2015.

BANCA EXAMINADORA

Prof. Dr. José Robério Rogério (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará (UFC)

Prof. Dr. João Montenegro de Miranda
Universidade Estadual do Ceará (UECE)

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

F936e Freitas, Carlos Wagner Almeida
Equações Diofantinas / Carlos Wagner Almeida Freitas.
– 2015.
201 f. : il., enc.; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2015.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Dr. José Robério Rogério.

1. Equações diofantinas. 2. Teoria dos números. 3. Máximo divisor comum. I. Título.

CDD 512.72

AGRADECIMENTOS

A Deus em primeiro lugar, por me abençoar com a sua maravilhosa Graça. Também pelas tuas misericórdias que se renovam a cada dia, pelo teu infinito amor, pela tua justiça perfeita e pela tua retidão, pois sem o Senhor eu nada teria realizado.

A minha querida esposa, NAYARA, por toda paciência, compreensão, carinho e amor, me deixando mais tranquilo nos momentos mais difíceis do curso e por me ajudar nos momentos mais difíceis. Sempre me dando apoio nas minhas decisões, por mais que algumas prejudiquem algumas das partes. Você foi à pessoa que compartilhou comigo os momentos de tristezas e alegrias. Além deste trabalho, dedico todo meu amor a você.

A minha mãe, Leoneide, que sempre confiou e acreditou no potencial que Deus me concedeu. Também quero dedicar todo o amor que sinto pela senhora, te amo mãe.

A minha família que me deu apoio nos momentos críticos, sem falar na compreensão com relação ao pouco tempo de atenção dedicado a ela durante essa caminhada.

Aos professores exemplares do núcleo PROFMAT-UFC que estiveram sempre dispostos a nos ensinar, auxiliar, ajudar e aconselhar quando necessário.

Aos colegas de turma que vivenciaram comigo o prazer de um crescimento pessoal e profissional, passando por momentos de dedicação, preocupação e descontração.

Ao professor orientador José Robério Rogério que com suas dicas e sua paciência me conduziram ao cumprimento desse trabalho.

A CAPES pelo auxílio financeiro nesses dois anos; sendo fundamental para os gastos necessários.

RESUMO

O atual trabalho tem como objetivo principal estruturar estudantes, professores e amantes da matemática para a melhor compreensão, interpretação e resolução de problemas que venham a ser solucionados usando-se as Equações Diofantinas. Para isso, foram usadas técnicas como o uso de inequações e o método paramétrico que são conteúdos estudados pelos professores do Ensino Fundamental e Médio. Também foi utilizada para isso a apresentação de vários exemplos, todos resolvidos, que servirão como objeto de estudo para professores, universitários, estudantes escolares e amantes da matemática. No primeiro capítulo abordaremos os fatos históricos de grandes matemáticos que contribuíram com o desenvolvimento das Equações Diofantinas. Já no segundo capítulo, vamos conhecer melhor a essência da Teoria Elementar dos Números, apresentando, demonstrando e exemplificando as ferramentas matemáticas que serão utilizadas na resolução das Equações Diofantinas. Por fim, no terceiro capítulo, introduziremos as Equações Diofantinas e os métodos de determinação de soluções das mesmas, aplicando-as em situações-problema do cotidiano. A conclusão desse trabalho enfatiza a importância da compreensão algébrica e geométrica das Equações Diofantinas, e que o contato com problemas desta área contribua para que o leitor desenvolva de modo criativo, suas habilidades cognitivas. É importante ressaltar que a introdução à resolução de problemas dessa natureza não necessita de conhecimentos superiores, podendo ser abordado no Ensino Fundamental e Médio.

Palavras-chave: Referencial Histórico. Teoria dos Números. Divisão Euclidiana. Máximo Divisor Comum. Equações Diofantinas.

ABSTRACT

The current work has as objective main to structuralize students, professors and loving of the mathematics for the best understanding, interpretation and resolution of problems that come to be solved using the Diofantinas Equations. For this, they had been used techniques as the use of inequalities and the parametric method that are contents studied for the professors of Basic and Average Education. Also the presentation of some examples, all decided, that they will serve as object of study for professors, college's student was used for this, pertaining to school and loving students of the mathematics. In the first chapter we will approach the facts historical of great mathematicians who had contributed with the development of the Diofantinas Equations. No longer according to chapter, we go to better know the essence of the Elementary Theory of the Numbers, presenting, demonstrating and exemplifying the mathematical tools that will be used in the resolution of the Diofantinas Equations. Finally, in the third chapter, we will introduce the Diofantinas Equations and the methods of determination of solutions of the same one, applying them in situation-problem of the daily one. The conclusion of this work emphasizes the importance of the algebraic and geometric understanding of the Diofantinas Equations, and that the contact with problems of this area contributes so that the reader develops in creative way, its cognitive abilities. It is important to stand out that the introduction to the resolution of problems of this nature does not need superior knowledge, being able to be boarded in Basic and Average education.

Key words: Reference History. Theory of the Numbers. Euclidean Division. Maximum Common Divider. Diofantinas Equations.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\in$	Pertence
$\pm$	Mais ou menos
$\mp$	Menos ou mais
$>$	Maior do que
$\geq$	Maior do que ou igual a
$<$	Menor do que
$\leq$	Menor do que ou igual a
$\mid$	Divisibilidade exata
$\nmid$	Divisibilidade não exata
$\neq$	Diferente
$\equiv$	Equivalente a; Côngruo a
$\Longrightarrow$	Implica; Acarreta
$\Leftrightarrow$	Se, e somente se; Equivalente (no caso de proposições)
$\exists$	Existe; Existe um; Existe pelo menos um
$\sum_{i=1}^{n} P(i)$	Somatório de P(i), em que i varia de 1 a n
$\prod_{k=1}^{n} P(k)$	Produtório de P(k), em que k varia de 1 a n
$/$	Tal que
$\forall$	Para todo; Qualquer que seja
$\approx$	Aproximadamente
$\subset$	Está contido
$\emptyset$	Conjunto vazio
$f : A \rightarrow B$	Função entre os conjuntos A e B

SUMÁRIO

1 INTRODUÇÃO

A ideia de desenvolver uma pesquisa sobre o tema “Equações Diofantinas” surgiu após meu contato com a disciplina de Teoria dos Números, pela Universidade Federal do Ceará, tema este que praticamente não é estudado pelos alunos do ensino fundamental e médio, e quando sim, pouco se é trabalhado a respeito.

A importância do ensino e da aprendizagem matemática devem possibilitar a expressão e a argumentação do aluno em diferentes linguagens (natural, aritmética, algébrica e gráfica), quando enfrentarem situações-problema e tomarem decisões que extrapolem a capacidade do âmbito original, examinando e percebendo outras possibilidades de enfrentamento dos contextos e possibilitando outros pontos de vista.

Este trabalho tem como objetivo mostrar que podemos e devemos ensinar as equações diofantinas aos alunos a partir dos últimos anos do Ensino Fundamental, apesar de não fazer parte dos conteúdos usualmente abordados. Então podemos fazer a exposição dos fatos históricos, dos conceitos e das definições, dos axiomas, das demonstrações de teoremas ou proposições e das aplicações que se relacionem com o cotidiano, capacitando-os de um modo sistemático a resolução dessas aplicações, que é bem mais eficiente do que a estratégia de solucionar por tentativa e erro que é apresentada normalmente.

Ao estudar as equações diofantinas, o estudante escolar terá o privilégio de conhecer um pouco do verdadeiro alicerce matemático, isto é, da essência básica matemática, daquilo que mais encanta os olhos e as mentes de seus adeptos, admiradores e estudiosos. O que mais fascina é o fato de que uma vez demonstrado determinado teorema, tal demonstração torna o teorema válido eternamente. No decorrer da história da humanidade existiram poucas mentes brilhantes que foram capazes de realizar tal feito e ao estudar as equações diofantinas, iremos vivenciar alguns dos grandes feitos realizados por estas mentes geniais.

Entretanto, antes de estudar as equações diofantinas, os alunos devem estar habilitados a diversos campos da matemática e assim utilizá-los e ampliá-los,

desenvolvendo de maneira mais ampla capacidades tão importantes quanto as de abstração, raciocínio em todas as suas vertentes, resolução de problemas de vários tipos, investigação, análise e compreensão de fatos matemáticos e de interpretação da própria realidade.

Nas resoluções de problemas cuja interpretação chega a uma Equação Diofantina, as ferramentas matemáticas utilizadas para o algoritmo são essencialmente conceitos previstos do Ensino Fundamental, tais como os números naturais e inteiros com suas propriedades e operações básicas, números primos e decomposição em fatores primos, algoritmo da divisão, estudo da divisibilidade, múltiplos, divisores, máximo divisor comum, mínimo múltiplo comum, critérios de divisibilidade e equação da reta, o que torna plausível o estudo em questão. Faremos uma revisão básica de alguns desses conteúdos com maior precisão, reformulando e apresentando mais proposições e mostrando outras alternativas de abordagem e cálculo, que nos levam a compreender e determinar as soluções destas equações.

Com o objetivo de organizar e estruturar o aprendizado sobre Equações Diofantinas e mostrar um resumo da história envolvida nesse processo, dividiremos este trabalho em três capítulos.

No primeiro capítulo apresentaremos um referencial histórico de Diofanto de Alexandria autor do tema principal deste trabalho. Também apresentaremos um resumo histórico de outros autores, que são Euclides, Pierre de Fermat, Leonhard Euler e Carl Friedrich Gauss, pois estes em muito contribuíram para a Álgebra, e em particular para as Equações Diofantinas.

No segundo capítulo faremos uma revisão básica à Teoria dos Números, com o objetivo de introduzir os resultados básicos da Teoria Elementar dos Números, desenvolver mecanismos de reconhecimento de padrões numéricos, introduzir o rigor nas demonstrações das proposições e mostrar suas aplicações através de exemplos. Este capítulo está dividido em dez seções, que são: conjuntos numéricos: naturais e inteiros; fatorial; axiomas de Peano; ordem dos números naturais; indução; divisibilidade; divisão euclidiana; máximo divisor comum; números primos e congruência, distribuídos nesta ordem. Cada seção contém um relato histórico, conceitos e definições,

proposições com suas demonstrações e inúmeros exemplos; sendo a divisão euclidiana o resultado mais importante.

Já no terceiro capítulo apresentaremos o estudo das Equações Diofantinas. Aqui dividimos o capítulo em seis seções, que estão organizadas da seguinte forma: métodos fundamentais para resolução de Equações Diofantinas; Equações Diofantinas de duas variáveis; aplicações da seção anterior tais como resolução de situações-problema e utilização dos programas Maple e Winplot; utilizando congruência para resolver Equações Diofantinas; Equações Diofantinas lineares com n variáveis e suas aplicações. Na primeira seção introduziremos métodos elementares tais como a decomposição, a aritmética modular, a indução matemática e a descida infinita de Fermat, com o objetivo de resolver algumas Equações Diofantinas. Na segunda seção demonstra-se um teorema que estabelece as condições necessárias e suficientes para que uma Equação Diofantina Linear tenha solução. Na terceira seção aplicaremos os conhecimentos e técnicas, apresentadas na segunda seção, na interpretação e resolução de problemas que envolvem tais equações, pretendendo-se também desenvolver uma integração entre Álgebra e Geometria ao utilizar os programas computacionais Winplot e Maple como suportes para a resolução e visualização gráfica das soluções inteiras das equações estudadas. Na quarta seção introduzimos a aplicação do importante conceito de congruência nas Equações Diofantinas, não deixando de discutir também o chamado Teorema chinês do resto. Nas quinta e sexta seções, abordaremos métodos de resoluções das Equações Diofantinas lineares com n variáveis e suas aplicações cotidianas.

Este trabalho é destinado não só a estudantes do ensino fundamental e médio, mas também a professores, universitários, participantes de competições matemáticas, assim como a qualquer interessado em matemática. Por fim esta dissertação deseja mostrar a importância e o desenvolvimento da interpretação algébrica e geométrica das Equações Diofantinas, e que o contato com este trabalho permita ao leitor conjecturar, comparar e estabelecer estratégias mentais de forma criativa na resolução de situações-problema de outras áreas do conhecimento relacionando-as com as tais equações.

2 REFERENCIAL HISTÓRICO

"A matemática é uma vasta aventura em ideias; sua história reflete alguns dos mais nobres pensamentos de incontáveis gerações".

(Dirk J. Sruik)

Iniciaremos esta seção histórica, contemplando um pouco da história do matemático Diofanto, autor das Equações Diofantinas, tema principal desta dissertação. Em seguida, abordaremos também um pouco da história de outros matemáticos que contribuíram de modo excepcional para a Álgebra, em particular para às Equações Diofantinas, que são Euclides, Pierre de Fermat, Leonhard Euler e Carl Friedrich Gauss.

2.1 Diofanto

Figura 1: Imagem de Diofanto adulto com um escrito de um epitáfio em seu túmulo.

Cerca de um século após Cláudio Ptolomeu, acredita-se que por volta de 250 d.C., um grande talento matemático floresceu na Universidade, o matemático

Diofanto de Alexandria e sua enorme contribuição, se deu nos campos da Álgebra e da Teoria dos Números. Pouco se sabe da vida de Diofanto, sendo inclusive incerto o período em que viveu, presume-se que nasceu em cerca de 200 d.C. em Alexandria, no Egito, uma colônia grega e morreu em cerca de 284 d.C., também em Alexandria. O único dado pessoal sobre ele encontra–se sob forma de problema, na chamada Antologia grega do 5º ou 6º século, onde Antólios Bispo de Laodiceia sendo um matemático de talento, que começou seu episcopado em 270 d.C, dedicou um livro à seu amigo Diofanto, no qual ele permite calcular quantos anos Diofanto viveu:

> Deus lhe concedeu ser menino pela sexta parte de sua vida, e somando sua duodécima parte a isso, cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança; depois de viver a metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números, ele terminou sua vida.

Resolvendo esse enigma, a equação que representa o problema será:

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

Concluímos que ele viveu 84 anos, se caso esse enigma for historicamente exato.

Outra forma de enunciar este enigma é “Diofanto passou 1/6 de sua vida como criança, 1/12 como adolescente e mais 1/7 na condição de solteiro. Cinco anos depois de se casar nasceu-lhe um filho que morreu 4 anos antes de seu pai, com metade da idade (final) de seu pai”.

Encontramos menção em Rocque e Pitombeira (1991) que as obras de Diofanto de Alexandria não obedecem à tradição clássica grega para os textos matemáticos, não se assemelhando e nem formando a base da Álgebra elementar dos dias atuais. Sua obra aproximava-se mais da álgebra babilônica no que se refere a

encontrar as soluções numéricas de uma equação. Porém, enquanto que os matemáticos babilônicos se ocupavam principalmente com soluções aproximadas de equações determinadas, a obra de Diofanto de Alexandria é quase toda dedicada à resolução exata de equações, tanto determinadas como indeterminadas.

Seguramente Diofanto escreveu três tratados: Aritmética, em 13 livros dos quais 6 sobreviveram, Sobre Números Poligonais, do qual restaram fragmentos, e Porismas, que foi perdido. Seu tratado Aritmético (no grego, significa "ciência dos números") é uma obra-prima, pioneira no tratamento do difícil assunto a que hoje chamamos de Teoria dos Números, sem deixar qualquer dúvida de que seu autor era um gênio do mais alto nível. Apesar de Euclides e outros já terem feito algumas descobertas importantes nessa área, Diofanto realizou avanços incomparáveis, mostrando em seu livro sucessivos exemplos das melhores qualidades de um grande matemático. Na dedicatória de Arithmetica, Diofanto escreve a Dionísio (muito provavelmente o bispo de Alexandria) que, embora o material do livro seja difícil, "*tornar-se-á fácil de dominar, com o seu entusiasmo e a minha capacidade de ensinar*". Segundo estudiosos, em sua obra "Aritmética", Diofanto só se interessava por soluções racionais positivas, não aceitando as negativas ou as irracionais. Aritmética é considerada o primeiro manual de álgebra que usa símbolos para indicar incógnitas e potências, e apresenta a resolução exata de equações indeterminadas. As outras obras tratam de um trabalho sobre frações, introduzindo o emprego de números fracionários. Os problemas estudados por Diofante são problemas indeterminados que exigem soluções inteiras (ou racionais) positivas e envolvem, em geral, equações de grau superior ao primeiro. Na Aritmética, ele resolve 130 problemas de naturezas variadas, como equações do primeiro, segundo e até terceiro graus. Ela foi encontrada em Veneza por Johann Müller (matemático e astrônomo alemão) em 1464 e a primeira tradução se deve a Wilhelm Holzmann (1532-1576). Essa obra representa, essencialmente, um novo ramo à matemática usando um método diferente de tudo que se conhecia na época. Lins e Gimenez (2005) apontam que Diofanto solucionava os problemas expostos utilizando aplicações numéricas específicas, introduzindo diversas técnicas de resolução, porém sem recorrer à teorização. Em 1621, aparece a edição de Bachet de Méziriac com o seguinte título: *Diophanti Alexandrini Arithmeticorum libri sex; et de Numeris multangulis liber unus. Nunc primun graece et latini editi atque absolutissimis*

commentariis illustrati, Paris 1621 (que contém para além do texto grego e a tradução em latim, esclarecimentos e notas).

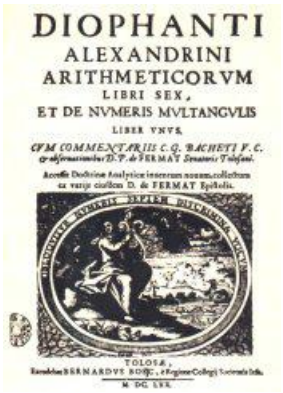
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
TOLOSÆ,

Figura 2. Capa do Livro *Aritmética*

Com relação aos seis livros recuperados da obra Aritmética, temos que:

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

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

Foi numa cópia do livro *Aritmética*, nas margens desse problema de número 8, no qual se achavam descritas as infinitas soluções da equação pitagórica $x^2 + y^2 = z^2$ que Pierre de Fermat (1601 - 1665) escreveu:

> Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que, todavia esta margem não é suficientemente grande para cabê-la.

Esta afirmação, conhecida como o *Último Teorema de Fermat*, só foi demonstrada em 1995, pelo matemático inglês Andrew Wiles. Alguns acreditam que a demonstração de Fermat não estaria totalmente correta, outros, que seria realmente uma

demonstração brilhante, uma vez que Wiles usou conhecimentos sofisticados e modernos em sua demonstração.

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

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

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

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

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

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

Vejamos alguns problemas dos livros da obra Aritmética:

Problema 1. (Problema 8, Livro II) Decompor o quadrado 16 em dois quadrados.

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

Problema 2. Dividir um número dado em dois números de diferença dada.

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

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

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

Problema 3. (Problema 15, Livro III) Encontrar três números tais que o produto de quaisquer dois somado à soma deles seja um quadrado.

Problema 4. (Problema 17, Livro I) Encontrar quatro números cuja soma três a três seja, respectivamente, 22, 24, 27 e 20.

Problema 5. (Problema 13, Livro III) Encontrar três números tais que o produto de quaisquer dois somado ao terceiro seja um quadrado.

Apesar de muitos problemas tratados no livro Aritmética estarem relacionados às equações diofantinas, Zerhusen, Rakes e Meece (2005) afirmam que a obra não contém problemas envolvendo as equações indeterminadas de primeiro grau, pois Diofanto não lhes atribuía qualquer importância.

Assim, Hefez (2005) aponta que Diofanto teve seu nome atribuído às equações diofantinas lineares como uma homenagem póstuma, dada por sua importância dentro do desenvolvimento da matemática.

A Aritmética de Diofanto foi uma espécie de garrafa lançada ao mar com uma importante mensagem: doze séculos depois de escrita, o matemático alemão Johann Muller encontrou em Pádua, na Itália, um exemplar em grego e reconheceu-lhe o valor. Em 1575 a obra foi traduzida e comentada por Wilhelm Holtzmann, da Universidade de Heidelberg, e foi com base nesse trabalho que o nobre francês Bachet de Méziriac publicou, em 1621, o texto grego acompanhado de sua versão em Latim. Contudo, depois de flutuar por mais de treze séculos, a garrafa acabou chegando às mãos de um pacato matemático amador francês, Pierre de Fermat, mais tarde conhecido como O Príncipe dos Amadores.

Diofanto é frequentemente chamado o pai da álgebra, mas talvez seja muito mais adequado tratá-lo como precursor da moderna teoria dos números, cujo ponto de partida seria o trabalho de Fermat no século XVII. É de realçar que o matemático persa al-Khwarizmi (780-850) partilha o título de “pai da álgebra” pelo seu próprio livro intitulado Álgebra, que continha uma solução sistemática de equações lineares e quadráticas. Al-Khwarizmi introduziu os numerais hindu-arábicos e os conceitos de

Álgebra na matemática europeia. As palavras algoritmo e álgebra decorrem do seu nome e al-jbr (é uma palavra árabe que significa operação matemática usada para resolver equações quadráticas), respectivamente.

Contudo, Diofanto foi pioneiro na criação de uma simbologia algébrica que, mesmo rudimentar, ajudava a tornar menos difíceis as representações de incógnitas, igualdades, somas, subtrações, inversos, potências, etc. Até o momento, o que existia era uma **álgebra retórica ou verbal**, conhecida também como desenvolvimento da álgebra pré-diofantina em que os argumentos da resolução de um problema são escritos em prosa pura, sem abreviações ou símbolos específicos; com Diofanto passou-se à **álgebra sincopada**, através do qual se adotavam algumas abreviações para as quantidades e operações que se repetiam mais frequentemente; somente no século XVI, de modo gradativo, começou a surgir à moderna **álgebra simbólica,** onde as resoluções se expressam numa espécie de taquigrafia matemática formada por símbolos que aparentemente nada têm a ver com os entes que representam.

Notemos que não há possibilidades de definir uma linha de demarcação exata acerca do desenvolvimento da álgebra na história da matemática. Visto que foram inúmeras influências em diferentes tempos que contribuíram para a formação da álgebra que estudamos.

Os Vários trabalhos de Diofanto foram preservados pelos Árabes e traduzidos em Latim no século XVI. Em Arithmetica, Diofanto interessou-se mais em encontrar soluções contendo números inteiros para equações como $ax^2 + bx = c$. Embora os Babilônicos conhecessem alguns métodos de resolução de equações lineares e quadráticas do tipo que fascinavam Diofanto, Ele é especial, de acordo com J. D. Swift, por ser o primeiro a introduzir notação algébrica extensiva e consistente, representando uma melhoria grandiosa em relação ao estilo puramente oral dos seus antecessores (e muitos sucessores). A redescoberta de Arithmetica através das fontes bizantinas contribuiu grandemente para o renascimento da matemática na Europa Ocidental e estimulou muitos matemáticos, entre os quais Fermat como expoente máximo.

As incursões de Diofanto na Geometria foram raras, mas em uma delas ele produziu uma pequena pérola, demonstrando, através de um diagrama geométrico, que no desenvolvimento do produto (a – b).(c – d) o produto (- b).(- d) é igual a (+ bd), ou seja, a famosa regra **menos vezes menos dá mais**. Isso precisa ser recebido com cuidado e bem entendido: trata-se de uma convenção que somos obrigados a estabelecer se quisermos que a propriedade distributiva do produto em relação à soma valha também para números negativos e essa é a essência da prova de Diofanto.

Por volta de 300 d.C., trabalhou na Universidade um geômetra de magnífico talento, conhecido como Pappus, de Alexandria. Pappus é considerado o último dos grandes geômetras gregos e, se a Idade de Ouro da Universidade foi o século de Euclides, Arquimedes e Apolônio, o século de Diofanto e Pappus foi a **Idade de prata**, o verdadeiro canto de cisne daquela célebre escola.

2.2 Euclides

Euclides de Alexandria que viveu aproximadamente entre 360 a 295 a.C., foi um professor, matemático e escritor. Teria sido educado em Atenas e frequentado a Academia de Platão, em pleno florescimento da cultura helenística. Convidado por Ptolomeu I para compor o quadro de professores da recém-fundada Academia, que tornaria Alexandria o centro do saber da época, tornou-se o mais importante autor de matemática da Antiguidade greco-romana e talvez de todos os tempos, com seu monumental Stoichia (**Os elementos**, 300 a.C.), uma obra composta de treze livros ou capítulos. Não é certo que tenham resultado do trabalho exclusivo de Euclides. Possivelmente, a obra foi fruto da colaboração de uma equipe de matemáticos coordenada por ele. Os primeiros quatro livros tratam de geometria plana elementar e estudam propriedades de figuras retilíneas e do círculo, abordando problemas cuja solução se faz com régua e compasso. O livro V aborda a teoria de proporções e o livro VI aplica essa teoria ao estudo de geometria. Os livros VII, VIII e IX versam sobre a teoria dos números. O livro X trata dos incomensuráveis e os livros XI, XII e XIII discorrem sobre geometria sólida. Vejamos um pouco mais sobre os assuntos abordados nos livros.

Livro I. Grande parte do conteúdo do livro I é conhecida por quem estuda geometria plana na escola: teoremas de congruência de triângulos, construções elementares com régua e compasso, desigualdades envolvendo ângulos e lados de triângulos, construções envolvendo retas paralelas. São apresentados definições e conceitos a serem usados no decorrer da obra. O livro I começa com 23 definições de intenso conteúdo intuitivo, estabelecidas tendo a realidade física como referência. No quadro abaixo, apresentamos algumas delas:

Figura 3. Iluminura do século XIV, em uma tradução latina dos *Elementos* de Euclides, atribuída a Adelardo de Bath; a figura feminina no papel de professora é provavelmente uma personificação da geometria — *The British Library*.

Os postulados e axiomas do livro I dos *Elementos* asseguram a existência de figuras geométricas fundamentais, tais como a reta e o círculo, a partir das quais as outras figuras geométricas são estabelecidas. Além disso, eles determinam propriedades do que hoje chamamos de *geometria euclidiana*: o espaço é homogêneo e infinito (toda reta finita pode ser dilatada continuamente, dois ângulos retos são iguais, as figuras geométricas não são alteradas por deslocamento). Além do mais, há a possibilidade de medir distâncias, uma vez que vale o Teorema de Pitágoras, provado em conjunto com seu recíproco no final do livro I.

Livro II. O livro II é pequeno, contém somente 13 proposições, e se ocupa de um tema conhecido hoje como álgebra geométrica. A álgebra, com seus artifícios simbólicos de representação e manipulação, só seria desenvolvida a partir da Idade Média. Euclides demonstra resultados de natureza algébrica de forma geométrica, com o uso de quadrados e retângulos. Soluções de alguns tipos de equações quadráticas também são apresentadas por meio da manipulação de áreas de quadrados e retângulos. Os gregos já sabiam da existência de grandezas incomensuráveis e ainda não dispunham do conhecimento de números reais para tratá-las. Assim, uma abordagem geométrica para problemas que hoje se acham dentro do domínio da álgebra parecia aos matemáticos gregos mais geral do que um tratamento genuinamente aritmético.

Livros III e IV. Os livros III e IV lidam com a geometria do círculo, material que possivelmente tem origem em Hipócrates de Quíos. O livro III inclui relações de interseção e tangências entre círculos e retas. Apresenta uma definição de tangente ao círculo da seguinte forma: "Uma linha reta que toca o círculo é qualquer linha reta que, encontrando o círculo, não corta o círculo". No livro IV são abordados problemas sobre a inscrição e a circunscrição de figuras retilíneas no círculo.

Livros V e X. O livro V trata da teoria de proporções de Eudoxo e o livro X aborda sobre os incomensuráveis. A matemática grega tendia a evitar proporções. Grandezas em razão da forma x : a = b : c eram tratadas geometricamente como uma igualdade de áreas do tipo cx = ab. A teoria de Eudoxo, uma das mais belas construções da matemática grega, contornou o problema da existência de incomensuráveis e colocou sobre bases sólidas toda a teoria geométrica envolvendo proporções. Ela é agrupada aos Elementos para ser aplicada nos livros subsequentes. O livro X faz uma classificação metódica de segmentos de reta incomensuráveis da forma

$$\sqrt{a} \pm \sqrt{\mathrm{b}}, \quad \sqrt{a \pm \sqrt{\mathrm{b}}}, \quad \sqrt{\sqrt{a} \pm \sqrt{\mathrm{b}}}$$

onde a e b são comensuráveis. O tratamento geométrico dispensado a esses objetos fazia Euclides considerar este como mais um livro de geometria.

Livros VII, VIII e IX. Esses livros são direcionados à teoria dos números, os quais, para os gregos, eram inteiros e positivos. Uma vez que nem todas as grandezas podiam ser representadas por números inteiros, Euclides agregava a cada número um segmento de reta e se referia a ele por AB. Não usava expressões do tipo "é múltiplo de" ou "é fator de". No lugar, empregava "é medido por" ou então "mede". O livro VII proporciona vinte e duas definições de tipos de números: par e ímpar, primo e composto, plano e sólido (produto de dois inteiros ou de três inteiros). As duas primeiras proposições do livro VII apresentam aquilo que hoje é conhecido como o algoritmo de Euclides para encontrar o maior divisor comum (maior medida comum, na linguagem de Euclides) de dois números. O processo é uma aplicação repetida do Postulado de Eudoxo. No livro IX, Euclides prova, dentre outros resultados, a infinitude dos números primos.

Livros XI, XII e XIII. O livro XI possui 39 proposições sobre geometria espacial. O livro XII se ocupa da medida de figuras, usando o método de exaustão. Ele inicia mostrando que polígonos análogos inscritos em dois círculos têm suas áreas em razão igual ao quadrado dos diâmetros dos círculos, para em seguida mostrar, usando o método de Eudoxo, que as áreas dos dois círculos seguem a mesma proporção. O processo é empregado ainda para o cálculo de volumes de pirâmides, cones, cilindros e esferas. Por fim, o último dos livros é dedicado ao estudo de propriedades dos quatro sólidos regulares, ou *sólidos platônicos*: cubo, tetraedro, octaedro, icosaedro (12 faces) e dodecaedro (20 faces). Um poliedro é regular se suas faces são polígonos regulares congruentes e, em cada vértice, o mesmo número de faces se encontram. Os sólidos platônicos têm um lugar relevante na filosofia de Platão, que associava os poliedros regulares aos elementos clássicos (terra, ar, água e fogo) e, deste modo, à própria composição do universo. Os sólidos platônicos já eram apreciados pelos pitagóricos, mas a demonstração de que existem apenas cinco poliedros regulares é devida a Theaetetus (417-369 a.C.), matemático ateniense contemporâneo de Platão. Provavelmente, boa parte do livro XIII se deve a esse matemático.

Considerando a importância de sua obra, pouco é conhecido sobre a vida de Euclides, onde e quando nasceu, ou sobre as circunstâncias de sua morte. Escrita em grego, à obra cobria toda a aritmética, a álgebra e a geometria conhecidas até então no mundo grego, reunindo o trabalho de seus predecessores, como Hipócrates e Eudóxio, e

sistematizava todo o conhecimento geométrico dos antigos e intercalava os teoremas já conhecidos então com a demonstração de muitos outros, que completavam lacunas e davam coerência e encadeamento lógico ao sistema por ele criado. Esta foi a mais brilhante obra matemática grega e um dos textos que mais influenciaram o desenvolvimento da matemática e da ciência. Foi um dos livros mais editados e lidos em toda a história, tendo sido usado como livro-texto no ensino de matemática até o final do século XIX e início do século XX. Após sua primeira edição foi copiado e recopiado inúmeras vezes e, versado para o árabe, tornou-se o mais influente texto científico de todos os tempos e um dos com maior número de publicações ao longo da história.

Os *Elementos* foram produzidos como um livro-texto, de caráter introdutório, cobrindo o que era considerado, na época, matemática elementar. A obra não se propunha a expor de forma exaustiva o conhecimento matemático de então ou a relatar resultados mais recentes e sofisticados. Euclides não foi o pioneiro na produção de livros-texto de geometria: Hipócrates de Quíos (470-410 a.C.) escreveu, mais de um século antes de Euclides, o primeiro livro-texto organizado de forma sistemática sobre geometria, do qual sobreviveram apenas fragmentos.

Pelas evidências que temos, não há descobertas matemáticas atribuídas a Euclides e sua contribuição foi, sobretudo no âmbito da compilação e da sistematização do conhecimento matemático. No entanto, há muito de originalidade em seu trabalho, tanto na forma de exposição quanto na estrutura das demonstrações. Euclides foi herdeiro de uma tradição matemática iniciada na Grécia pelo menos três séculos antes. Os Elementos incorporaram as ideias de Platão quanto à natureza abstrata dos objetos matemáticos, mas, sobretudo as de Aristóteles no que diz respeito à estrutura do conhecimento matemático e dos elementos lógicos usados em sua construção. A obra é rigorosa quanto à estrutura lógica, criteriosa na escolha das noções básicas: definições, axiomas e postulados admitidos sem demonstração, e clara nas demonstrações de proposições mais complexas a partir das mais simples. É um perfeito retrato do caráter abstrato e dedutivo da matemática grega.

Depois da queda do Império Romano, os seus livros foram recuperados para a sociedade européia pelos estudiosos árabes da península Ibérica. Escreveu ainda Óptica (295 a.C.), sobre a óptica da visão e sobre astrologia, astronomia, música e mecânica, além de outros livros sobre matemática. Entre eles citam-se Lugares de superfície, Pseudaria e Porismas. Algumas das suas obras, como Os elementos, Os

dados, outro livro de texto, uma espécie de manual de tabelas de uso interno na Academia e complemento dos seis primeiros volumes de Os Elementos, Divisão de figuras, sobre a divisão geométrica de figuras planas, Os Fenômenos, sobre astronomia, e Óptica, sobre a visão, sobreviveram parcialmente e hoje são, depois de A Esfera de Autólico, os mais antigos tratados científicos gregos existentes. Pela sua maneira de expor nos escritos deduz-se que tenha sido um habilíssimo professor.

2.3 Pierre de Fermat

Figura 4. Imagem de Pierre de Fermat.

Pierre de Fermat (1601-1665) foi um advogado e político francês que habitou na cidade de Toulouse. Fermat apreciava a matemática como um hobby e jamais atuou como matemático profissional. Entretanto, foi um dos maiores gênios fecundos da matemática do seu período. Deixou contribuições expressivas em diversas áreas, que o fazem ser visto como um dos precursores da atual teoria dos números e também como um dos criadores da geometria analítica e do cálculo diferencial. Fermat não escreveu obras completas, sendo que muitos dos seus trabalhos permaneceram manuscritos em vida e ficaram conhecidos por meio de cartas a seus amigos e colaboradores. Seu pai, Dominique de Fermat era um rico mercador de peles e lhe propiciou um ensino excepcional, primeiramente no mosteiro franciscano de Grandselve

e depois na Universidade de Toulouse. Ingressou no serviço público em 1631. Em 1652 ele foi promovido para Juiz Supremo na Corte Criminal Soberano do Parlamento de Toulouse, entretanto esta promoção se deu pela eventual chegada da praga, que levou a vida de grande parte da população da Europa. Neste mesmo ano Fermat também adoeceu e chegou-se a garantir que ele havia morrido, porém ele se recuperou e permaneceu vivo por mais de uma década. Sua morte, de fato, deu-se a 12 de Janeiro de 1665, em Castres.

Em razão de seu cargo, Fermat não podia ter muitos amigos para não ser incriminado de favoritismo em seus julgamentos, também em razão da tumultuosa fase que passava a França de então, com o Cardeal Richelieu sendo primeiro-ministro. Ao se averiguar a produção matemática de Fermat, percebe-se naturalmente a característica amadora predominante em seus trabalhos. Na verdade, com raríssimas exceções, ele não publicou nada em vida e nem fez qualquer apresentação sistemática de suas descobertas e de seus métodos, tinha as questões da matemática mais como desafios a serem resolvidos.

Considerado o Príncipe dos amadores, Pierre de Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Jurista e magistrado por profissão, dedicava à Matemática apenas suas horas de lazer e, mesmo assim, foi considerado por Pascal o maior matemático de seu tempo.

Contudo, seu grande gênio matemático perpassou várias gerações, fazendo com que várias mentes se debruçassem com respeito sob o seu legado, que era composto por contribuições nas mais diversas áreas das matemáticas, as principais: cálculo geométrico e infinitesimal; teoria dos números; e teoria da probabilidade. Entre os estudiosos com os quais mantinha contato postal, estão: Sir Kenelm Digby, John Wallis, Nicholas Hensius, além de Blaise Pascal, Assendi, Roberval, Beaugrand e o padre Marin Mersenne.

Em seus estudos de aritmética, Fermat retomou o trabalho de Diofanto, cujas obras, traduzidas para o latim, feitas por Claude Gaspar Bachet de Méziriac, um texto sobrevivente da famosa Biblioteca de Alexandria, queimada pelos árabes no ano 646 d.C., e que reunia cerca de dois mil anos de conhecimentos matemáticos, haviam despertado o interesse dos matemáticos desde o Renascimento. Fermat, de posse de uma tradução latina da *Aritmética* de Diofanto, fez comentários nas margens do livro que se tornariam célebres. Diofanto, em seus problemas, considerava soluções racionais, enquanto Fermat limitou o universo de soluções possíveis aos números inteiros. Seus

interesses principais em aritmética estavam nos números primos e nas propriedades de divisibilidade. Alguns dos resultados propostos por ele seriam demonstrados apenas por seus sucessores. Por exemplo, o chamado *Pequeno Teorema de Fermat*, que afirma que *"Se p é primo e a é um número não divisível por p o número* $a^{p-1} - 1$ *é divisível por p."*

A primeira demonstração desse resultado foi anunciada por Leonhard Euler em 1741. Fermat presumiu ainda que os números da forma $F_n = 2^{2^n} + 1$ fossem todos primos. Euler provou que a conjectura falha para $F_5 = 2^{32} + 1$.

A matemática do século XVII estava ainda se restaurando da Idade das Trevas, deste modo não é de se admirar o caráter amador dos trabalhos de Fermat. No entanto, se ele era um amador, então era o melhor deles, devido à precisão e à importância de seus estudos, que, diga-se também, estavam sendo realizados longe de Paris, o único centro que abrigava grandes matemáticos, mas até então ainda não prestigiados estudiosos da Matemática, como Pascal, Gassendi, Mersenne, entre outros.

O padre Marin Mersenne teve um papel importante na história da matemática francesa do século XVII e também foi uma das poucas amizades de Fermat. Entretanto, é importante observar mais de perto o desenvolvimento da Matemática nesta época.

Diferentemente da famosa escola pitagórica, os franceses não tinham o costume de trocar com os colegas os avanços recentes de suas pesquisas, devido à influência dos cosistas do século XVI, italianos que utilizavam símbolos para representar quantidades desconhecidas. Mersenne tinha o costume, desagradável para seus contemporâneos matemáticos, de divulgar os trabalhos dos pesquisadores. Em suas viagens pela França e por países estrangeiros, acabou conhecendo Fermat e trocando com ele várias correspondências. No entanto, mesmo com a insistência do padre, Fermat não publicou nada.

A mais célebre conjectura atribuída a Fermat ficaria conhecida como o Último Teorema de Fermat, que firma "Para $n > 2$, não existem números inteiros positivos x, y e z satisfazendo a identidade $x^n + y^n = z^n$." Este resultado foi conjecturado por Fermat em uma anotação escrita na margem da *Aritmética* de Diofanto. Fermat, usando um método indutivo, expôs uma demonstração do resultado para $n = 4$. Ressaltou, porém, que não havia espaço para escrever a demonstração do caso geral. Mesmo assim Fermat afirmou que tinha uma prova para a proposição. Ele escreveu sua afirmação nas margens do livro *Aritmética* de Diofanto, uma versão feita

por Claude Gaspar Bachet (1581–1683). Ele afirmou: "*Tenho uma prova maravilhosa para esta proposição, mas a margem é muito pequena para cabê-la*". Muitos matemáticos tentaram, sem sucesso, uma prova: Euler, Gauss, Dirichlet, Legendre, Lamé, Kummer, Dedekind entre outros. De fato, o Último Teorema de Fermat se transformou em um dos problemas mais célebres da história da matemática, atraindo a atenção de várias gerações de matemáticos e estimulando enormes desenvolvimentos na teoria dos números. Em setembro de 1994, o matemático Andrew Wiles, de Princeton, e seu estudante Richard Taylor concluíram uma prova, mas a demonstração satisfatória foi obtida em 1995, usaram fatos sobre curvas elípticas, que são métodos bem sofisticados, o que faz crer aos historiadores da matemática que, de fato, uma demonstração geral do resultado não estava ao alcance de Fermat.

Fermat se dedicou em reconstruir a obra *Lugares Planos*, de Apolônio, a partir das citações contidas na *Coleção* de Pappus. Nesse trabalho, Fermat descobriu, em 1636, o princípio básico da geometria analítica: uma equação envolvendo duas variáveis descreve uma curva no plano. Fez essa comprovação um ano antes da publicação da *Geometria* de Descartes e, por essa razão, Fermat pode ser considerado coinventor da geometria analítica. Fermat realizou estudos sobre equações de retas e de cônicas e abordou esses temas em um pequeno tratado intitulado *Introdução aos Lugares Planos e Sólidos*, publicado somente após a sua morte. Sua exibição era muito mais clara e ordenada que a de Descartes e seu método muito mais próximo da visão moderna. Por exemplo, Fermat faz uso de um sistema de eixos coordenados ortogonais. O uso de coordenadas representou um desenvolvimento histórico essencial na matemática, tendo aparecido em um contexto no qual as técnicas algébricas desenvolvidas pelos matemáticos medievais e renascentistas foram aplicadas aos problemas geométricos clássicos.

Fermat produziu mais um tratado intitulado Método para Encontrar Máximos e Mínimos. Fermat analisou curvas do tipo $y = x^n$, onde $n \in \mathbb{Z}$, hoje conhecidas como "parábolas" ou "hipérboles de Fermat", nos casos em que n é positivo ou negativo, respectivamente. Para curvas polinomiais da forma $y = f(x)$, determinou um método para achar os pontos de máximo e de mínimo que o coloca como um dos precursores do cálculo diferencial.

Fermat também desenvolveu um procedimento para encontrar tangentes a uma curva polinomial do tipo $y = f(x)$. Não apresentou justificativas convincentes para seu processo, limitando-se a dizer que ele era análogo àquele usado para encontrar

máximos e mínimos. Por isso, o método de Fermat não ganhou aceitação vasta pelos matemáticos de sua época.

Fermat também conseguiu resultados a respeito de áreas sob curvas, produzindo um procedimento para calcular, na notação moderna, $\int_a^b x^n \, dx$, para n fracionário, com $n \neq 1$. Generalizou um resultado de Bonaventura Cavalieri, outro dos precursores do cálculo.

2.4 Leonhard Euler

Figura 5. Leonhard Euler, pintura de 1753 — *Kunstmuseum Basel*, Suíça

Da bela cidade suíça de Basel também surgiu aquele que foi a maior mente matemática do século XVIII, um dos gênios que mais influenciaram os estudos adotados pela matemática moderna: Leonhard Euler (1707-1783). Euler estudou na Universidade de Basel, onde foi aluno de Jean Bernoulli, que desde cedo reconheceu a aptidão de seu pupilo para a matemática e investiu em seu desenvolvimento. Em 1727 Euler se transferiu para São Petersburgo, capital russa, onde adquiriu um posto na Academia de Ciências Imperial. Em 1741, a solicitação de Frederico da Prússia, aceitou um ofício na Academia de Berlim. Conviveu e trabalhou em Berlim até 1766, quando voltou para São Petersburgo. Euler foi considerado o matemático mais produtivo de seu tempo e, provavelmente, foi o mais prolífico matemático da história. Em sua vida, publicou 560 livros e artigos, número que se aproxima de 800 quando também contabilizados os manuscritos divulgados após sua morte. Em 1765, Euler perdeu a

visão de um de seus olhos, e, logo após seu retorno à Rússia, a visão em seu outro olho começou a deteriorar. E em 1766 ficou totalmente cego, porém manteve o ritmo de sua produção matemática até o final de sua vida, acreditando em sua memória e ditando seus trabalhos para um assistente.

Euler foi tão importante não somente para a matemática, mas também para a física, engenharia e astronomia. Euler escreveu sobre Álgebra, Geometria, Teoria dos Números, Topologia, Cálculo, Equações Diferenciais, Geometria Diferencial, Música, Astronomia, Mecânica, Engenharia, Acústica, etc. Euler escreveu livros que estruturaram diversas teorias, construídas a partir de resultados que se achavam dispersos e desordenados. Seus livros tiveram muita consideração e acabaram por estabelecer uma ampla parcela das notações e da terminologia hoje usadas na álgebra, na geometria e na análise.

Euler foi responsável pela admissão de vários símbolos aplicados na escrita matemática. A letra "*e*" para o número cujo logaritmo hiperbólico vale 1, foi introduzida por Euler, provavelmente tendo como referência a primeira letra da palavra exponencial. Apesar de que não tenha sido invenção sua, o símbolo π, significando a razão entre a circunferência e o diâmetro do círculo, passou a ter uso generalizado após ser metodicamente empregado por Euler. O ingresso do símbolo i para $\sqrt{-1}$ e das notações sin.v, cos.v, tang.v, cosec.v, sec.v, cot.v para as funções trigonométricas também são devidas a Euler. Em geometria, Euler constituiu a convenção de se usar letras minúsculas a, b e c para os lados de um triângulo e letras maiúsculas A, B e C para os ângulos opostos. Em escritos sobre teoria de probabilidades, introduziu a notação $\left[\frac{p}{q}\right]$ para o que hoje denotamos por $\binom{p}{q} = \frac{n!}{p!(n-p)!}$.

Seu pai era um padre calvinista que mantinha expectativas de que seu filho o precedesse no clericato. Ele instruiu a Euler a matemática. Quando seu filho entrou na Universidade de Basel, estudou Teologia e a língua Hebraica, e recebia a uma aula de uma hora por semana com Johannes Bernoulli. Ele fez amizade com Daniel e Nicolaus Bernoulli, e recebeu seu primeiro mestrado aos dezessete anos. Os Bernoullis, então, tiveram de convencer seu pai a deixá-lo prosseguir com a carreira acadêmica. Aos dezenove anos, Euler recebeu menção honrosa por uma solução que proclamou a um problema posto pela academia de Paris. Mais tarde, ele ganhou o primeiro prêmio nesta mesma competição doze vezes.

Os Bernoullis obtiveram para Euler uma posição de pesquisa na Academia de São Petersburgo, porém em Medicina, sob o reinado de Catarina I. Contudo, ela morreu logo após, e um regime de condições desordenadas se seguiu, com Euler passando à seção de matemática da Academia. Euler ansiou por muito tempo regressar à Europa, porém os constantes nascimentos de seus filhos o impediram. Entretanto, este foi um momento muito produtivo para ele – era arriscado falar ou até mesmo sair às ruas, consequentemente Euler meditou seus esforços na pesquisa e desenvolveu costumes que manteve pelo resto de sua vida. Euler também escreveu livros didáticos para escolas russas, supervisionou o departamento de geografia do governo e auxiliou a revisar o sistema de pesos e medidas. Ele continuou na Rússia até 1740, quando aceitou a solicitação de Frederico O Grande para ingressar na academia de Berlin, onde passou os próximos 24 anos. Euler, entretanto, não era tão sofisticado quanto os outros componentes da corte de Frederico e estes anos não foram completamente agradáveis para ele. Contudo, ele conviveu relativamente bem e manteve uma casa em Berlin assim como uma fazenda. A circunstância na Rússia melhorou bastante durante este tempo, e em 1766 Catarina A Grande o trouxe de volta a São Petersburgo. Ela deu a ele (e a seus 18 dependentes) uma casa mobiliada, e até mesmo um cozinheiro próprio.

Euler foi um cristão por toda a sua vida e frequentemente lia a Bíblia a sua família. Uma história sobre sua religião durante sua estadia na Rússia envolve o dito filósofo ateu Diderot. Diderot foi convocado à corte por Catarina, mas tornou-se inconveniente ao tentar converter todos ao ateísmo. Catarina solicitou a Euler que defendesse, e Euler disse a Diderot, que era ignorante em matemática, que lhe daria uma prova matemática da existência de Deus, se ele desejasse ouvir. Diderot disse que sim, e, conforme conta De Morgan, Euler se aproximou de Diderot e disse, sério, em um tom de perfeita convicção: "(a + bn) / n = x, portanto, Deus existe". Diderot ficou sem resposta, e a corte caiu na gargalhada. Diderot voltou imediatamente à França.

Euler teve contribuições a várias áreas da ciência, incluindo dinâmica dos fluidos, teoria das órbitas lunares (marés), mecânica, "A teoria matemática do investimento" (seguros, anuidades, pensões), bem como basicamente todas as áreas da matemática que existiam naquela época. Ele continuou sadio e alerta até o fim da sua vida, quando morreu de um derrame aos 76 anos. O trabalho ativo de Euler provocou uma tremenda demanda da academia de São Petersburgo, que permaneceu publicando seus trabalhos por mais de 30 anos após sua morte.

A memória de Euler era fabulosa, assim como suas capacidades de concentração. Chamado de "Análise Encarnada", ele era capaz de recitar toda a Eneida de cor, e nunca ficou perdido por interrupções ou desatenções, de maneira que boa parte de seu trabalho foi concretizado tendo suas crianças à sua volta. Ele era capaz de realizar cálculos extraordinários de cabeça, uma necessidade depois que ele ficou cego. Seu matemático contemporâneo, Condorcet, conta uma história onde dois dos discípulos de Euler estavam calculando independentemente uma sofisticada série infinita, e chegaram a uma discussão depois de somarem dezessete termos, por uma diferença na quinquagésima casa decimal. Euler resolveu o debate realizando a soma de cabeça.

Em sua obra *Introductio in analisin infinitorum* (Introdução à análise do infinito), de 1748, Euler analisou séries infinitas, tais como as de e^x, sen$x$ e cos$x$, e expôs a reconhecida relação e^{ix} = cos(x) + i.sin(x). Estudou curvas e superfícies a partir de suas equações, o que faz com que esse seja considerado o primeiro livro de geometria analítica. Seu aspecto mais ressaltante, no entanto, é o fato de ser o primeiro texto em que a noção de função surge como elemento essencial da análise matemática. Euler definiu função de uma quantidade variável como "uma expressão analítica composta de alguma maneira da quantidade variável e de números ou de quantidades constantes". Isto é, para Euler, uma função era uma expressão obtida a partir das operações fundamentais admitidas em seu tempo: polinomiais, exponenciais, logarítmicas, trigonométricas e trigonométricas inversas. A definição de Euler, apesar de ser imprecisa à luz da matemática moderna, englobava um universo limitado de funções. Euler buscou caracterizar as funções categorizando-as, de acordo com o modo como eram produzidas, entre algébricas e transcendentes, uniformes e multiformes, explícitas e implícitas. A notação $f(x)$ para uma função de x também foi introduzida por Euler. Ainda introduziu a conhecida fórmula V - A + F = 2 para qualquer poliedro simples com V vértices, A arestas e F faces.

Em seu livro *Institutiones calculi differentialis* (Fundamentos do cálculo diferencial), de 1755, e nos três volumes de *Institutiones calculi integralis* (Fundamentos do cálculo integral), publicados entre 1768 e 1774, além de proporcionar um tratamento mais extenuante da teoria do cálculo, Euler desenvolveu a teoria de equações diferenciais. É devida a Euler a distinção entre equações "lineares", "exatas" e "homogêneas", adotadas hoje nos cursos rudimentares de equações diferenciais. Euler foi o maior responsável pelos procedimentos de solução estudados nesses cursos: o uso

de fatores integrantes, o método de solução de equações lineares, a distinção entre equações lineares homogêneas e não homogêneas, as noções de solução particular e de solução geral.

Os trabalhos de Euler no campo de teoria dos números foram expressivos. Ele provou o Pequeno Teorema de Fermat e mostrou sua capacidade de computação demonstrando que $F_5 = 4.294.967.297$ não é primo. Euler colaborou para demonstração do Último Teorema de Fermat ao provar que, para n = 3, não existe solução inteira para a equação $x^n + y^n = z^n$.

2.5 Carl Friedrich Gauss

Figura 6. Gauss, litografia publicada na *Astronomische Nachrichten* em 1828.

Carl Friedrich Gauss (1777-1855) comprovou desde cedo uma admirável aptidão matemática. Sinônimo de genialidade soberana, de capacidade inexplicável, de raciocínio lógico em sua condição mais pura. Titã, Colosso de Rodes, Príncipe dos Matemáticos, foram alguns dos apelidos que seus colegas, com justificado respeito e admiração, concederam-lhe ao longo de uma das mais espetaculares carreiras já vistas nas Ciências Exatas. Filho de um honrado, mas inculto trabalhador braçal da cidade de Brunswick, Alemanha, ele tinha pouco mais de três anos quando mostrou ao pai uma

falha que este cometera ao calcular o quanto deveria pagar a alguns pedreiros que o auxiliavam. Conta-se a história de que, quando criança, seu professor, para manter a turma ocupada, solicitou aos alunos que somassem todos os números de 1 a 100. Gauss, sem fazer maiores cálculos, imediatamente apresentou o resultado correto, provavelmente usando a expressão n(n + 1) / 2 para a soma dos n primeiros números naturais. A habilidade do jovem estudante chamou a atenção do Duque de Braunschweig, sua cidade natal, que custeou sua educação. Em 1795, Gauss iniciou seus estudos na Universidade de Gottingen. No ano seguinte, aos 18 anos de idade, provou que o polígono regular de 17 lados poderia ser construído com régua e compasso. Até então, os únicos polígonos com número de lados primo construídos eram o triângulo e o pentágono regulares.

Gauss ainda não sabia se dedicaria a vida à Matemática ou a sua outra paixão, o estudo de línguas. Como Euler, ele era também um gênio linguístico e já dominava o Grego, o Latim, o inglês, o Francês e o Dinamarquês, com apenas 18 anos. Gauss concluiu seu doutorado em 1799. Na sua tese forneceu uma demonstração para o Teorema Fundamental da Álgebra: todo polinômio não constante com coeficientes complexos possui pelo menos uma raiz complexa. Falhas nas tentativas de demonstração deste teorema por d'Alembert foram corrigidas por Gauss. A demonstração contida em sua tese foi uma das quatro demonstrações para o Teorema Fundamental da Álgebra que ele produziria ao longo de sua vida.

Quando Gauss começou a trabalhar na sua obra *Disquisitiones arithmeticae* (Investigações aritméticas) em 1801, a teoria dos números era simplesmente uma bagunça de resultados isolados. Nessa obra ele introduziu a noção de congruência e, ao fazê-lo, agregou a teoria dos números. *Disquisitiones* contempla a aritmética modular, com base nas relações da congruência. Gauss também proclamou e provou o famoso teorema da reciprocidade quadrática, que ficou incompletamente demonstrado anos antes pelo matemático francês, Adrien-Marie Legendre (1752-1833). Entretanto, este teorema liga a solvabilidade de duas equações quadráticas relacionadas em aritmética modular. Em *Disquisitiones,* a abordagem de Gauss de criar teoremas, acompanhados de demonstrações, corolários e exemplos, foi usada por outros autores posteriormente.

Gauss ficou famoso quando, aos 24 anos de idade, calculou a órbita do planetoide de Ceres, um asteroide existente entre as órbitas de Marte e Júpiter. Descoberto em 1801 pelo astrônomo italiano Giuseppe Piazzi, esse corpo celeste teve sua órbita perdida em algumas semanas. A partir de poucas informações observacionais,

Gauss desenvolveu um método matemático que previu a órbita do planetoide. Conhecido como *método de Gauss*, ele envolvia a solução de uma equação de grau oito. Esse método ainda hoje é usado para rastrear satélites. O reconhecimento pelos trabalhos de Gauss em astronomia levou-o a ser designado, em 1807, diretor do observatório de Gottingen.

Desde o surgimento do cálculo diferencial e integral, os procedimentos dessa teoria foram empregados para o estudo de curvas e superfícies. Gauss, em sua obra *Disquisitiones circa superficies curvas* (Investigações sobre superfícies curvas), de 1827, inovou o estudo da geometria de superfícies ao utilizar procedimentos analíticos para explorar suas propriedades locais. O texto de Gauss foi marcante no desenvolvimento da geometria diferencial, apontando direções para o avanço da teoria. Nele, Gauss inovou ao analisar superfícies partindo de suas equações paramétricas. A partir da parametrização da superfície, Gauss estudou suas propriedades métricas. Conseguiu intensos trabalhos geodésicos, publicou uma obra-prima sobre Astronomia, chamada *Teoria motus corporum coelestium*; desenvolveu pesquisas sobre eletricidade e magnetismo, entre outras coisas.

Um tratado divulgado por Gauss em 1831 teve importância histórica por proporcionar a representação geométrica dos números complexos, estabelecendo a correspondência entre o número $z = x + iy$ e o ponto do plano cartesiano de coordenadas (x, y). Uma representação geométrica análoga dos números complexos já tinha sido obtida, em 1797, pelo norueguês Caspar Wessel (1745-1818). Entretanto, foi o trabalho de Gauss que a difundiu dentro da sociedade matemática, de tal maneira que o plano dos números complexos é hoje conhecido como *plano Gaussiano*. O termo "número complexo" também foi sugerido por Gauss, em substituição à nomenclatura "número imaginário", que ajudava a manter dúvidas sobre a existência desses objetos. Gauss contribuiu significativamente para a estruturação da teoria dos números complexos, sugerindo diversas aplicações à álgebra e à aritmética. Por exemplo, designou uma nova teoria de números primos, dentro da qual $5 = (1 + 2i).(1 - 2i)$ não mais era considerado primo.

Nos últimos anos de sua vida, muitas de suas publicações estiveram vinculadas ao seu trabalho no observatório astronômico. Nesse período, desenvolveu estudos dentro do que hoje é considerada matemática aplicada. Gauss, além de trabalhador incansável, era um perfeccionista, que só se permitia publicar trabalhos sobre teorias devidamente acabadas. Muitas de suas descobertas permaneceram em um

diário pessoal e não foram publicadas. Um exemplo disso são seus estudos sobre geometrias não euclidianas. Em seus anos de estudante em Gottingen, Gauss fez tentativas de demonstrar o postulado das paralelas, chegando à conclusão de que não era possível uma prova. As conclusões não publicadas de Gauss o tornariam inventor das geometrias não euclidianas. Gauss morreu aos 78 anos, em sua casa, no observatório de Gottingen, ainda desfrutando plenamente de seus incomparáveis dotes intelectuais.

3 INTRODUÇÃO BÁSICA A TEORIA DOS NÚMEROS

> *"Seis é um número perfeito nele mesmo, e não porque Deus criou o mundo em seis dias; a recíproca é que é verdade: Deus criou o mundo em seis dias porque esse número é perfeito, e continuaria perfeito mesmo se o trabalho de seis dias não existisse."*
>
> (Agostinho)

A Teoria dos Números é a parte da Matemática que se dedica em especial ao estudo dos números inteiros. Não existem dúvidas de que o conceito de inteiro é um dos mais antigos e fundamentais da ciência em geral, tendo acompanhado o homem desde os primórdios de sua história. Então, é de certo modo surpreendente que a Teoria dos Números seja atualmente uma das áreas de pesquisa mais efervescentes da Matemática e que, de forma intensa, continue a fascinar e desafiar as atuais gerações de matemáticos. São três os principais ramos em que se divide a Teoria dos Números: Teoria Elementar, Teoria Analítica e Teoria Algébrica. Neste capítulo vamos nos limitar à parte elementar, onde apresentaremos resultados básicos, através de Definições, Proposições e exemplos, que serão necessários para a fórmula geral que fornece o número total de soluções inteiras das Equações Diofantinas.

3.1 Conjuntos Numéricos: Naturais e Inteiros

Os números foram considerados durante milênios como entes intuitivos e algumas de suas propriedades, como por exemplo, a comutatividade e a associatividade da adição e da multiplicação, eram consideradas inerentes à sua própria natureza, e assim, não necessitando de demonstração. O enorme avanço matemático a partir da criação do Cálculo Diferencial, no século dezessete, colocou diante dos matemáticos

novos problemas que, para serem mais bem compreendidos e solucionados, requeriam uma fundamentação mais rigorosa do conceito de número. Os números naturais ainda resistiram às investidas por algum tempo. Só no final do século dezenove, quando os fundamentos de toda a matemática foram questionados e intensamente repensados, é que a noção de número passou a ser baseada em conceitos da teoria dos conjuntos, considerados mais primitivos. O grande capítulo da construção dos números ficou encerrado quando em 1888 Dedekind publicou um trabalho onde, a partir de noções básicas da teoria dos conjuntos, ele elabora um modelo para os números naturais, definindo as operações de adição e multiplicação e demonstrando as suas propriedades básicas. A construção de Dedekind não teve muita difusão na época por ser bastante complicada. Tornando-se mais popular com a axiomática que Giuseppe Peano deu em 1889. Para os números inteiros daremos um tratamento axiomático, tendo como ponto de partida uma lista de propriedades básicas que os caracterizarão completamente, para delas deduzir as demais propriedades.

A noção básica de conjunto não é definida, isto é, é aceita intuitivamente e, por isso, chamada noção primitiva. Ela foi utilizada primeiramente por Georg Cantor (1845-1918), matemático nascido em São Petersburgo. Segundo Ele, a noção de conjunto designa uma coleção de objetos bem definidos e discerníveis, chamados elementos do conjunto.

Denomina-se número natural a “tudo que for definido por um conjunto e, por todos os conjuntos que lhe sejam equivalentes.” (Bertrand Russel).

Consideremos o conjunto dos naturais como sendo,

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

isto é, o conjunto dos inteiros positivos.

O conjunto $\mathbb{Z}$ dos números inteiros é munido de duas operações, uma adição (+) que tem como elemento neutro o número inteiro zero (0) e uma multiplicação (.) que também tem seu elemento neutro, o número inteiro um (1). Consideremos o conjunto dos números inteiros como sendo,

$$\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \pm4, \pm5, \pm6,...\},$$

ou seja, o conjunto formado pelos números naturais e os números inteiros negativos, e

$$\mathbb{Z}^* = \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6,...\},$$

que representa os números inteiros não nulos,

$$\mathbb{Z}_+ = \{1, 2, 3, 4, 5, 6,...\},$$

que representa os números inteiros positivos, e

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

que representa os números inteiros negativos.

Sendo a e b dois números inteiros quaisquer, denotaremos por a + b a soma de a e b e a.b (ou ab) o produto de a por b.

Vejamos algumas propriedades que assumiremos aqui como axiomas.

I) A adição e a multiplicação são bem definidas:

$\forall\ a, b, c, d \in \mathbb{Z}$, $a = c$ e $b = d \Rightarrow a + b = c + d$ e $a.b = c.d$.

II) A adição e a multiplicação são comutativas:

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

III) A adição e a multiplicação são associativas:

$\forall\ a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a.b).c = a.(b.c)$.

IV) A multiplicação é distributiva com relação à adição:

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

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

1) $a = b$
2) $\exists\ c \in \mathbb{Z}^*,\ b = a + c$ (também equivale a dizer que $a < b$)
3) $\exists\ c \in \mathbb{Z}^*,\ a = b + c$ (também equivale a dizer que $b < a$)

VI) **Lei da Existência de Inversos Aditivos:** Para todo inteiro a existe um inteiro x tal que $a + x = x + a = 0$. Nesse caso, denotamos x por $-a$ que pode ser chamado também de oposto ou simétrico de a. Sendo a e b dois inteiros, define-se $a - b = a + (-b)$.

VII) **Lei do Cancelamento da Multiplicação:** Se $a, b, c \in \mathbb{Z}$, com $c \neq 0$ e $a.c = b.c$ então $a = b$.

VIII) **Lei do Cancelamento da Adição:** Se $a, b, c \in \mathbb{Z}$ e $a + c = b + c$ então $a = b$.

Curiosidades

I) Define-se googol ao número 1 seguido de 100 zeros, ou seja, 1 googol é igual a 10^{100}. A palavra “Googol” foi inventada em 1938, por um garoto americano de 9 anos, Milton Sirotta, a pedido do seu tio, o matemático Edward Kasner. Kasner usou o conceito de “googol” para explicar aos alunos, a diferença entre um número incrivelmente grande e o infinito. Esta palavra foi utilizada pelos fundadores do Google, Larry Page e Sergey Brinn, com o objetivo de ilustrar a enorme quantidade de informações que o sistema por eles criado, pretendia sistematizar. Este menino sugeriu, também, o nome googolplex para um número ainda maior do que o googol, o 1 googolplex = $10^{1\,googol}$.

II) Vivencie a seguinte brincadeira: Como adivinhar a idade do amigo (a)?

Instruções:

Peça que ele (ela) escreva dois dígitos cuja diferença seja maior do que um.
Que entre os dois dígitos escreva um algarismo qualquer.
Peça que inverta a ordem dos algarismos do número obtido.
Peça que diminua o menor número obtido do maior.
Peça que inverta a ordem dos dígitos da diferença acima obtida.
Peça que some o último número obtido ao resto anterior.
Peça que some o número obtido à idade do amigo (a).
Peça para ele dizer qual o último resultado obtido.
Você então dirá a idade do amigo (a).

Qual é o truque?

Solução.

Vamos imaginar que seu amigo escreveu os dígitos 7 e 2 e entre os dois colocou o número 4, formando o número 742. Seguindo as instruções, invertendo o número, obtém-se 247. Diminuindo o menor número do maior, tem-se: 742 – 247 = 495. Invertendo a ordem dos dígitos da diferença obtida, encontramos 594, que somado a 495 nos dá: 594 + 495 = 1089. Se a idade do amigo for, por exemplo, 17, você soma 1089 + 17 = 1106.

Qual é o truque?

O truque é o seguinte: qualquer que seja a escolha dos dígitos, antes de somar a idade do amigo, encontramos sempre o resultado 1089. Quando ele diz o resultado final, você subtrai 1089, obtendo a idade do amigo. Experimente com outros valores e comprove!

III) Um número é dito **perfeito**, segundo definição dos próprios pitagóricos que os classificaram, se for igual à soma de seus divisores, excluindo o próprio número. Exemplos: 6 = 1 + 2 + 3, 28 = 1 + 2 + 4 + 7 + 14, 496 e 8128 são números perfeitos.

Estes são os únicos números perfeitos menores que 10.000. O menor número perfeito, 6, era ligado, pelos escribas místicos e religiosos à perfeição; isso justifica por que a Criação de um mundo tão perfeito tenha necessitado apenas de 6 dias. Existe ou não uma infinidade deles? Ainda não se sabe. A descoberta de Euclides para encontrar números desse tipo, só fornece números perfeitos pares, daí surge outra pergunta: existe algum número perfeito ímpar? Até hoje não se encontrou qualquer deles. Esse talvez seja o mais antigo problema em aberto da teoria dos números e talvez de toda Matemática, resistindo fortemente a qualquer demonstração, há 24 séculos! Outra propriedade interessante dos números perfeitos é que todo ele é a soma de n números naturais consecutivos, para algum $n \in \mathbb{N}$; $6 = 1 + 2 + 3$, $28 = 1 + 2 + 3 + 4 + 5 + 6 + 7$, $496 = 1 + 2 + 3 + 4 + 5 + ... + 15$, etc.

IV) Dois números são ditos **amigos** quando um deles for igual à soma dos divisores do outro, excluindo os próprios números. Os pitagóricos já conheciam o menor desses pares de números, que é (220 e 284). Vamos conferir: a soma dos divisores de 220 é $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$, a soma dos divisores de 284 é $1 + 2 + 4 + 71 + 142 = 220$. O segundo exemplo de par de números amigos, só foi dado muitos séculos mais tarde, por Fermat, e o terceiro, por Descartes, ambos no século XVII. Coube a Euler descobrir outros 60 pares desses números. Quem vir os pares de números amigos encontrados por Euler pode constatar sua capacidade em trabalhar com números enormes, numa época em que uma calculadora manual era apenas um sonho. Apesar da sua argúcia e habilidade para lidar com produtos e somas de grandes números, é importante registrar que Euler deixou escapar, desapercebidamente, um par de números amigos relativamente pequenos: (1184, 1210). Ficou para Nicolò Paganini, um garoto de apenas 16 anos, a descoberta desse par, em 1866. Muitos acreditavam que, como os quadrados mágicos, os pares de números amigos tinham poderes sobrenaturais e os usavam em talismãs e poções mágicas. Com a computação, se conhece mais de dois milhões de pares de números amigos, e essa quantidade cresce a cada momento.

V) Os dados de Whodunni.

Grumpelina, a bela assistente do Grande Whodunni, colocou uma venda nos olhos do famoso ilusionista. Uma pessoa da plateia jogou então três dados.

− Multiplique o número do primeiro dado por 2 e adicione 5 − disse Whodunni. − Então multiplique o resultado por 5 e some o número do segundo dado. Finalmente, multiplique o resultado por 10 e some o número do terceiro dado.

Enquanto ele falava, Grumpelina anotava os cálculos num quadro-negro virado para a plateia, de modo que Whodunni não conseguisse vê-lo, mesmo que a venda fosse transparente.

− Quanto deu? − perguntou Whodunni.

− Setecentos e sessenta e três − disse Grumpelina.

Whodunni fez estranhos passes no ar.

− Então os dados foram ...

Quais? Como ele conseguiu?

Solução.

Os dados foram 5, 1 e 3.

Se os dados mostrarem as letras *a*, b e c, o cálculo irá gerar os números

$2a + 5$

$5.(2a + 5) + b = 10a + b + 25$

$10.(10a + b + 25) + c = 100a + 10b + c + 250$

Portanto Whodunni subtraiu 250 de 763, ficando com 513, os números dos três dados. Basta subtrairmos 2 do primeiro algarismo da resposta, 5 do segundo e não mexer no terceiro, fácil.

3.2 Fatorial

Denomina-se fatorial de um número natural n (indica-se por n!), ao produto de todos os números naturais de 1 até n, ou seja, $n! = n.(n – 1).(n – 2)....2.1$, para $n \geq 2$.

Vejamos duas consequências:

I) Podemos escrever para qualquer $n \in \mathbb{N}$ e $n > 2$:

n! = n.(n – 1)!

Veja que na igualdade 9! = 9.8.7.6.5.4.3.2.1, temos 9.(8.7.6.5.4.3.2.1) = 9.8!

II) Vamos estender o conceito de fatorial de n para n = 1 e n = 0. Em cada extensão deve-se conservar a propriedade n! = n.(n – 1)!

Observe que,

a) Se n = 2, temos n! = n.(n – 1)!

2! = 2.(2 – 1)!

2! = 2.1!

2.1 = 2.1! (dividindo os dois membros por 2)

1 = 1!

Portanto,

1! = 1

b) Se n = 1, temos n! = n.(n – 1)!

1! = 1.(1 – 1)!

1! = 1.0!

1 = 1.0!

Para que essa igualdade seja verdadeira, definimos: **0! = 1**

Observe que são os únicos números que têm o mesmo fatorial.

Exemplo 1. Calculando 6! temos, 6! = 6.5.4.3.2.1 = 720.

Exemplo 2. Simplificar: $\frac{100! - 99! - 98!}{100! + 99! + 98!}$.

Solução. Colocando-se 98! em evidência, teremos: $\frac{98!\,(100 \,.99 - 99 - 1)}{98!(100 \,.99 + 99 + 1)} = \frac{49}{50}$.

Exemplo 3. Determinar o maior número primo divisor de 87! + 88!.

Solução. 87! + 88! = 87! + 88.87! = 89.87!

Logo, o maior número primo é 89.

Exemplo 4. Resolva a equação (n – 5)! = 5040.

Ora, (n – 5)! = 5040 $\Longrightarrow$ (n – 5)! = 7.6.5.4.3.2.1 $\Longrightarrow$ (n – 5)! = 7! $\Longrightarrow$ n – 5 = 7 $\Longrightarrow$ n = 12.

3.3 Axiomas de Peano

A essência da caracterização de $\mathbb{N}$ reside na palavra "sucessor". Intuitivamente, quando x, y $\in \mathbb{N}$, dizer que y é o *sucessor* de x significa que y vem logo depois de x, isto é, não existem outros números naturais entre x e y. Fica claro que esta explicação apenas substitui "sucessor" por "logo depois", logo não é uma definição. O termo primitivo "sucessor" não é definido explicitamente. Contudo, no século XX, o matemático italiano Giuseppe Peano deu uma forma concisa e precisa para esses números, através da enumeração dos quatro axiomas abaixo que são conhecidos como Axiomas de Peano.

I) Todo número natural tem um único sucessor;

II) Números naturais diferentes têm sucessores diferentes;

III) Existe um único numero natural, chamado "um" e representado pelo símbolo 1, que não é sucessor de nenhum outro;

IV) Seja X um conjunto de números naturais (isto é, X $\subset \mathbb{N}$). Se 1 $\in$ X e se, além disso, o sucessor de todo elemento de X também pertence a X, então X = $\mathbb{N}$.

Tudo o que se sabe sobre os números naturais pode ser provado como consequência desses axiomas. O último dos axiomas de Peano é conhecido como o *axioma da indução*.

3.4 Ordem entre os números naturais

Sejam x, y ∈ ℕ, diz-se que x é menor do que y, e escreve-se x < y, para significar que existe algum b ∈ ℕ tal que y = x + b. A relação x < y tem as seguintes propriedades:

Transitividade: Se x < y e y < b então x < b.

Tricotomia: Dados x, y ∈ ℕ, vale uma, e somente uma, das alternativas: x = y, x < y ou y < x.

Monotonicidade: Se x < y então, para qualquer b ∈ ℕ, tem-se x + b < y + b e x.b < y.b.

A próxima propriedade é conhecida como a *Boa-ordenação* ou também como a técnica da *prova pelo contraexemplo mínimo*.

Princípio da Boa Ordenação

O conjunto ℕ dos inteiros positivos é bem ordenado, isto é, todo subconjunto não vazio de ℕ possui um menor elemento. Em outras palavras, para cada conjunto C, subconjunto de ℕ, se C ≠ ∅, então existe c ∈ C tal que c ≤ x, para todo x ∈ C. Este princípio é equivalente ao princípio da indução, assunto que veremos no próximo subcapítulo.

Exemplo 1. Seja P = {x ∈ ℕ; x é um número par}. Este conjunto é um subconjunto não vazio dos números naturais. Pelo Princípio da Boa Ordenação, P contém um elemento mínimo. Naturalmente, o elemento mínimo em P é 2.

Exemplo 2. Demonstrar que toda função f: $\mathbb{N} \to \mathbb{N}$ monótona não crescente (isto é, $n \leq m \Rightarrow f(n) \geq f(m)$) é constante a partir de um certo número natural.

Solução. Seja $A \subset \mathbb{N}$ a imagem de f. Pelo Princípio da Boa Ordenação, tal conjunto possui elemento mínimo x_0. Seja n_0 um natural tal que $f(n_0) = x_0$. Como a função é monótona não crescente então para todo $n \geq n_0$ temos que $f(n) \leq f(n_0)$, mas pela definição de x_0 temos $f(n) \geq x_0$. Logo $f(n) = x_0$ para todo $n \geq n_0$, como queríamos demonstrar.

3.5 Indução

Em vários problemas de Matemática, em especial da Teoria dos Números, precisamos verificar a veracidade de uma afirmação, A(n), que depende de um número natural n. Se a afirmação A(n) é de fato verdadeira, usamos o método de indução para facilitar a sua prova. Os historiadores da Matemática têm opiniões diferentes sobre quem primeiro formulou o Princípio da Indução Matemática. Mas, é certo que os matemáticos da antiga Grécia usaram argumentos indutivos, basta ver o Teorema IX-20 em *Os Elementos*, de Euclides, onde ele prova a existência de infinitos números primos. Alguns historiadores argumentam que a formulação precisa do método e do processo de indução deveu-se a Jacob Bernoulli (1654-1705) e Blaise Pascal (1623-1662). Em 1889, quando estudava os números naturais, Giuseppe Peano (1858-1932) introduziu o Princípio da Indução Matemática como um dos axiomas dos números naturais.

Indução é uma importante ferramenta utilizada em matemática, que tem por objetivo fazer generalizações, isto é, é um método usado para demonstrar uma propriedade que envolve números naturais, não para descobrir qualquer propriedade. Nem todos os resultados envolvendo números podem ou devem ser provados por indução, por exemplo, a soma de um número ímpar com um número par, ambos positivos, é um número ímpar. Veremos dois tipos de indução: a *indução empírica* e a *indução matemática*.

3.5.1 Indução empírica

Se, em uma sequência (x_1 , x_2 , x_3 , x_4 ,..., x_n), chegarmos a uma generalização baseada apenas na observação de certa regularidade de um número finito de termos, diremos que a mesma trata-se de uma indução empírica.

Exemplo. 2, 4, 6, 8,...

Observe que:

Se $x_1 = 1.2$, $x_2 = 2.2$, $x_3 = 3.2$, ... então, $x_n = n.x_1$ → indução empírica.

Em Matemática, é inaceitável generalizar uma sequência somente através da observação, haja vista que existem fórmulas que se verificam para um número limitado de termos.

Exemplo. A afirmação de que a expressão n^2 - n + 41 gera sempre um número primo, qualquer que seja n, é falsa. Ela se verifica para n = 1, 2, 3,..., 40, mas não é válida para n = 41.

3.5.2 Indução Matemática

É um processo que permite demonstrar uma indução supostamente empírica, através de poucos termos de uma sequência.

Axioma de indução: Seja C um subconjunto de ℕ tal que:

I) $1 \in C$.
II) C é fechado com respeito à operação de "somar 1" a seus elementos, ou seja,
$\forall n, n \in C \Rightarrow n + 1 \in C$.

Então, C = ℕ.

Teorema (Princípio de Indução Finita ou Matemática). Seja $a \in \mathbb{N}$ e P(n) uma sentença aberta de n. Suponha que:

I) P(a) é verdadeira;

II) P(n) é verdadeira para algum número natural $n \geq a$.
Então P(n +1) é verdadeira para algum número natural $n \geq a$.

Demonstração. Seja $W = \{n \in \mathbb{N}; P(n)\}$; ou seja, W é o subconjunto dos elementos de $\mathbb{N}$ para os quais P(n) é verdade.

Considere o conjunto $S = \{m \in \mathbb{N}; a + m \in W\}$,

Que verifica trivialmente $a + S \subset W$.

Como, pela condição I), temos que $P(a)$ é verdadeira e pela condição II) $P(a + 1)$ é verdadeira, logo $a + 1 \in W$, segue-se que $1 \in S$.

Por outro lado, se $m \in S$, então $a + m \in W$ e, por II), temos que $a + m + 1 \in W$; portanto, $m + 1 \in S$. Assim, pelo Axioma de Indução, temos que $S = \mathbb{N}$. Logo,

$\{m \in \mathbb{N}; m \geq a\} = a + \mathbb{N} \subset W$,

o que prova o resultado.

■

A demonstração por indução também pode ser pensada como a diversão de arrumar dominós em fila e derrubá-los como uma onda: derrubamos a primeira peça, que ao cair bate na segunda, que ao cair bate na terceira e assim sucessivamente, até que todas elas estejam tombadas. Agora, em vez de peças de dominós, pense numa sequência de afirmações A(1), A(2), A(3), ..., A(n), ... Imagine que seja possível provar as duas etapas seguintes:

I) a primeira afirmação, A(1), seja verdadeira;
II) sempre que uma afirmação for verdadeira, a posterior também será verdadeira.

Concluímos que todas as afirmações A(1), A(2), A(3), ..., A(n), ... são verdadeiras. Relacionando com as peças de dominó, I) seria a derrubada da primeira peça, II) seria a queda de uma peça de dominó provocada pela queda da peça anterior. A parte I) é chamada a **hipótese de indução** e II) é a **etapa indutiva**.

Exemplo 1. Este exemplo ilustra o primeiro registro da utilização do Princípio Indução Matemática feita por Francesco Maurolycus em 1575. Queremos provar a validez, para todo número natural n, da igualdade $P(n) = 1 + 3 + 5 + ... + (2n - 1) = n^2$

Solução. Usaremos Indução.

I) Verificação de P(1), P(1) é válida, pois $1 = 1^2 = 1$

II) Hipótese de indução:

Suponhamos P(n) verdadeira para certo valor de n.

III) O que se quer demonstrar:

Queremos mostrar que P(n + 1) vale. Ora, da hipótese $1 + 3 + ... + (2n - 1) = n^2$, somamos 2n + 1 a ambos os membros da igualdade, obtendo:

$$1 + 3 + 5 + ... + (2n - 1) + (2n + 1) = n^2 + 2n + 1, \text{ ou seja:}$$

$$1 + 3 + 5 + ... + [2(n + 1) - 1] = (n + 1)^2.$$

Mas esta última igualdade é P(n + 1). Portanto $P(n) \Rightarrow P(n + 1)$. Assim, P(n + 1) vale para todo $n \in \mathbb{N}$.

Exemplo 2. P(n) pode ser uma identidade:

$$1 + r + r^2 + ... + r^{n-1} + r^n = \frac{1 - r^{n+1}}{1 - r}, \text{ se } r \neq 1.$$

Solução.

I) Verificação de P(1):

P(1) é válida, pois

$$\frac{1-r^{1+1}}{1-r} = \frac{1-r^2}{1-r} = \frac{(1-r)(1+r)}{1-r} = 1 + r = 1 + r^1$$

II) Hipótese de indução:

Suponha P(k) válida para algum k > 1:

$$1 + r + r^2 + \ldots + r^{k-1} + r^k = \frac{1-r^{k+1}}{1-r}$$

III) O que se quer demonstrar:

Queremos mostrar que P(k + 1) vale, ou seja,

$$1 + r + r^2 + \ldots + r^k + r^{k+1} \stackrel{?}{=} \frac{1-r^{k+2}}{1-r}$$

A interrogação acima da igualdade indica que a identidade ainda não foi provada. A ideia é usar a expressão do lado esquerdo para deduzir a expressão do lado direito, usando a hipótese P(k):

$$1 + r + r^2 + \ldots + r^k + r^{k+1} = (1 + r + r^2 + \ldots + r^k) + r^{k+1} = \frac{1-r^{k+1}}{1-r} + r^{k+1} = \frac{1-r^{k+1}+r^{k+1}(1-r)}{1-r} = \frac{1-r^{k+1}+r^{k+1}-r^{k+2}}{1-r} = \frac{1-r^{k+2}}{1-r}.$$

Exemplo 3. P(n) pode ser uma desigualdade, como a Desigualdade de Bernoulli, bastante útil em um curso de Análise Real. Prove:

$$(1 + x)^n \geq 1 + nx, \text{ se } x \geq -1.$$

Solução.

I) Verificação de P(1):

P(1) é válida, visto que $(1 + x)^1 \geq 1 + x = 1 + 1 \,.\, x$.

II) Hipótese de indução:

Suponha que P(k) vale para algum k > 1, isto é,

$$(1 + x)^k \geq 1 + kx.$$

III) O que se quer provar:

Devemos provar que P(k + 1) é válida, ou seja,

$$(1 + x)^{k+1} \overset{?}{\geq} 1 + (k + 1)x.$$

Ora, por hipótese, $x \geq -1$, donde $(1 + x) \geq 0$. Portanto, desse fato e do fato de que P(k) vale, temos

$(1 + x).(1 + x)^k \geq (1 + x)(1 + kx) \Rightarrow (1 + x)^{k+1} \geq 1 + kx + x + kx^2 = 1 + (1 + k)x + kx^2 \geq 1 + (1 + k)x$, já que $kx^2 \geq 0$ para qualquer x.

Exemplo 4. Demonstrar que, para todo número natural n, $M_n = n(n^2 - 1)(3n + 2)$ é múltiplo de 24.

Solução. Veja que se n = 1 então $M_1 = 0$, que é um múltiplo de 24 (base da indução).

Agora, suponhamos que para certo inteiro k o número M_k é divisível por 24 (hipótese de indução) e vamos mostrar que M_{k+1} também é divisível por 24 (passo indutivo). Calculamos primeiramente a diferença

$M_{k+1} - M_k = (k + 1)((k + 1)^2 - 1)(3(k + 1) + 2) – k(k^2 - 1)(3k + 2) = k(k + 1)[(k + 2)(3k + 5) – (k – 1)(3k + 2)] = 12k(k + 1)^2$.

Um dos números naturais consecutivos k e k + 1 é par donde $k(k + 1)^2$ é sempre par e $12k(k + 1)^2$ é divisível por 24. Por hipótese de indução, M_k é divisível por 24 e temos, portanto que $M_{k+1} = M_k + 12k(k + 1)^2$ também é divisível por 24.

Exemplo 5. (Jakob Steiner – 1796-1863) Mostre, usando indução, que o número máximo de regiões definidas por n retas no plano é $L_n = \frac{n.(n+1)}{2} + 1$.

Solução. Para n = 1, o plano fica dividido em duas regiões. Assim $L_1 = \frac{1.(1+1)}{2} + 1 = 2$.

O que mostra que a afirmação é verdadeira para n = 1.

Traçando duas retas concorrentes, o plano fica dividido em 4 regiões. A expressão dada é verdadeira $L_2 = \frac{2.(2+1)}{2} + 1 = 4$.

Agora, observe que, traçando uma terceira reta, verificamos que esta divide no máximo três das quatro regiões já existentes, independentemente da posição das duas primeiras retas traçadas. Logo, com n = 3 retas, dividimos o plano em, no máximo, 7 regiões e a fórmula se verifica $L_3 = \frac{3.(3+1)}{2} + 1 = 7$.

Observe que, $L_2 = L_1 + 2$. $L_3 = L_2 + 3$.

Agora, para $n \geq 1$, a n-ésima reta aumenta o número de regiões do plano de k se, e só se, essa reta divide k das regiões já existentes. Por outro lado, a n-ésima reta intercepta k regiões já existente se ela intercepta as retas anteriores em k – 1 pontos. Mas, duas retas se interceptam em no máximo um ponto. Portanto, a n-ésima reta só pode interceptar as n - 1 retas anteriores em no máximo n – 1 pontos. Assim, como $k \leq n$, $L_n \leq L_{n-1} + n$.

Agora, desenhando a n-ésima reta de tal maneira que ela não seja paralela a nenhuma das outras n - 1 retas e não passe por nenhum dos pontos de interseção já existentes, temos que $L_n = L_{n-1} + n$. Essa igualdade foi verificada acima para n = 2 e n = 3. Observe que o passo da indução de n para n + 1 é dado por:

$$L_{n+1} = L_n + (n + 1) = \left[\frac{n.(n+1)}{2} + 1\right] + (n + 1) = \left[\frac{n.(n+1)}{2} + (n + 1)\right] + 1 =$$

$$(n + 1).\left(\frac{n}{2} + 1\right) + 1 = \frac{(n+1).[(n+1)+1]}{2} + 1.$$

Portanto, o número máximo de regiões definidas por n retas no plano é $L_n = \frac{n.(n+1)}{2} + 1$, para todo número natural n.

A Torre de Hanói

A Torre de Hanói é um quebra-cabeça que foi apresentado em 1883 por Édouard Lucas (1842-1891), um professor do Lycées Saint-Louis, na França, no seu livro *Récréations Mathématiques*, volume III, p. 56. Lucas anexou ao seu brinquedo

uma lenda romântica sobre uma torre, a Torre de Brama, que supostamente tem 64 discos de ouro empilhados em três agulhas de diamantes:

> No início dos tempos, ele disse, Deus colocou estes discos de ouro na primeira agulha e mandou um grupo de sacerdotes transferir para a terceira agulha, movendo apenas um disco de cada vez e sem colocar um disco maior em cima de um menor. Os sacerdotes, ao que se saiba, trabalham dia e noite nesta tarefa. Quando eles terminarem, a Torre ruirá e o mundo irá acabar.

A primeira solução do problema da Torre de Hanói apareceu na literatura matemática em 1884, num artigo de Allardice e Farser, La Tour d'Hanoi publicado em *Proc. Edinburgh Math. Soc*., v. 2, p. 50 – 53, 1884.

Agora, enunciamos o problema da Torre de Hanói de modo mais geral.

Exemplo 6. É dada uma torre com n discos, inicialmente empilhados por tamanhos decrescentes em um dos três pinos dados, conforme Figura 7. O objetivo é transferir a torre inteira para um dos outros pinos, movendo apenas um disco de cada vez e sem colocar um disco maior em cima de um menor.

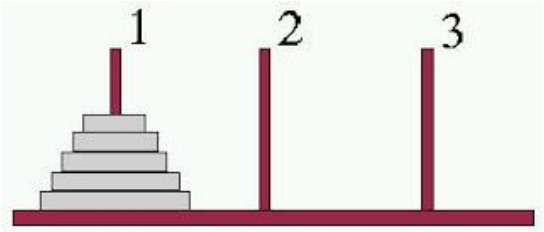

Figura 7. A Torre de Hanói

a) Determine a menor quantidade de movimentos necessários para transferir todos os discos de um dos pinos para outro.

b) Mais precisamente: prove que podemos realizar a transferência dos n discos, de acordo com as regras de Édouard Lucas, com, no mínimo, $2^n - 1$ movimentos.

Solução.

a) Na notação de indução associada à brincadeira do dominó, a afirmação, A(n), a ser provada é: "a menor quantidade de movimentos para transferir os n discos é igual a $2^n - 1$".

Assim, A(1) será entendida como a afirmação: "A quantidade mínima de movimentos para transferir um disco é igual a $2^1 - 1 = 1$";

A(2): a menor quantidade de movimentos para transferir dois discos é igual a 2^2 - 1;

A(3): a menor quantidade de movimentos para transferir três discos é igual a $2^3 - 1$, e assim sucessivamente.

Etapa 1: Verifiquemos a base da indução, isto é, vamos verificar que A(1) é verdadeira. Para isso, observe que, para transferir um só disco, basta um único movimento. Nesse caso, $1 = 2^1 - 1$ e a fórmula se verifica.

Etapa 2: Vamos supor que para n = k, onde k é o número de discos, a menor quantidade de movimentos para realizar a transferência seja $2^k - 1$, onde $k \geq 1$.

b) Agora, provaremos que, para n = k +1 discos, o número mínimo de movimentos que realizam a transferência é dado por $2^{k+1} - 1$.

De fato, se temos (k + 1) discos, podemos pensar em dois blocos de discos: um bloco com k discos, contendo todos os discos, com exceção do disco maior, que está embaixo da pilha, e outro, só com o disco maior. Pela hipótese de indução, podemos transferir os k primeiros discos com, no mínimo, $2^k - 1$ movimentos. Assim, transferimos o bloco contendo k discos para um dos pinos vazios, realizando $2^k - 1$ movimentos e, em seguida, transferimos o disco maior para o outro pino vazio e, por último, transferimos o bloco dos k discos para o pino em que se encontra o disco maior, com no mínimo $2^k - 1$ movimentos. Portanto, o total mínimo de movimentos realizados foi:

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

o que conclui a prova.

No caso de n = 64 discos, o número mínimo de movimentos será $2^{64} - 1$, necessários antes que o mundo se acabe...

Agora, observe que o número $2^{64} - 1$ é igual a 18.446.744.073.709.551.615. Se fizermos uma transferência por segundo, 24 horas por dia, durante 365 dias no ano, levaríamos 58.454.204.609 séculos e mais seis anos para terminar o trabalho!

Teorema do 2º Princípio da Indução (Princípio de Indução Forte ou Completa). Seja $a \in \mathbb{N}$ e P(n) uma sentença aberta de n. Suponha que:
I) P(a) é verdadeira;
II) P(k) é verdadeira para todo natural k tal que $a \leq k \leq n$.
Então P(k +1) é verdadeira.

Demonstração. Seja $F = \{n \in \mathbb{N}; n \geq a \text{ e } P(n) \text{ é falso}\}$. Queremos provar que F é vazio. Suponha, por absurdo, que $F \neq \emptyset$. Como F é limitado inferiormente (por a), pelo Princípio da Boa Ordenação, temos que F possui um menor elemento b. Como $b \in F$ temos que $b \geq a$, mas por I), temos que $a \notin F$, logo $b \neq a$ e, portanto, $b > a$. Sendo b o menor elemento de F, temos que $b - 1 \notin F$, logo P(b – 1) é verdadeira. De II) segue-se então que P(b) é verdadeira e, portanto, $b \notin F$, contradição.

■

Exemplo 1. A sequência de Fibonacci F_n é a sequência definida recursivamente por

$F_0 = 0$, $F_1 = 1$ e $F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$.

Assim, seus primeiros termos são

$F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, ...

Mostre que $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ onde $\alpha = \frac{1+\sqrt{5}}{2}$ e $\beta = \frac{1-\sqrt{5}}{2}$ são as raízes de $x^2 = x + 1$.

Solução.

Temos que $F_0 = \frac{\alpha^0 - \beta^0}{\alpha - \beta} = 0$ e $F_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta} = 1$ (base de indução).

Agora seja $n \geq 1$ e suponha que $F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ para todo k com $0 \leq k \leq n$ (hipótese de indução). Assim,

$$F_{n+1} = F_n + F_{n-1} = \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} = \frac{(\alpha^n + \alpha^{n-1}) - (\beta^n + \beta^{n-1})}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$

pois $\alpha^2 = \alpha + 1 \implies \alpha^{n+1} = \alpha^n + \alpha^{n-1}$ e analogamente $\beta^{n+1} = \beta^n + \beta^{n-1}$.

Veja que, neste exemplo, como o passo indutivo utiliza os valores de dois termos anteriores da sequência de Fibonacci, a base requer verificar a fórmula para os dois termos iniciais F_0 e F_1 e não apenas para o primeiro termo.

Exemplo 2. Seja P um polígono no plano. Triangular um polígono é traçar diagonais pelo interior do polígono de modo que as diagonais não se cruzem e cada região formada é um triângulo. Esses triângulos são chamados triângulos exteriores porque dois de seus três lados situam-se no exterior do polígono original. Prove que se um polígono com quatro ou mais lados for triangulado, então ao menos dois dos triângulos formados são exteriores.

Solução.

Seja n o número de lados do polígono.

Caso Comum: Como este resultado somente tem sentido para $n \geq 4$, o caso comum é n = 4. A única maneira de triangular um quadrilátero é traçar uma das duas diagonais possíveis. Em qualquer hipótese, os dois triângulos formados devem ser exteriores.

Hipótese da indução forte: Suponhamos que tenha sido provada para todos os polígonos com n = 4, 5,...,k lados.

Seja P um polígono arbitrário triangulado com k + 1 lados. Devemos provar que ao menos dois de seus triângulos são exteriores.

Seja d uma das diagonais. Esta diagonal separa P em dois polígonos A e B, em que A e B são polígonos triangulares com menor número de lados do que P. É possível que A, ou B, ou ambos sejam, eles próprios, triângulos. Consideramos os casos em que nenhum, apenas um, ou ambos, A e B, são triângulos.

I) Se A não é um triângulo. Então, como A tem ao menos quatro, mas, no máximo, k lados, sabemos, pela indução forte, que dois ou mais dos triângulos de A são exteriores. Agora temos motivo para preocupação: os triângulos exteriores de A são realmente triangulares exteriores de P? Não necessariamente. Se um dos triângulos exteriores de A utiliza d como diagonal, então não é um triângulo exterior de P. Não obstante, o outro triângulo exterior de A também não pode utilizar a diagonal d e, assim, ao menos um triângulo exterior de A é também triângulo de P.

II) Se B não é um triângulo. Tal como no caso anterior, B contribui com ao menos um triângulo exterior para P.

III) Se A é um triângulo. Então A é um triângulo exterior de P!

IV) Se B é um triângulo. Então B é um triângulo exterior de P!

Em qualquer caso, tanto A como B contribuem com ao menos um triângulo exterior para P, e assim P tem ao menos dois triângulos exteriores.

A prova por indução é um método alternativo da prova por boa ordenação, ou seja, qualquer resultado que provemos por indução pode ser provado igualmente com o método da boa ordenação, porém, as provas por indução são mais populares.

Curiosidades

I) O italiano Leonardo de Pisa, mais conhecido como Fibonacci, que significa filho de Bonacci, nasceu em 1180 na cidade de Pisa, na época do início da

construção da famosa Torre de Pisa, e introduziu na Europa o sistema de numeração hindu-arábico através do seu famoso livro Líber Abaci (1202). Fibonacci é considerado o maior matemático da Idade Média. Seu livro *Líber Abaci* contém um problema famoso sobre coelhos, cuja solução é agora conhecida como a Sequência de Fibonacci. Surpreendentemente, os números de Fibonacci, isto é, os números que comparecem na Sequência de Fibonacci, servem para representar modelos da natureza, como o número de espirais em determinadas rosas e frutas, como os girassóis, a pinha, o abacaxi, entre outros.

II) Outra curiosidade da sequência de Fibonacci, diz respeito ao *triângulo de Pascal* (Blaisé Pascal - 1623-1662) quando observado formando um triângulo retângulo. Observe na figura abaixo que surpreendentemente aparecem aí os números de Fibonacci como soma dos elementos das diagonais: 1, 1, 2, 3, 5, 8, 13, ...

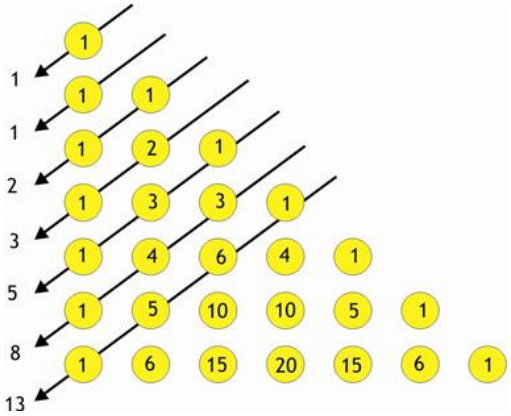

Figura 8. Triângulo de Pascal, formando um triângulo retângulo.

III) Considere a razão $r_n = \frac{f_{n+1}}{f_n}$, com n = 1, 2, 3, 4,..., entre os números de Fibonacci consecutivos. A sequência r_n, dada por: $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}$, ..., possui propriedades fascinantes:

(i) os termos de ordem par são decrescentes: $r_2 > r_4 > r_6 > r_8 > r_{10} > ....$
(ii) os termos de ordem ímpar são crescentes: $r_1 < r_3 < r_5 < r_7 < r_9 < ....$
(iii) os termos consecutivos aparecem em ordem alternada: $r_1 < r_2$, $r_2 > r_3$, $r_3 < r_4$, $r_4 > r_5$, ...

(iv) a sequência dos intervalos fechados: $[r_1, r_2]$, $[r_3, r_4]$, $[r_5, r_6]$, $[r_7, r_8]$, ..., é encaixante, isto é, cada um dos intervalos, a partir do segundo, está inteiramente contido no anterior: $[r_1, r_2] \supseteq [r_3, r_4] \supseteq [r_5, r_6] \supseteq [r_7, r_8] \supseteq$ .... Além disso, o limite do comprimento desses intervalos tende a zero quando n tende ao infinito.

3.6 Divisibilidade

Como a divisão de um número inteiro por outro nem sempre é exata, se expressa esta possibilidade através da relação de divisibilidade. Se não existir uma relação de divisibilidade entre dois números, veremos no próximo subcapítulo, que ainda assim, será possível efetuar uma "divisão com resto", chamada de divisão euclidiana. Euclides, que viveu por volta de 300 a.C., escreveu o mais célebre e importante tratado matemático de sua época, "Os *Elementos*". Composto por treze livros, dos quais três, foram dedicados à aritmética, essa coleção é composta de vários assuntos, entre eles, uma sistematização da teoria dos números naturais e um mecanismo que possibilita a divisão com resto, de *a* por *b*. Os números primos, assunto que trataremos mais adiante, constituem um dos objetos mais fundamentais da matemática. O aspecto de indivisibilidade que carrega consigo cada número primo, tem despertado o interesse e a admiração dos matemáticos ao longo dos séculos. A importância dos primos se deve à capacidade que eles têm de gerar todos os números inteiros. Tal importância tem motivado o estudo dos números primos desde a antiguidade grega até os nossos dias.

Definição: Dados dois números inteiros a e b, com $a \neq 0$, dizemos que a divide b, e escrevemos $a \mid b$, se existir um número inteiro k tal que $b = a.k$. Caso a não divida b, escrevemos $a \nmid b$. Se a dividir b, dizemos que a é um divisor ou um fator de b, ou que b é divisível por a, ou ainda que b é um múltiplo de a. Observe que todo inteiro não nulo é um divisor de si mesmo e de 0.

Exemplo 1. $5 \mid 0$; $3 \mid 9$; $3 \nmid 7$; $6 \nmid 17$.

Exemplo 2. Um inteiro n é **par** se for um múltiplo de 2; caso contrário, n é **ímpar**. De acordo com a definição, os inteiros pares são precisamente os que podem ser escritos na forma 2k, para algum k ϵ $\mathbb{Z}$, isto é, são os inteiros

..., - 6, - 4, - 2, 0, 2, 4,...

Os inteiros restantes, isto é,

..., - 5, - 3, - 1, 1, 3,... ,

são os ímpares. Assim, todo ímpar é igual a um par mais 1, de modo que podemos denotar um inteiro ímpar escrevendo 2k + 1, onde k ϵ $\mathbb{Z}$. Os inteiros são classificados assim, pelo menos, desde Pitágoras, 500 anos antes de Cristo.

Proposição 3.6.1. Seja $a \epsilon \mathbb{Z}$, mostre que $a \mid 0$, que $1 \mid a$ e que $a \mid a$.

Demonstração. Ora, $a \mid 0$ pois $0 = a.0$, $1 \mid a$ pois $a = 1.a$ e $a \mid a$ pois $a = a.1$

■

Proposição 3.6.2. Se $a \mid 1$, então $a = \pm 1$.

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

■

Proposição 3.6.3. Sejam a e b inteiros e diferentes de zero, se $a \mid b$ e $b \mid a$ então $a = \pm$ b.

Demonstração. Existe u, v ϵ $\mathbb{Z}$ tais que se $a \mid b$ então $b = a.u$ e se também $b \mid a$ então a = b.v. Logo, $a = (a u)v = a.(u.v)$ que implica u.v = 1, assim $u \mid 1$ e daí temos que $u = \pm 1$ e que $a = \pm b$.

■

Proposição 3.6.4. Sejam a e b inteiros com $a \neq 0$, se $a \mid b$ então b = 0 ou $|a| \leq |b|$.

Demonstração. Suponha que $a \mid b$, com $a \neq 0$ e $b \neq 0$. Assim, existe $u \in \mathbb{Z}$ com $u \neq 0$ tal que $b = a.u$, ou seja, $|b| = |a|.|u|$. Como $u \neq 0$, temos que $|u| \geq 1$, desse modo segue que $|b| \geq |a|$.

■

Proposição 3.6.5. Se a, b e c são inteiros com $a \neq 0$ e $b \neq 0$, tais que $a \mid b$ e $b \mid c$ então $a \mid c$.

Demonstração. Como $a \mid b$ e $b \mid c$ existem inteiros m e n tais que $b = am$ e $c = bn$. Substituindo o valor de b na equação $c = bn$ teremos $c = (am).n = a(mn)$, logo, $a \mid c$.

■

Exemplo. Como $3 \mid 12$ e $12 \mid 72$, então $3 \mid 72$. Como não existe inteiro c satisfazendo $25 = 6c$, então $6 \nmid 25$.

Proposição 3.6.6. Sejam a, b e c inteiros com $c \neq 0$. Se $c \mid b$, então $c \mid ab$.

Demonstração. Se $b = cm$, com $m \in \mathbb{Z}$, então $ab = c(am)$, com $am \in \mathbb{Z}$. Logo, $c \mid ab$.

■

Proposição 3.6.7. Se a, b, c e d são inteiros com $a \neq 0$ e $c \neq 0$, tais que $a \mid b$ e $c \mid d$ então $ac \mid bd$.

Demonstração. Existe $u, v \in \mathbb{Z}$ tais que se $a \mid b$ então $b = u.a$ e se $c \mid d$ então $d = vc$. Multiplicando-se as equações membro a membro temos que $bd = (uv).ac$, daí, $ac \mid bd$.

■

Exemplo. Em particular, sejam a, b e c inteiros com $b \neq 0$ e $c \neq 0$. Se $b \mid a$, então $bc \mid ac$. Ora, se $a = bm$, com $m \in \mathbb{Z}$, então $ac = (bc)m$ e, daí, $bc \mid ac$.

Proposição 3.6.8. Sejam a, b e c inteiros, com $a \neq 0$. Se $a \mid (b + c)$, então $a \mid b \Leftrightarrow a \mid c$.

Demonstração. Como a | (b + c), então existe k ∈ ℤ tal que (b + c) = ak. Vamos supor que a | b, então, existe w ∈ ℤ tal que b = aw. Logo, b + c = aw + c = ak, donde segue-se que c = ak − aw = a(k − w), que nos diz que a | c. Agora, se a | c, então, existe h ∈ ℤ tal que c = ah. Logo, b + c = b + ah = ak, donde segue-se que b = ak − ah = a(k − h), que nos diz que a | b. Portanto, a | b ⇔ a | c.

■

Proposição 3.6.9. Se a, b, c, m, n ∈ ℤ, com c | a e c | b, então c | (ma ± nb).

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

■

Exemplo 1. Observe que 5 | 15 e 5 | 60 e, consequentemente 5 | (6.15 − 1.60), ou seja, 5 | 30.

Exemplo 2. Encontre todos os inteiros positivos n tais que $2n^2 + 1 \mid n^3 + 9n - 17$.

Solução. Utilizando o "$2n^2 + 1$ divide" para reduzir o grau de $n^3 + 9n - 17$, temos que

$$\begin{cases} 2n^2 + 1 \mid n^3 + 9n - 17 \\ 2n^2 + 1 \mid 2n^2 + 1 \end{cases}$$

implica $2n^2 + 1 \mid (n^3 + 9n - 17).2 + (2n^2 + 1).(-n) \Leftrightarrow 2n^2 + 1 \mid 17n - 34$.

Como o grau de 17n – 34 é menor do que o de $2n^2 + 1$, podemos utilizar a proposição 2.6.4 para obter uma lista finita de candidatos a n. Temos 17n – 34 = 0 ⇔ n = 2 ou $|2n^2 + 1| \leq |17n - 34| \Leftrightarrow$ n = 1, 4 ou 5. Destes candidatos, apenas n = 2 e n = 5 são soluções.

Proposição 3.6.10. Sejam a, b, n ∈ ℕ, com a > b > 0. Então a − b divide $a^n - b^n$.

Demonstração. Vamos provar o resultado usando indução sobre n. É óbvio que para n = 0 a afirmação é verdadeira, pois a − b divide a^0 − b^0 = 0. Suponhamos, agora, que (a − b) | (a^n − b^n). Escrevamos a^{n+1} − b^{n+1}, obtemos:

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

Como, (a − b) | (a − b) e, por hipótese, (a − b) | (a^n − b^n), segue da Proposição 3.6.9 que (a − b) | (a^{n+1} − b^{n+1}) o que completa a demonstração.

■

Exemplo 1. Veja que, para todo n ∈ ℕ, 3 | 10^n - 7^n, pois 3 = 10 – 7 e pela proposição 3.6.10, 10 – 7 | 10^n - 7^n.

Exemplo 2. Observe que, para todo n ∈ ℕ, 8 | 3^{2n} - 1, pois 8 = 9 – 1 e 3^{2n} – 1 = 9^n - 1^n, e pela proposição 3.6.10 temos que 9 – 1 | 9^n - 1^n.

Proposição 3.6.11. Sejam a, b, n ϵ ℕ com a ≥ b > 0. Então a + b divide $a^{2n} - b^{2n}$.

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

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

Como, (a + b) | ($a^2 - b^2$) e, por hipótese, (a + b) | ($a^{2n} - b^{2n}$), segue das igualdades acima e da Proposição 3.6.9 que (a + b) | $a^{2(n+1)} + b^{2(n+1)}$ o que completa a demonstração.

■

Exemplo 1. Mostre que, para todo n ∈ ℕ, 53 | 7^{4n} - 2^{4n}.

Ora, 53 = 49 + 4 e 7^{4n} - 2^{4n} = $(7^2)^{2n}$ - $(2^2)^{2n}$ = 49^{2n} - 4^{2n}, contudo, pela proposição 3.6.11 temos que 49 + 4 | 49^{2n} - 4^{2n}, logo 53 | 7^{4n} - 2^{4n}.

Exemplo 2. Veja que, para todo n ∈ ℕ, 13 | 9^{2n} - 2^{4n}, pois 13 = 9 + 4 e 9^{2n} - 2^{4n} = 9^{2n} - $(2^2)^{2n}$ = 9^{2n} - 4^{2n}, e pela proposição 3.6.11 temos que 9 + 4 | 9^{2n} - 4^{2n}.

Proposição 3.6.12. Sejam a, b, n ϵ ℕ, com a + b ≠ 0. Então a + b divide a^{2n+1} + b^{2n+1}.

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

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

Como, (a + b) | (a^2 − b^2) e, por hipótese, (a + b) | (a^{2n+1} + b^{2n+1}), segue das igualdades acima e da Proposição 3.6.9 que (a + b) | ($a^{2(n+1)+1}$ + $b^{2(n+1)+1}$) o que estabelece o resultado para todo n ∈ ℕ.

■

Exemplo 1. Observe que, para todo n ∈ ℕ, 19 | 3^{2n+1} + 4^{4n+2}, pois 19 = 3 + 16 e 3^{2n+1} + 4^{4n+2} = 3^{2n+1} + $4^{2(2n+1)}$ = 3^{2n+1} + $(4^2)^{2n+1}$ = 3^{2n+1} + 16^{2n+1}, assim pela proposição 3.6.12 temos que 3 + 16 | 3^{2n+1} + 16^{2n+1}.

Exemplo 2. Veja que, para todo n ∈ ℕ, 14 | 5^{2n+1} + 3^{4n+2}, pois 14 = 5 + 9 e 5^{2n+1} + 3^{4n+2} = 5^{2n+1} + $3^{2(2n+1)}$ = 5^{2n+1} + $(3^2)^{2n+1}$ = 5^{2n+1} + 9^{2n+1}, contudo pela proposição 3.6.12 temos que 5 + 9 | 5^{2n+1} + 9^{2n+1}.

3.7 Divisão Euclidiana

Neste subcapítulo, estudaremos o Algoritmo da Divisão, proposto por Euclides, e seus usos nas questões de divisibilidade dos números inteiros. Observe que o

inteiro 11 não divide o inteiro 52 e que 11 não divide 14. Por outro lado, podemos escrever 52 = 4.11 + 8 e 14 = 1.11 + 3. É fácil criar vários exemplos de dois números inteiros onde um número não divide outro. Assim, concluímos que a divisão é bastante restritiva no conjunto dos números inteiros. Existe um processo de divisão de um número natural qualquer por outro, que amplia o conceito de divisibilidade e pelo qual se determina o **quociente** e o **resto da divisão**, sendo eles determinados unicamente. Esse processo é conhecido como **Algoritmo da Divisão** (apresentado por Euclides), e se estende de modo natural para o conjunto de todos os inteiros, com a restrição do divisor ser diferente de zero (ou divisor positivo, para facilitar).

Sabemos que 5 não divide 48, mas, no entanto, podemos escrever 48 = 9.5 + 3. Nesse caso, 9 é o **quociente** e 3 é o **resto da divisão** de 48 por 5. Outro exemplo, -26 = (-7).4 + 2, nesse caso, -7 é o **quociente** e 2 é o **resto da divisão** de -26 por 4. Agora, observe que, como 5 divide 35, podemos escrever 35 = 7.5 + 0; nesse caso, 7 é o **quociente** e 0 é o **resto da divisão** de 35 por 5. É nesse sentido que dizemos que o Algoritmo de Euclides amplia o conceito de divisibilidade. De uma maneira geral temos:

Teorema 3.7.1. Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que

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

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

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

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

de r ser o menor elemento de S. Portanto, b = aq + r com r < a, o que prova a existência de q e r.

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

■

Nas condições do teorema, os números q e r são chamados, respectivamente, de quociente e de resto da divisão de b por a. Veja que o resto da divisão de b por a é zero se, e só se, a divide b. Uma das mais importantes consequências do Algoritmo da Divisão é que qualquer natural b ou é divisível por a (sendo a natural maior do que 1) ou deixa resto 1 ou 2 ou 3 ou ... ou a – 1 na divisão por a.

Exemplo 1. Vamos achar o quociente e o resto da divisão de 24 por 5.

Solução. Considere as diferenças sucessivas:

$$24 - 5 = 19, \quad 19 - 5 = 14, \quad 14 - 5 = 9, \quad 9 - 5 = 4 < 5.$$

Isto nos dá q = 4 e r = 4.

Exemplo 2. Vamos mostrar aqui que o resto da divisão de 10^n por 9 é sempre 1, qualquer que seja o número natural n.

Solução. Faremos por indução sobre n. Para n = 1, temos que $10^1 = 9.1 + 1$; portanto, o resultado vale.

Suponha, agora, o resultado válido para um dado n, isto é $10^n = 9.q + 1$. Considere a igualdade

$$10^{n+1} = 10.\ 10^n = (9 + 1)\ 10^n = 9.\ 10^n + 10^n = 9.\ 10^n + 9.q + 1 = 9(10^n + q) + 1,$$

provando que o resultado vale para n + 1 e, consequentemente, vale para todo n ∈ ℕ.

Exemplo 3. Mostre que de três inteiros consecutivos um e apenas um deles é múltiplo de 3.

Solução. Suponha que os três inteiros consecutivos sejam a, $a + 1$ e $a + 2$. Temos as seguintes possibilidades: a deixa resto 0, 1 ou 2 quando dividido por 3.

I) Suponha que a deixe resto 0 quando dividido por 3, ou seja, $a = 3q$. Logo, $a + 1 = 3q + 1$ e $a + 2 = 3q + 2$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, a.

II) Suponha que a deixe resto 1 quando dividido por 3, ou seja, $a = 3q + 1$. Logo, $a + 1 = 3q + 2$ e $a + 2 = 3q + 3 = 3.(q + 1)$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 2$.

III) Suponha que a deixe resto 2 quando dividido por 3, ou seja, $a = 3q + 2$. Logo, $a + 1 = 3q + 3 = 3.(q + 1)$ e $a + 2 = 3.q + 4 = 3.(q + 1) + 1$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 1$.

Corolário 3.7.2. Dados dois números naturais a e b com $1 < a \leq b$, existe um número natural n tal que

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

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

■

Exemplo 1. Fixado um número natural $n \geq 2$, pode-se sempre escrever um número qualquer m, de modo único, na forma $m = n.k + r$, onde k, r ∈ ℕ e $r < n$.

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

Ou ainda, todo número natural n pode ser escrito em uma, e só uma, das seguintes formas: 4k, 4k + 1, 4k + 2, ou 4k + 3.

Exemplo 2. Dados a, n ∈ ℕ, com $a > 2$ e ímpar, vamos determinar a paridade de $\frac{(a^{n}-1)}{2}$.

Solução. Como a é ímpar, temos que $a^{n} - 1$ é par, e, portanto $\frac{(a^{n}-1)}{2}$ é um número natural. Logo, é legítimo querer determinar a sua paridade. Sabemos que

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

Sendo a ímpar, temos que $a^{n-1} + ... + a + 1$ é par ou ímpar, segundo n é par ou ímpar. Portanto, a nossa análise se reduz à procura da paridade de $\frac{a-1}{2}$.

Sendo a ímpar, ele é da forma 4k + 1 ou 4k + 3. Se a = 4k + 1, então $\frac{a-1}{2}$ é par, enquanto que, se a = 4k + 3, então $\frac{a-1}{2}$ é ímpar.

Contudo, temos que $\frac{(a^{n}-1)}{2}$ é par se, e só se, n é par ou a é da forma 4k + 1.

Teorema 3.7.3. (Algoritmo da divisão em ℤ). Se a e b são inteiros, com b ≠ 0, então existem únicos inteiros q e r tais que a = b.q + r e 0 ≤ r < $|b|$.

Demonstração. Primeiramente demonstraremos supondo b > 0. Pelo teorema 3.7.1 e tomando $a \geq 0$, existem números naturais q e r satisfazendo a = b.q + r e 0 ≤ r < b. Se a < 0 então $|a| > 0$. Aplicando o teorema 3.7.1, existem naturais q e r satisfazendo: $|a|$ = b.q + r e 0 ≤ r < b . Como $|a| = -a$, temos então $-a$ = bq + r, ou seja, a = b.(− q) + (− r). Se r = 0, temos a = b.(− q) + 0, sendo então − q e 0 o quociente e o resto da divisão de a por b, respectivamente.

Se r > 0 temos:

a = b.(− q) + (− r)

a = b.(− q) − b + b − r, logo

a = b.(− q − 1) + (b − r)

Como 0 < r < b, temos − b < - r < 0 e, então, somando b aos três membros desta última desigualdade, 0 < b − r < b. Fazendo q'= − q − 1e r = b − r', temos a = b.q' + r' com 0 < r' < b.

Para mostrar a unicidade do quociente q e do resto r, suponhamos que seja possível fazer:

a = b.q_1 + r_1 = b.q_2 + r_2 com q_1, q_2, r_1 e r_2 inteiros, 0 ≤ r_1 < b e 0 ≤ r_2 < b.

Mostraremos que necessariamente q_1 = q_2 e r_1 = r_2.

A partir da igualdade b.q_1 + r_1 = b.q_2 + r_2, obtemos 0 = b.(q_1 - q_2) + (r_1 - r_2) ou equivalentemente, (r_2 - r_1) = b.(q_1 - q_2).

Logo, b divide (r_2 - r_1). Por outro lado, como 0 ≤ r_1 < b e 0 ≤ r_2 < b, segue que − b < r_2 - r_1 < b e portanto |r_2 - r_1| < b. Como b divide |r_2 - r_1| < b (pois divide r_2 - r_1), temos necessariamente r_2 - r_1 = 0 e consequentemente q_1 - q_2 = 0. Segue, portanto, a unicidade q_1 = q_2 e r_1 = r_2.

Agora, para o caso b < 0 é análogo, temos que $|b|$ > 0, pelo caso anterior b > 0, existem inteiros q_1 e r_1 únicos tais que

a = $|b|$. q_1 + r_1 com 0 ≤ r_1 < $|b|$.

Como $|b|$ = - b, segue que

a = b.(- q_1) + r_1 com 0 ≤ r_1 < $|b|$.

ou seja, existem e são únicos os inteiros q = (- q_1) e r = r_1 tais que

a = b.q + r com 0 ≤ r < $|b|$.

■

Exemplo 1. Seja m um inteiro positivo. Então m é dito um **quadrado perfeito** se m = n^2, para algum inteiro n (podemos supor não negativo). Prove que todo quadrado perfeito:

a) deixa resto 0 ou 1 quando dividido por 3.
b) deixa resto 0 ou 1 quando dividido por 4.

Solução. Seja n um natural

a) Pelo algoritmo da divisão, o resto da divisão de n por 3 é 0, 1 ou 2, de modo que n = 3q, 3q + 1 ou 3q + 2, para algum q ∈ ℤ. Agora:

I) Se n = 3q, então $n^2 = 3.3q^2$.

II) Se n = 3q + 1, então $n^2 = 3.(3q^2 + 2q) + 1$.

III) Se n = 3q + 2, então $n^2 = 3.(3q^2 + 4q + 1) + 1$.

No primeiro caso, n^2deixa resto 0 quando dividido por 3; nos outros dois casos, n^2deixa resto 1 quando dividido por 3.

b) Novamente pelo algoritmo da divisão, o resto da divisão de n por 4 é 0, 1, 2 ou 3, de modo que n = 4q, 4q + 1, 4q + 2 ou 4q + 3, para algum q ∈ ℤ, e podemos dar uma prova análoga à do item a). Vejamos, contudo, uma prova mais simples; invocando o algoritmo da divisão, temos n = 2q ou 2q + 1 para algum q ∈ ℤ.

I) Se n = 2q, então $n^2 = 4q^2$.

II) Se n = 2q + 1, então $n^2 = 4.(q^2 + q) + 1$.

No primeiro caso, n^2 deixa resto 0 quando dividido por 4; no segundo, n^2 deixa resto 1 quando dividido por 4.

Exemplo 2. O quadrado de qualquer inteiro ou é da forma 4q ou 4q + 1, onde q é um inteiro.

Solução. Dado um inteiro b qualquer, temos que: ou b é par ou b é ímpar. Logo, ou b = 2k ou b = 2k + 1, onde k é um inteiro. Portanto, ou

$$b^2 = 4k^2 = 4q, \text{ onde } q = k^2,$$

ou

$$b^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 = 4q + 1, \text{ onde } q = k^2 + k \in \mathbb{Z}.$$

Portanto, o quadrado de qualquer inteiro é da forma 4q ou 4q + 1, onde q é um inteiro.

Exemplo 3. Nenhum número da lista abaixo é um quadrado perfeito, isto é, um quadrado de um número inteiro:

11, 111, 1111, 11111, 111111, 1111111, ...

Solução. Ora, Basta observar que todo número da lista é da forma 4q + 3, com $q \in \mathbb{Z}$, pois, $11\ldots11 = 11\ldots100 + 11 = 4r + (4.2 + 3) = 4q + 3$, com $r \in \mathbb{Z}$. Vejamos que:

11 = 4.2 + 3;
111 = 4.27 + 3;
1111 = 4.277 + 3
.....

Mas, de acordo com o exemplo 2, o quadrado de qualquer número inteiro é da forma 4q ou 4q + 1, onde q é um inteiro. Portanto, nenhum número da lista dada é um quadrado perfeito.

Corolário 3.7.4. Dados inteiros a_1, a_2 e b, sendo $b \neq 0$, temos que $b \mid (a_1 - a_2)$ se, e só se, a_1 e a_2 deixam restos iguais na divisão por b.

Demonstração. Suponha primeiro que $a_1 = b.q_1 + r$ e $a_2 = b.q_2 + r$, com $q_1, q_2, r \in \mathbb{Z}$.

Então a_1 - a_2 = b.(q_1 - q_2), i.e., b $\mid$ (a_1 - a_2). Reciprocamente, suponha que b $\mid$ (a_1 - a_2), e sejam a_1 = b.q_1 + r_1, a_2 = b.q_2 + r_2, com q_1, q_2, r_1, r_2 $\in \mathbb{Z}$ e $0 \leq r_1, r_2 < |b|$.

Portanto,

$$a_1 - a_2 = (q_1 - q_2).b + (r_1 - r_2).$$

E, como b $\mid$ (a_1 - a_2) e b $\mid$(q_1 - q_2).b, segue da proposição 3.6.9 que b divide r_1 - r_2 = (a_1 - a_2) - (q_1 - q_2).b. Por outro lado, $0 \leq r_1, r_2 < |b|$ implica $|r_1 - r_2| < |b|$, de modo que a única possibilidade é ser $|r_1 - r_2| = 0$ ou, ainda, $r_1 = r_2$.

■

Exemplo. O último algarismo de um quadrado perfeito só pode ser 0, 1, 4, 5, 6 ou 9.

Solução. Veja primeiro que o resto da divisão de um número natural por 10 coincide com seu último algarismo (o algarismo mais à direita, na representação decimal do número). De fato, seja m = 10m' + a_0, com m' $\in \mathbb{Z}_+$ e $0 \leq a_0 \leq 9$; como o inteiro 10m' termina por 0, segue que a representação decimal da soma 10m' + a_0 (que é igual a m) termina à direita com o algarismo a_0.

Sejam, agora, n $\in \mathbb{N}$ e q, r $\in \mathbb{Z}$ tais que n = 10q + r, com $0 \leq r \leq 9$. Então

$n^2 = (10q + r)^2 = 100q^2 + 20qr + r^2 = 10.(10k^2 + 2kr) + r^2$,

de sorte que 10 $\mid$ (n^2 - r^2) e o corolário 3.7.4 garante que n^2 e r^2 deixam restos iguais na divisão por 10. Portanto, segue de nossa observação inicial que o último algarismo de n^2 é igual ao último algarismo de r^2.

Para terminar, basta checar quais são os últimos algarismos dos números r^2 quando r varia de 0 a 9: $0^2 = 0$; 1^2 e 9^2 terminam em 1; 2^2 e 8^2 terminam em 4; 3^2 e 7^2 terminam em 9; 4^2 e 6^2 terminam em 6; 5^2 termina em 5. Assim, os possíveis últimos algarismos de n^2 são 0, 1, 4, 5, 6 ou 9.

3.8 Máximo divisor comum

O conceito de Máximo Divisor Comum é bastante usado nas mais variadas áreas do conhecimento. Com essa ferramenta somos capazes, por exemplo, de prever

alinhamentos de corpos celestes, estudar o ciclo de vida de alguns seres vivos, construir, de modo a garantir o mínimo de desperdício, mosaicos de azulejos que podem ser utilizados na arquitetura, dentre outros.

Dados dois números inteiros a e b com $a \neq 0$ ou b $\neq 0$, dizemos que um inteiro d é um divisor comum de a e b quando d $\mid a$ e d $\mid$ b. Note que a e b sempre têm divisores comuns: por exemplo, 1. Ademais, desde que qualquer inteiro não nulo tem apenas um número finito de divisores, a e b têm apenas um número finito de divisores comuns. Contudo, a definição a seguir tem sentido.

Definição. O máximo divisor comum dos inteiros não ambos nulos a e b, denotado mdc(a, b) (alguns autores usam a notação (a, b)), é o maior dentre os divisores comuns de a e b. Os inteiros a e b são primos entre si, ou relativamente primos, se mdc(a, b) = 1. Para a = b = 0 convencionamos mdc(0, 0) = 0. O mdc de a e b não depende da ordem em que a e b são tomados, temos que (a, b) = (b, a). Se d é máximo divisor comum entre a e b, então d também é máximo divisor comum entre a e - b, - a e b, e ainda, entre - a e - b. Esta definição de mdc para inteiros a e b também é válida para uma quantidade finita de inteiros a_1, a_2, a_3,..., a_n, como por exemplo, o mdc entre três números:

mdc(a_1, a_2, a_3) = mdc(mdc(a_1, a_2), a_3) = mdc(a_1, mdc(a_2, a_3)).

Vejamos a definição dada por Euclides nos elementos e se constitui em um dos pilares da sua aritmética.

Diremos que d é um máximo divisor comum de a e b se conter as seguintes propriedades:

I) d é um divisor comum de a e de b,

II) d é divisível por todo divisor comum de a e b.

A condição II) acima pode ser reenunciada como se segue:

II') Se c é um divisor comum de a e b, então c $\mid$ d.

Portanto, se d é um mdc de a e b e c é um divisor comum desses números, então c $\leq$ d. Em particular, isto nos mostra que, se d e d_1 são dois mdc de um mesmo par

de números, então $d \leq d_1$ e $d_1 \leq d$, e, consequentemente, $d = d_1$. Ou seja, o mdc de dois números, quando existe, é único.

Vejamos dois modos de determinar o mdc:

I) Com auxílio da decomposição em fatores primos. Regra:

a) Decompõem-se os números dados em fatores primos;

b) A potência, ou o produto, resultante das potências do(s) fator(es) primo(s) comum(ns) da(s) base(s) elevada(s) ao(s) menor(es) expoente(s), será o mdc procurado.

Exemplo. Determine o mdc dos números 48 e 40.

Solução. Vamos decompor os números em fatores primos:

$$48 = 2^4.3 \quad \text{e} \quad 40 = 2^3.5$$

Portanto, o mdc(48, 40) = 2^3 = 8.

II) Através da intersecção dos divisores comuns. Para isto, basta determinarmos, separadamente, os divisores dos números dados e, em seguida, os divisores comuns.

Exemplo 1. Determine o mdc dos números 60 e 36.

Solução.

D(60) = {1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60}

D(36) = {1, 2, 3, 4, 6, 12, 18, 36}

D(60) ∩ D(36) = {1, 2, 3, 4, 6, 12}

Logo, mdc(60, 36) = 12.

Exemplo 2. Sejam a = 12 e b = 18. Determine o mdc(12, 18).

Solução. Vamos determinar os divisores de 12, que são:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12;$$

e os divisores de 18, que são:

$$\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18.$$

Tomando o maior divisor comum, obtemos: mdc(12, 18) = 6.

No entanto, quando um dos dois números for grande, esse método fica impraticável, pois achar os divisores de um número grande é muito complicado. O que fazer então? Euclides, três séculos antes de Cristo, nos dá uma solução para este problema descrevendo um algoritmo muito eficiente para fazer este cálculo.

Lema 3.8.1 (Lema de Euclides). Sejam a, b, n $\in \mathbb{Z}$, então o mdc(a, b) = mdc(a, b - na).

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

■

Exemplo 1. Determine o mdc(3264, 1234).

Solução. mdc(3264, 1234) = mdc(1234, 3264 - 1234) = mdc(1234, 2030) = mdc(1 234, 2030 - 1234) = mdc(1234, 796) = mdc(796, 1234 - 796) = mdc(796, 438) = mdc(796 - 438, 438) = mdc(358, 438) = mdc(358, 438 - 358) = mdc(358, 80) = mdc(358 – 80, 80) = mdc(278, 80) = mdc(198, 80) = mdc(118, 80) = mdc(38, 80) = mdc(38, 42) = mdc(38, 4) = mdc(34, 4) = mdc(30, 4) = mdc(26, 4) = mdc(22, 4) = mdc(18, 4) = mdc(14, 4) = mdc(10, 4) = mdc(6, 4) = mdc(2, 4) = mdc(2, 2) = 2.

Exemplo 2. Dados a, m $\in \mathbb{N}$ com $a > 1$, temos que:

$$\left(\frac{a^m - 1}{a-1}, a - 1\right) = (a - 1, m).$$

Solução. Ora, seja d o primeiro membro da igualdade, temos que

d = (a^{m-1} + a^{m-2} + ... + a + 1, a - 1) = ((a^{m-1} - 1) + (a^{m-2} - 1) + ... + (a - 1) + m, a - 1).

Como, pela proposição 3.6.10, temos que:

$$a \text{ - } 1 \mid (a^{m-1} \text{ - } 1) + (a^{m-2} \text{ - } 1) + \ldots + (a \text{ - } 1),$$

segue-se que (a^{m-1} - 1) + (a^{m-2} - 1) + ... + (a - 1) = n.(a - 1) para algum n ∈ ℕ, e, portanto, pelo lema 3.8.1, tem-se que:

$$\text{d} = (\text{n}.(a \text{ - } 1) + \text{m}, a - 1) = (a - 1, \text{n}.(a \text{ - } 1) + \text{m}) = (a - 1, \text{m}).$$

Exemplo 3. Determine os valores de a e n para os quais a + 1 divide a^{2n} + 1.

Solução. Veja que: a + 1 ∣ a^{2n} + 1 ⇔ (a + 1, a^{2n} + 1) = a + 1.

Como a^{2n} + 1 = (a^{2n} – 1) + 2, e pela proposição 3.6.11, a + 1 ∣ a^{2n} – 1, segue-se, pelo lema 3.8.1, que para todo n,

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

Portanto, a + 1 ∣ a^{2n} + 1, para algum n ∈ ℕ, se, e só se, a + 1 = (a + 1, 2), o que ocorre se, e só se, a = 0 ou a = 1.

Teorema 3.8.2. (Bachet-Bézout). Seja d o máximo divisor comum de a e b. Então existem n_1 e m_1 inteiros tais que d = n_1.a + m_1.b.

Demonstração. Seja B o conjunto de todas as combinações lineares na + mb, com n e m inteiros. Obviamente, B contém números negativos, positivos e também o zero. Vamos escolher n_1 e m_1 tais que c = $n_1 . a$ + m_1.b seja o menor inteiro positivo pertencente ao conjunto B. Primeiramente, vamos provar que c | a e c | b. Suponhamos que c ł a, neste caso, pelo Teorema 3.7.1, existem q e r tais que a = qc + r com 0 < r < c. Portanto, r = a – qc = a – q.(n_1.a + m_1.b) = (1 – q. n_1).a + (− q. m_1).b. Isto mostra que r ∈ B, o que é uma contradição, uma vez que 0 < r < c e, por hipótese, c era o menor elemento positivo de B. Logo, c | a e de forma análoga se prova que c | b.

Como d é um divisor comum de a e b, existem inteiros w_1 e w_2 tais que a = w_1.d e b = w_2.d e, portanto, c = n_1.a + m_1.b = n_1.w_1.d + m_1.w_2.d = d.(n_1.w_1 + m_1.w_2) o que implica d | c. Por serem d e c ambos positivos, segue da proposição 3.6.4, que d ≤ c. Como d < c não é possível, uma vez que ele é o máximo divisor comum, concluímos que d = c, isto é, d = n_1.a + m_1.b. ■

Corolário 3.8.3. Sejam a, b, c ∈ ℤ. A equação ax + by = c admite solução inteira em x e y se, e só se, mdc(a, b) ⎪ c.

Demonstração. Se a equação admite solução inteira, então mdc(a, b) divide o lado esquerdo, logo deve dividir o direito também. Reciprocamente, se mdc(a, b) ⎪ c, digamos c = k.mdc(a, b) com k ∈ ℤ, pelo teorema 3.8.2 existem inteiros x_0 e y_0 tais que a.x_0 + b.y_0 = mdc(a, b) e multiplicando tudo por k obtemos que x = k.x_0 e y = k.y_0 são soluções da equação dada.

■

Corolário 3.8.4. Sejam a e b inteiros não nulos e d seu mdc. Se d' ∈ ℕ, então d' ⎪ a, b se, e só se, d' ⎪ d.

Demonstração. Tome inteiros x e y tais que d = a.x + b.y. Uma vez que d' ⎪ a, b, a proposição 3.6.9 nos garante que d' ⎪ d. A recíproca é imediata.

■

Corolário 3.8.5. Sejam a e b inteiros não nulos e d seu mdc. Então d = 1 se, e só se, existirem inteiros x e y tais que a.x + b.y = 1.

Demonstração. Se d = 1, a existência de inteiros x e y como pede o enunciado segue do teorema 3.8.2. Reciprocamente, sejam x e y inteiros como no enunciado. Como d $\mid$ a, b, segue novamente da proposição 3.6.9 que d $\mid$ a.x + b.y, isto é, d $\mid$ 1. Logo, d = 1.

■

Exemplo. Sejam a, b, c, d inteiros não nulos, tais que c + d ≠ 0 e a.d – b.c = 1. Prove que a fração $\frac{a+b}{c+d}$ é irredutível.

Solução. Queremos provar que mdc(a + b, c + d) = 1. Para tanto, procuremos, de acordo com o corolário 3.8.5, inteiros x, y tais que (a + b).x + (c + d).y = 1. Ora, uma vez que ad – bc = 1, basta tomarmos x = d e y = - b.

Proposição 3.8.6. Para todo inteiro positivo t e a, b ∈ ℤ, tem-se que (ta, tb) = t(a, b).

Demonstração. Pelo Teorema 3.8.2, existem k, w ∈ ℤ tais que (a, b) = ak + bw. Então t(a, b) = tak + tbw. Assim, (ta, tb) $\mid$ ta, tb. Por outro lado, (a, b) $\mid$ a, b ⇒ t(a, b) $\mid$ta, tb ⇒ t(a, b) $\mid$(ta, tb). Portanto, (ta, tb) = t(a, b).

■

Proposição 3.8.7. Se c > 0 e a e b são divisíveis por c, então

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

Demonstração. Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são números inteiros. Substituindo a por $\frac{a}{c}$ e b por $\frac{b}{c}$ e tomando t = c na Proposição 3.8.6 chegamos ao resultado desejado.

■

Corolário 3.8.8. Se (a, b) = d, então

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

Demonstração. Da proposição 3.8.7, c é um divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, isto é, c = d, teremos o resultado desejado. ■

Exemplo. Como (21, 35) = 7 temos que $\left(\frac{21}{7}, \frac{35}{7}\right)$ = (3, 5) = 1.

Proposição 3.8.9. Sejam a, b e c inteiros não nulos, temos que:

a) Se a | bc e mdc(a, b) = 1, então a | c.

b) Se c ∣ b e mdc(a, b) = 1, então mdc(a, c) = 1

Demonstração.

a) Como mdc(a, b) = 1 pelo Teorema 3.8.2, existem inteiros w e k tais que wa + kb = 1. Multiplicando os dois membros dessa última equação por c temos que w.(ac) + k.(bc) = c. Como a | ac e, por hipótese, a | bc, então, pela Proposição 3.6.9, a | c.

b) Sejam d ∈ ℤ tal que b = cd e u, v ∈ ℤ tais que au + bv = 1. Então, au + c.(dv) = 1 e segue, do corolário 3.8.5, que mdc(a, c) = 1.

■

Exemplo. 4 ∣ (29.16), logo 4 ∣ 16 uma vez que (4, 29) = 1; agora, 5 ∣ 20 e mdc(7, 20) = 1, então mdc(7, 5) = 1.

Proposição 3.8.10. Para a, b e c inteiros não nulos, temos que se a + bc ≠ 0, então mdc(a + bc, b) = mdc(a, b).

Demonstração. Sejam d = mdc(a + bc, b) e d' = mdc(a, b). Como d' ∣ a, b, temos que d' ∣ a, a + bc. Portanto, pelo corolário 3.8.4 temos que d' ∣ d. Reciprocamente, como d ∣ (a + bc) e d ∣ b, temos que d ∣ [(a + bc) – bc], isto é, d ∣ a e d ∣ b. Novamente pelo corolário 3.8.4, temos que d ∣ d' e, portanto, d = d'.

■

Lema 3.8.11. Sejam a e b dois inteiros positivos e a = bq + r, com $0 \leq r < b$. Então mdc(a, b) = mdc(b, r).

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

■

Agora podemos enunciar o algoritmo de Euclides.

Teorema 3.8.12. (Algoritmo de Euclides). Sejam a e b inteiros positivos, com $a \geq b$. Usando sucessivamente o algoritmo da divisão, segue do lema 3.8.11 que o problema de achar o mdc(a, b) reduz-se a achar o mdc(r_{n-1}, r_n), com $n \in \mathbb{N}$.

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

$a = b.\ q_1 + r_1$, com $0 \leq r_1 < b$

$b = r_1.\ q_2 + r_2$, com $0 \leq r_2 < r_1$

$r_1 = r_2.\ q_3 + r_3$, com $0 \leq r_3 < r_2$

.....

.....

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

$r_{n-1} = r_n.\ q_{n+1} + r_{n+1}$, com $r_{n+1} = 0$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões deve ser exata. Suponhamos então que r_{n+1} seja o primeiro resto nulo, como está indicado antes. Do lema 3.8.11, temos que:

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

Finalmente, como $r_n \mid r_{n-1}$ é fácil ver que $\text{mdc}(r_n, r_{n-1}) = r_n$, logo, $\text{mdc}(a, b) = r_n$.

■

Exemplo 1. Calcule o mdc(1126, 522).

Solução. Realizando as divisões sucessivas, temos:

1126 = 2.522 + 82
522 = 6.82 + 30
82 = 2.30 + 22
30 = 1.22 + 8
22 = 2.8 + 6
8 = 1.6 + 2
6 = 3.2 + 0

Assim, temos mdc(1126, 522) = mdc(522, 82) = mdc(82, 30) = mdc(30, 22) = mdc(22, 8) = mdc(8, 6) = mdc(6, 2) = mdc(2, 0) = 2.

Exemplo 2. Sejam m ≠ n dois números naturais. Mostre que

$$\text{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & se\ a\ \text{é}\ par, \\ 2 & se\ a\ \text{é}\ ímpar. \end{cases}$$

Solução. Suponha sem perda de generalidade que m > n e observe a fatoração

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-1}} - 1) = \ldots = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1) \ldots (a^{2^n} + 1)(a^{2^n} - 1).$$

Logo, $a^{2^m} + 1 = (a^{2^n} + 1).q + 2$ com $q \in \mathbb{Z}$ e assim

$$\text{mdc}(a^{2^m} + 1, a^{2^n} + 1) = \text{mdc}(a^{2^n} + 1, 2)$$

que é igual a 2 se $a^{2^n} + 1$ for par, isto é, se a for ímpar, e é igual a 1 caso contrário.

Exemplo 3. Se a, m e n são naturais tais que $a > 1$ e $m = nq + r$, com $0 \leq r < n$, prove que

$$\text{mdc}(a^m - 1, a^n - 1) = a^{mdc(m,n)} - 1.$$

Solução. Mostremos inicialmente que, se r = 0, então $(a^n - 1) \mid (a^m - 1)$. Para tanto, basta observar que $a^m - 1 = (a^n)^q - 1$ e lembrar, pela proposição 3.6.10, que $a^n - 1$ divide $(a^n)^q - 1$.

Provemos agora que, se r > 0, então $\text{mdc}(a^n - 1, a^m - 1) = \text{mdc}(a^n - 1, a^r - 1)$.

De fato, fazendo $a^n = b$ quando conveniente, temos:

$a^m - 1 = a^{n.q+r} - 1 = (a^{n.q} - 1).a^r + (a^r - 1) = ((a^n)^q - 1).a^r + (a^r - 1) =$
$(a^n - 1).(b^{q-1} + \ldots + b + 1).\ a^r + (a^r - 1).$

Sendo

$$\begin{cases} c = (b^{q-1} + b^{q-2} + \cdots + b + 1)a^r \\ d = mdc(a^m - 1, a^n - 1) \\ d' = mdc(a^n - 1, a^r - 1) \end{cases},$$

temos

$$a^m - 1 = (a^n - 1).c + (a^r - 1).$$

Portanto, segue da proposição 3.8.10 que $\text{mdc}(a^m - 1, a^n - 1) = \text{mdc}((a^n - 1).c + (a^r - 1), a^n - 1) = \text{mdc}(a^r - 1, a^n - 1)$.

Para o que falta suponhamos, sem perda de generalidade, que m ≥ n. Se m = n, nada há a fazer. Suponhamos, pois, m > n e consideremos o algoritmo de Euclides para m e n:

$m = n.\ q_1 + r_1$, com $0 < r_1 < n$;

$n = r_1.\ q_2 + r_2$, com $0 < r_2 < r_1$;

$r_1 = r_2.\ q_3 + r_3$, com $0 < r_3 < r_2$;

.....

$r_{j-2} = r_{j-1}.\ q_j + r_j$, com $0 < r_j < r_{j-1}$;

$r_{j-1} = r_j.\ q_{j+1} + 0$.

Nossa discussão anterior garante que:

$mdc(m, n) = mdc(n, r_1) = mdc(r_1, r_2) = ... = mdc(r_{j-1}, r_j) = r_j$.

Portanto, aplicando a discussão acima sucessivas vezes, concluímos que:

$mdc(a^n - 1, a^m - 1) = mdc(a^n - 1, a^{r_1} - 1) = mdc(a^{r_1} - 1, a^{r_2} - 1) = ... =$

$mdc(a^{r_{j-1}} - 1, a^{r_j} - 1) = a^{r_j} - 1 = a^{mdc(m,n)-1}$.

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

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

	q_1	
b	a	
r_1		

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

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Seguindo o procedimento, enquanto for possível, teremos:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n	0	

Exemplo 1. Calculemos o mdc de 372 e 162, temos:

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6	0	

Veja que, o algoritmo de Euclides nos fornece:

6 = 18 – 1.12

12 = 48 – 2.18

18 = 162 – 3.48

48 = 372 – 2.162

Donde se segue que

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.

Temos, então, que mdc(372, 162) = 6.

Exemplo 2. Determinar o maior número natural pelo qual se deve dividir 574 e 754, a fim de que os restos sejam 15 e 23, respectivamente.

Solução. Seja d o número desejado. De acordo com os dados, teremos:

I) 574 = d.q_1 + 15 $\Leftrightarrow$ d. q_1 = 574 – 15 $\Leftrightarrow$ $q_1 = \frac{559}{d}$

II) 754 = d. q_2 + 23 $\Leftrightarrow$ d. q_2 = 754 – 23 $\Leftrightarrow$ $q_2 = \frac{731}{d}$

Como d é divisor simultâneo de 559 e 731, e queremos determinar o maior, basta calcularmos o mdc dos números 559 e 731, ou seja:

	1	3	4
731	559	172	43
172	43	0	

Portanto, o mdc(731, 559) = 43, isto é, o número procurado é o 43.

Exemplo 3. Calcular a diferença (positiva) de dois números naturais, que têm para produto 2304 e para mdc o número 12.

Solução. Supondo x e y dois números, teremos, de acordo com os dados:

$$\begin{cases} x.y = 2304 \\ \text{mdc}(x, y) = 12 \end{cases}$$

I) $\frac{x}{12}$ = q' $\Leftrightarrow$ x = 12.q'

II) $\frac{y}{12}$ = q'' $\Leftrightarrow$ y = 12.q''

Multiplicando-se I) por II), teremos:

$$(12.q').(12.q'') = x.y \Leftrightarrow (12.q').(12.q'') = 2304 \Leftrightarrow q'.q'' = \frac{2304}{144} \Leftrightarrow q'.q'' = 16.$$

Como q’ e q’’ são números primos entre si, teremos que determinar o(s) par(es) de números que satisfazem tal condição, daí, se q’.q’’ = 16, então, q’ = 1 e q’’ = 16. Substituindo q’ e q’’ em I) e II), teremos:

$$x = 12.1 \Leftrightarrow x = 12.$$
$$y = 12.16 \Leftrightarrow y = 192.$$

Logo, a diferença positiva será 192 – 12 = 180.

3.9 Números Primos

> *“O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e dos mais úteis em Aritmética. A própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e tão famoso.”*
>
> (Gauss)

Os números primos constituem um dos objetos mais fundamentais da Matemática. O aspecto de indivisibilidade que carrega consigo cada número primo, tem despertado o interesse e a admiração dos matemáticos ao longo dos séculos. A importância dos primos se deve à capacidade que eles têm de gerar todos os números inteiros, veremos adiante quando abordarmos o Teorema Fundamental da Aritmética.

Tal importância tem motivado o estudo dos números primos desde a antiguidade grega até os nossos dias.

Desde a Grécia antiga, os químicos se esforçaram para identificar os elementos básicos da natureza. Tal esforço culminou com a elaboração da tabela periódica de Dimitri Mendeleev (1834 -1907), professor da Universidade de São Petersburgo, na Rússia. Cada uma das moléculas do mundo físico pode ser decomposta por átomos da tabela periódica de elementos químicos. Para os matemáticos, os números primos são os elementos de nossa tabela periódica. Mas, apesar do sucesso que os gregos antigos tiveram na identificação de blocos de números que permitem um amplo domínio da aritmética, os matemáticos têm dificuldade de entender a tabela dos números primos. O matemático que primeiro construiu uma tabela de primos foi Eratóstenes, que foi diretor da biblioteca de Alexandria no século III a.C.. A lista de matemáticos que se esforçaram para entender a tabela dos números primos é imensa, contando com nomes como Euclides, Fibonacci, Gauss, Euler, Goldbach, Riemann, Fourier, Jacobi, Legendre, Cauchy, Hilbert, Hardy, Littlewood, Ramanujan, Minkowski, Landau, entre outros. Até os dias de hoje ainda se procura entender a tabela dos primos.

Eratóstenes, astrônomo e matemático grego que foi diretor da biblioteca de Alexandria na época de Ptolomeu III, inventou uma técnica para achar todos os primos menores do que ou iguais a um dado número n, que ficou conhecida como **Crivo de Eratóstenes**. A técnica consistia em listar todos os números de 2 até n; em seguida, riscar todos os múltiplos de 2, maiores do que 2; logo após, riscar todos os múltiplos de 3, maiores do que 3; depois, riscar todos os múltiplos de 5, maiores do que 5, e assim por diante. Eratóstenes sabia que um dos fatores primos de um número composto era menor do que ou igual à raiz quadrada do número. Assim, ele continuaria o processo até que o maior número primo menor do que ou igual a $\sqrt{n}$ fosse atingido. Nessa altura, todos os números compostos de 2 até n já teriam sido riscados, restando somente os números primos de 2 até n. Eratóstenes também foi atleta, poeta, filósofo e historiador. Como atleta, fez sucesso nos III Jogos Olímpicos, da Grécia antiga.

Um inteiro $p > 1$ é **primo** se seus únicos divisores positivos forem 1 e p. Dados p e q dois números primos e um $a \in \mathbb{N}$, decorrem da definição os seguintes fatos:

I) Se $p \mid q$, 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 ł a, então (p, a) = 1.

De fato, se (p, a) = d, temos que d | p e d | a. Portanto, d = p ou d = 1. Mas, d ≠ p, pois p ł a e, consequentemente, d = 1.

Um inteiro n > 1 que não é primo é dito **composto**. Logo, se n é composto, existirá um divisor b de n tal que b ≠ 1 e b ≠ n. Portanto, existirá um número natural c tal que n = b.c, com 1 < b < n e 1 < c < n.

Por exemplo, 2, 3, 5 e 7 são números primos, enquanto que 4, 6 e 8 são números compostos. Note que a definição não classifica os números 0 e 1 nem como primos nem como compostos. Exceto esses dois números, todo número natural ou é primo ou é composto.

Nosso objetivo é estudar os números primos e sua relação com os números compostos. Uma pergunta que surge espontaneamente é a seguinte: Quantos são os números primos? Euclides de Alexandria, em 300 a.C., ou seja, há mais de 2 300 anos, mostrou que existem infinitos números primos. Como terá Euclides feito isto? Será que ele exibiu todos os números primos? Seria isto possível? Veremos mais adiante como Euclides realizou tal façanha.

Determinar se um dado número é primo ou composto pode ser uma tarefa muito árdua. Para se ter uma ideia da dificuldade, você saberia dizer se o número 241 é primo? Muito mais difícil é decidir se o número 4 294 967 297 é primo ou composto. O matemático francês Pierre de Fermat (1601-1655) afirmou que esse número é primo, enquanto que o matemático suíço Leonhard Euler (1707-1783) afirmou que é composto. Qual deles estava com a razão? Veremos como solucionar a todas estas perguntas e também a outras.

Dois ou mais números são ditos primos entre si, quando o seu único divisor comum for à unidade. Por exemplo, 4 e 9 são primos entre si, pois D(4) = {1, 2, 4} e D(9) = {1, 3, 9}, donde o único divisor comum é o 1.

Agora, vejamos algumas propriedades, das quais não demonstraremos:

I) Dois números naturais sucessivos são sempre primos entre si.

II) As potências de dois ou mais números primos entre si também são números primos entre si.

III) Se dentre vários números naturais, dois quaisquer deles forem primos entre si, então todos eles serão também números primos entre si.

IV) Se dois números x e y forem primos entre si, a soma e o produto deles serão sempre números primos entre si.

V) Se x e y são dois números naturais quaisquer não nulos, os números y e x.y + 1 são sempre primos entre si.

VI) Os números x, x + 1 e 2x + 1 são sempre primos entre si, dois a dois.

VII) Um número ímpar qualquer diferente de 1 e a metade de seu sucessivo são sempre primos entre si.

VIII) Dois números x e y, cuja soma seja um número primo p, são primos entre si.

IX) Dois números ímpares consecutivos x e y são sempre primos entre si.

Proposição 3.9.1. Se p | a.b, p primo, então p | a ou p | b.

Demonstração. Se p ∤ a, então mdc(p, a) = 1 o que implica, pelo item a) da proposição 3.8.9, p | b.

■

Lema 3.9.2. (Euclides). Todo inteiro positivo maior que 1 pode ser expresso como o produto de um número finito de primos, não necessariamente distintos.

Demonstração. Iremos fazer a prova por indução sobre n. Se n = 2, nada há a fazer. Suponha, agora, que todo inteiro n tal que 2 ≤ n < m pode ser escrito como o produto de um número finito de primos; provemos que este é também o caso para m: se m for primo, nada há a fazer. Senão, existem inteiros a e b tais que m = a.b, com 1 < a, b <

m. Pela hipótese de indução, a e b podem ser escritos como produtos de números finitos de primos, digamos $a = p_1 \dots p_k$, $b = q_1 \dots q_j$, com $k, j \geq 1$ e $p_1 \dots p_k, q_1 \dots q_j$ primos. Logo, $m = a.b = p_1 \dots p_k.q_1 \dots q_j$, é também o produto de um número finito de primos.

■

Corolário 3.9.3. (Eratóstenes). Se um inteiro $n > 1$ for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.

Demonstração. Seja $n = a.b$, com $1 < a \leq b$. Sendo p um divisor primo de a, segue que $p \mid n$ e

$$p^2 \leq a^2 \leq a.b = n,$$

de modo que $p \leq \sqrt{n}$.

■

Exemplo 1. Prove que 641 é primo.

Solução. Inicialmente, note que $25 < \sqrt{641} < 26$. Portanto, se 641 for composto, segue do corolário 3.9.3 que 641 deve possuir um divisor primo $p \leq 25$, de modo que

$$P \in \{2, 3, 5, 7, 11, 13, 17, 19, 23\}.$$

No entanto, é imediato verificar que, dentre as divisões de 641 pelos primos acima, nenhuma é exata. Logo, 641 é primo.

Decompor um número em fatores primos significa obter uma multiplicação onde todos os fatores sejam necessariamente primos e o produto deles seja igual ao número dado.

Exemplo 2. Analise, justificando, se o número 377 é primo.

Solução. Como $\sqrt{377} = 19{,}416...$, pelo corolário 2.9.3, basta procurar um divisor para 377 dentre os inteiros primos de 1 até 19. É fácil ver que 13 divide 377 e, portanto, 377 não é primo.

O Teorema Fundamental da Aritmética coloca em evidência o papel dos números primos na estrutura dos inteiros. Ele nos assegura que um número pode ser

expresso como um produto de números primos de modo único, a menos da ordem desses fatores primos.

Teorema 3.9.4. (Teorema Fundamental da Aritmética). Seja n ≥ 2 um número natural. Podemos escrever n de uma única forma como um produto

$$n = p_1 \dots p_k$$

onde k ≥ 1 é um natural e $p_1 \leq \dots \leq p_k$ são primos.

Demonstração. Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar, escrevemos k = 1, p_1 = n. Se n é composto podemos escrever n = a.b, a, b ∈ ℕ, 1 < a < n, 1 < b < n. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b, reordenado os fatores, obtemos uma fatoração de n. Agora, para mostrar a unicidade, suponha por absurdo que n possui duas fatorações diferentes, temos

$$n = p_1 \dots p_k = q_1 \dots q_j,$$

com $p_1 \leq \dots \leq p_k$, $q_1 \leq \dots \leq q_j$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_i$ para algum valor de i pela proposição 3.9.1 (no caso geral). Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$\frac{n}{p_1} = p_2 \dots p_k = q_2 \dots q_j,$$

admite uma única fatoração, pela minimalidade de n, donde k = j e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações.

■

Outra maneira de escrever a fatoração é $n = {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k}$, com $p_1 < \dots < p_k$ e $\alpha_i > 0$. Também temos a formulação $n = 2^{\alpha_2}.3^{\alpha_3}.5^{\alpha_5} \dots p^{\alpha_p} \dots$. estas expressões são ditas fatoração canônica de n em primos.

Exemplo 1. Decomponha em fatores primos o número inteiro 120.

Solução. O número dado se escreve (ou se decompõe) como produto de primos da seguinte maneira: 120 = 2.2.2.3.5. Na prática, escrevemos: $120 = 2^3.3.5$, onde 2 < 3 < 5.

Exemplo 2. Decomponha em fatores primos o número inteiro 4.667.544.

Solução. O número dado se escreve (ou se decompõe) como produto de primos da seguinte maneira: 4.667.544 = 2.2.2.3.3.3.3.3.7.7.7.7. Na prática, escrevemos: $4.667.544 = 2^3 . 3^4 . 7^4$, onde $2 < 3 < 7$.

Exemplo 3. Determine todas as ternas (a, b, c) de inteiros positivos tais que $a^2 = 2^b + c^4$.

Solução. Como $a^2 = 2^b + c^4 \Leftrightarrow (a - c^2).(a + c^2) = 2^b$, pelo Teorema 3.9.4 existem dois naturais m > n tais que m + n = b, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2.c^2 = 2^m - 2^n \Leftrightarrow c^2 = 2^{n-1}.(2^{m-n} - 1)$. Como 2^{n-1} e $2^{m-n} - 1$ são primos entre si e o seu produto é um quadrado perfeito, novamente pelo Teorema Fundamental da Aritmética 2^{n-1} e $2^{m-n} - 1$ devem ser ambos quadrados perfeitos, logo n – 1 é par e $2^{m-n} - 1 = (2k - 1)^2$ para algum inteiro positivo k. Como $2^{m-n} = (2k - 1)^2 + 1 = 4.k.(k - 1) + 2$ é divisível por 2 mas não por 4, temos m – n = 1. Portanto, fazendo n – 1 = 2t, temos que todas as soluções são da forma (a, b, c) = $(3.2^{2t}, 4.t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções.

Exemplo 4. Sejam $x, y \in \mathbb{N}$, tais que $3x^2 + x = 4y^2 + y$. Prove que x – y é um quadrado perfeito.

Solução. Sejam p um primo e p^a, p^b e p^c as maiores potências de p que dividem x, y e x – y, respectivamente. Suponha, por um momento, que $a \leq b$. Então $p^{2a} \mid x^2, y^2$, e segue da proposição 3.6.9 que $p^{2a} \mid (4y^2 - 3x^2)$. Mas, como $x - y = 4y^2 - 3x^2$, temos então que $p^{2a} \mid (x - y)$ e, daí, $c \geq 2a$. Por outro lado, escrevendo:

$$x^2 = (x - y) - 4.(y^2 - x^2) = (x - y).[1 + 4.(y + x)],$$

concluímos que $p^c \mid x^2$, de modo que $c \leq 2a$ pelo mesmo argumento acima. Portanto, c = $2a$, um número par. Se $a \geq b$, concluímos de modo análogo, que c = 2b. Por fim, como o primo p foi escolhido arbitrariamente, segue do Teorema Fundamental da Aritmética que x – y é um produto de potências de primos com expoentes pares, logo um quadrado perfeito.

Conforme afirmamos antes, Euclides, em sua obra *Os Elementos*, demonstrou o seguinte:

Teorema 3.9.5. (Euclides). Existem infinitos primos.

Demonstração. Suponha por absurdo que p_1, ..., p_k fossem todos os primos. O número $N = p_1 ... p_k + 1 > 1$ não seria divisível por nenhum primo p_i, o que contradiz o Teorema Fundamental da Aritmética.

■

Exemplo. Prove que há infinitos primos da forma 4k – 1.

Solução. Suponha que só houvesse uma quantidade finita de primos da forma 4k – 1, digamos $p_1 = 3$, $p_2 = 7$, $p_3 = 11$, ..., p_t, e considere o número $m = 4.p_1.p_2...p_t - 1$. Claramente, $m > 1$ e, sendo $m' = p_1.p_2...p_t$, temos $m = 4m' – 1$. Por outro lado, o lema 3.9.2 garante a existência de primos ímpares q_1, ..., q_l tais que $m = q_1... q_l$. Observe, agora, que todo primo ímpar é da forma $4q' – 1$ ou $4q' + 1$, para algum $q' \in \mathbb{Z}$. Se fosse $q_i = 4q_i' + 1$ para $1 \leq i \leq t$, teríamos:

$$m = (4q_1' + 1) ... (4q_l' + 1) = 4q + 1,$$

para algum $q \in \mathbb{N}$, contradizendo o fato de ser $m = 4m' – 1$. Portanto, existe $1 \leq i \leq s$ tal que $q_i = 4q_i' - 1$. Finalmente, como $p_1, p_2,..., p_t$ são todos os primos dessa forma, deveríamos ter $q_i = p_j$ para algum $1 \leq j \leq t$. Mas, como $q_i \mid m$, seguiria então que p_j seria um divisor do número $m = 4.p_1.p_2...p_t – 1$, o que é uma contradição. Logo, existem infinitos primos da forma 4k – 1.

Parte inteira de x.

Seja x um número real, sua **parte inteira** $\lfloor x \rfloor$ é definida por:

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}.$$

De outro modo, para $n \in \mathbb{Z}$, temos:

$$\lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1.$$

Por exemplo, como $1 < \sqrt{3} < 2$, temos que $\lfloor \sqrt{3} \rfloor = 1$.

Proposição 3.9.6. (Fórmula de Legendre). Seja p um primo. Então a maior potência de p que divide n! é p^{α} onde

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Observe que a soma é finita, pois os termos $\left\lfloor \frac{n}{p^i} \right\rfloor$ são nulos para $n < p^i$.

Demonstração. No produto n! = 1.2.....n, apenas os múltiplos de p contribuem com um fator p. Há $\left\lfloor \frac{n}{p} \right\rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim sucessivamente, resultando na fórmula de Legendre.

■

Exemplo 1. Determine com quantos zeros termina 1000!.

Solução. O problema é equivalente a determinar qual a maior potência de 10 que divide 1000! E como há muito mais fatores 2 do que 5 em 1000!, o expoente desta potência coincide com a da maior potência de 5 que divide 1000!, ou seja,

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 249.$$

Portanto, 1000! termina com 249 zeros.

Exemplo 2. Qual é a maior potência de 165 que divide em 2000! ?

Solução. Temos que 165 = 3.5.11 e vale $a_{11}(2000) = \left\lfloor \frac{2000}{11} \right\rfloor + \left\lfloor \frac{2000}{121} \right\rfloor + \left\lfloor \frac{2000}{1331} \right\rfloor = 181 + 16 + 1 = 198$. Portanto, é a 198-ésima a maior potência de 165 e também a maior de 11 que divide 2000!.

Curiosidades

I) Em 1970, três pesquisadores que trabalhavam no Massachussets Institute of Tecnology – MIT, nos Estados Unidos, Ron Rivest, Adi Shamir e Leonard Adleman, explorando os trabalhos de Pierre de Fermat, feitos no século XVII, descobriram um

modo de usar os números primos para proteger nossos cartões de créditos, quando fazemos compras pela Internet. Sem o poder dos números primos, esse tipo de comércio jamais poderia existir. Os três pesquisadores citados usaram um processo para manter o número de nossos cartões de crédito em segurança, usando números primos com 100 dígitos. O sistema inventado se chama RSA, sendo R a primeira letra do segundo nome do primeiro cientista, S a primeira letra do segundo nome do segundo cientista e A a primeira letra do segundo nome do terceiro. Hoje em dia, para aumentar a segurança, já se usa números primos com 600 dígitos.

II) Existem infinitos pares de primos da forma (p, p + 2), como (3, 5), (5, 7), (11, 13), (1000000000061, 1000000000063)? Ainda não se sabe.

Eles são chamados **primos gêmeos**. Quantos pares de primos gêmeos você conhece? Com o advento dos computadores, intensificou-se a busca por esses tipos de primos.

III) Os números da forma $M_n = 2^n - 1$ são chamados de **números primos de Mersenne**, devido à importância que estes números têm no estudo da primalidade de outros números, e devido ao padre e matemático francês Marin Mersenne (1588-1648), que estudou essas e várias outras questões sobre números. Se n for um número primo, $2^n - 1$ é chamado número de Mersenne, e pode ser um número primo ou não. Existem infinitos números primos de Mersenne? Acredita-se que sim, mas até o presente momento se conhecem apenas 48 primos de Mersenne, cujo maior número de Mersenne que foi descoberto em 2013, é $2^{57.885.161} - 1$ e tem 17.425.170 dígitos! Deduza daí o maior número perfeito conhecido. Alguns desses cálculos para checar se um número é ou não um primo de Mersenne levam, por exemplo, 29 dias para serem feitos, usando-se um processador 3.0 GHz Intel Core2!

IV) Uma palestra silenciosa.

Em 1644, entre os números da forma $2^n - 1$ que Mersenne afirmara serem primos, estava $2^{67} - 1$. Com referência a esse número, em um encontro da American Mathematical Society, em 1903, o matemático F. N. Cole (1861-1927) deu o que parece ter sido a única palestra silenciosa de toda história. Ao ser anunciada sua conferência, o matemático dirigiu-se lentamente à lousa, escreveu silenciosamente quanto valia $2^{67} - 1$

e, sem pronunciar qualquer palavra, escreveu quanto resultava o produto dos números 193.707.721 e 761.838.257.287, mostrando que dava o mesmo valor. Logo depois, soltou o giz e retornou em silêncio à sua cadeira. Toda a plateia explodiu em entusiástica vibração!

V) Os números da forma $F_n = 2^{2^n} + 1$ ficaram conhecidos como **números de Fermat**, e os números primos dessa forma, como **números primos de Fermat**. Fermat achava que todo número desta forma era primo, mas ele foi traído por seus cálculos. Em 1732, Euler, com sua usual habilidade em lidar com números muito grandes, mostrou a decomposição $2^{2^5} + 1 = 6.700.417 \times 641$. Existem outros primos de Fermat, além de $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$? Os cálculos computacionais não são animadores, já que, até onde se conseguiu verificar, todos os outros números de Fermat são compostos. Chega-se a acreditar que a resposta a essa pergunta é negativa, mas caso exista algum deles será um número muito grande, com vários dígitos. Só para se ter uma ideia do "tamanho" gigantesco desses números, em dezembro de 2014, descobriram que o número $44.670.651 \times 2^{9749} + 1$ divide F_{9747}. Com certeza, brevemente essa descoberta já estará superada.

VI) Alguns problemas em aberto envolvendo números primos:

a) Existe sempre um número primo entre dois quadrados consecutivos de números naturais n^2 e $(n + 1)^2$?

b) Há infinitos primos da forma n! – 1 ou n! + 1? Esses primos são chamados **primos fatoriais**. E primos da forma $n^2 + 1$?

c) Mesma pergunta anterior, onde n! é substituído por #n. Define-se #n como o produto de todos os primos menores do que ou iguais a n.

3.10 Congruência

A teoria da congruência é uma das noções mais revolucionárias do estudo da aritmética, é o instrumento adequado quando se quer dar ênfase ao resto na divisão euclidiana por um número fixado. Ela foi introduzida e extensivamente estudada por

Carl Friederich Gauss (1777-1855) no seu famoso trabalho Disquisitiones Arithmeticae, publicado em 1801, quando tinha apenas 24 anos. Várias ideias de grande importância, que serviram de base para o desenvolvimento da teoria dos números, aparecem neste trabalho. As noções introduzidas por Gauss e suas notações foram imediatamente adotadas pelos matemáticos da época e ainda são usadas na atualidade. Para termos uma ideia ilustrativa da noção de congruência, consideremos o seguinte problema.

Se hoje é quarta-feira, que dia da semana será daqui a 2015 dias?

Para resolver o problema vamos indicar (0) para o dia de hoje (quarta), o 1 para o dia de amanhã (quinta) e assim por diante. Veja a tabela:

Quarta	Quinta	Sexta	Sábado	Domingo	Segunda	Terça
0	1	2	3	4	5	6
7	8	9	10	11	12	13
...	...	...	...	...	...	...

Tabela 1. Dias da semana.

Vamos determinar a coluna em que se encontra o número 2015. Observe que dois números na sequência 0, 1, 2,..., estão na mesma coluna se, e só se, sua diferença é divisível por 7. Suponhamos que o número 2015 está na coluna encabeçada pelo número $0 \leq x \leq 6$. Fazendo uso da divisão euclidiana temos que para algum $q \in \mathbb{Z}$, $2015 = 7.q + x$, com $0 \leq x \leq 6$. E ainda pela unicidade do resto na divisão euclidiana segue-se $2015 = 7.287 + 6$. Assim, temos que após 2015 dias será uma terça-feira.

Definição. Sejam a, b, $n \in \mathbb{Z}$, sendo $n > 1$. Dizemos que a é congruente a b módulo n se os restos da divisão de a e b por n forem iguais, e denotamos $a \equiv b \bmod n$, se $n \mid (a - b)$. Se $n \nmid (a - b)$ dizemos que a é incongruente a b módulo n e denotamos $a \not\equiv b \bmod n$.

Exemplos: $3 \equiv 5 \bmod 2$, pois $2 \mid (3 - 5)$; $2 \equiv -1 \bmod 3$, pois $3 \mid (2 - (-1))$; $15 \not\equiv 10 \bmod 7$, pois $7 \nmid (15 - 10)$.

A notação de congruência módulo n enxerga apenas o resto da divisão de um número por n, contudo podemos estar se perguntando quais as vantagens que teremos em utilizá-la. A primeira contribuição ao se usar congruências é computacional; provaremos algumas propriedades elementares de congruências, as quais vão nos

permitir, por exemplo, calcular mecânica e rapidamente o resto da divisão de 13^{2015} por 11, tarefa que não é fácil de cumprir com os métodos de que dispomos até o presente momento.

Proposição 3.10.1. Sejam dados a, b, c, d, m e n inteiros, com m, n > 1, temos:

a) $a \equiv a$ mod n;

b) Se $a \equiv$ b mod n, então b $\equiv a$ mod n;

c) Se $a \equiv$ b mod n e b $\equiv$ c mod n, então $a \equiv$ c mod n;

d) Se $a \equiv$ b mod n e c $\equiv$ d mod n, então a + c $\equiv$ b + d mod n. Em particular, se $a \equiv$ b mod n, então k.$a \equiv$ k.b mod n para todo k $\in \mathbb{Z}$;

e) Se $a \equiv$ b mod n e c $\equiv$ d mod n, então a.c $\equiv$ b.d mod n;

f) Se $a \equiv$ b mod n, então $a^k \equiv b^k$ mod n, para todo k $\in \mathbb{N}$;

g) Se a.c $\equiv$ b.c mod n e mdc(c, n) = d, então $a \equiv$ b mod $\frac{n}{d}$. Em particular, se mdc(c, n) = 1, então $a \equiv$ b mod n;

h) Se $a \equiv$ b mod n e se m $\mid$ n, então $a \equiv$ b mod m;

i) Se $a \equiv$ b mod n, então mdc(a, n) = mdc(b, n);

j) Se a + c $\equiv$ b + c mod n, então $a \equiv$ b mod n;

k) Se $a \equiv$ b (mod m.n), então $a \equiv$ b mod m e $a \equiv$ b mod n;

l) Se $a \equiv$ b mod n e $a \equiv$ b mod m, com mdc(n, m) = 1, então $a \equiv$ b (mod n.m).

Demonstração.

a) Observe que n $\mid$ $a - a$ = 0.

b) Se n $\mid$ a – b, então n $\mid$ - (a – b) $\Leftrightarrow$ n $\mid$ b – a.

c) Se n $\mid a$ – b e n $\mid$ b – c, então n $\mid (a$ – b) + (b – c) $\Leftrightarrow$ n $\mid a$ – c.

d) Se n $\mid a$ – b e n $\mid$ c – d, logo n $\mid (a$ – b + c – d) e, portanto, a + c $\equiv$ b + d mod n. O caso particular segue de k $\equiv$ k mod n.

e) Temos que n $\mid a - b$ e n $\mid$ c – d. Como a.c – b.d = a.(c – d) + d.(a – b), segue-se que n $\mid$ (a.c – b.d) e, consequentemente, a.c ≡ b.d mod n.

f) Fazendo c = a e d = b no item e), obtemos $a^2 \equiv b^2$ mod n. Se já mostramos que $a^j \equiv b^j$ mod n, para um certo j ∈ ℕ, então, novamente do item e) (dessa vez com c = a^j e d = b^j), obtemos $a^{j+1} = a.\ a^j \equiv$ b. $b^j = b^{j+1}$ mod n. O item f) segue, por indução sobre k.

g) Sejam n = d.n' e c = d.c', com c' e n' inteiros primos entre si. De a.c ≡ b.c mod n, segue que (d.n') $\mid$ [d.c'.(a – b)] ou, ainda, que n' $\mid$ c'.(a – b). Mas, como mdc(n', c') = 1, segue da proposição 3.8.9 que n' $\mid a -$ b ou, o que é o mesmo, $a \equiv$ b mod $\frac{n}{d}$. O resto é imediato.

h) Se n $\mid a -$ b e como m $\mid$ n, segue-se que m $\mid a -$ b. Logo, $a \equiv$ b mod m.

i) Como $a \equiv$ b mod n, existe q ∈ ℤ tal que a = b + n.q. Queremos, pois, mostrar que mdc(b + n.q, n) = mdc(b, n). Mas isso é imediato a partir da proposição 3.8.10.

j) Se a + c ≡ b + c mod n, então n divide (a + c) – (b + c) = a – b, o que é o mesmo que $a \equiv$ b mod n.

k) Se m.n $\mid a -$ b, então m $\mid a -$ b. Mas essa última relação equivale a $a \equiv$ b mod m; analogamente, $a \equiv$ b mod n.

l) Como m, n $\mid a -$ b e mdc(m, n) = 1, segue do item b) da proposição 3.8.9 que m.n $\mid a -$ b, que é o que queríamos provar.

■

Chamaremos de sistema completo de resíduos módulo n a todo conjunto de números naturais cujos restos pela divisão por n são os números 0, 1, ..., n – 1, sem repetições e numa ordem qualquer. Além disso, dois desses números distintos não são congruentes módulo n. O sistema de invertíveis módulo n é todo conjunto de números naturais tais que o máximo divisor comum entre n e qualquer elemento do conjunto é um, isto é, mdc(n, k) = 1 para todo k pertencente ao conjunto.

Exemplo 1. Ana, Bernardo e Carla arrumam laranjas para vender na feira, colocando 12 laranjas em cada saco. Ana tinha 389 laranjas, Bernardo 188 e Carla 97. Depois de arrumar todas as laranjas nos sacos, quantas sobraram ao todo?

Solução. Para resolvermos o problema, temos que observar que precisamos considerar, para cada um deles, a quantidade de laranjas módulo 12. Como 389 ≡ 5 mod 12, 188 ≡ 8 mod 12 e 97 ≡ 1 mod 12, quando Ana terminou de arrumar as laranjas nos sacos, sobraram 5 laranjas, das laranjas de Bernardo sobraram 8 e das de Carla sobrou 1. Portanto, no final sobraram 5 + 8 + 1 = 14 laranjas. Mas, 14 ≡ 2 mod 12. Isso significa que eles, em conjunto, poderiam completar mais um saco com 12 laranjas e sobrariam apenas 2 laranjas.

Exemplo 2. Calcule o resto da divisão do número 17^{2002} por 13.

Solução. Como 17 ≡ 4 mod 13 e 16 ≡ 3 mod 13, segue do item f) da proposição 3.10.1 que, módulo 13, $17^{2002} \equiv 4^{2002} \equiv 16^{1001} \equiv 3^{1001}$.

Notando, agora, que $3^3 \equiv 1$ mod 13 e aplicando os itens e) e f) da proposição 3.10.1, obtemos:

$$3^{1001} \equiv 3^2 . 3^{999} \equiv 9.(3^3)^{333} \equiv 9. 1^{333} = 9, \text{ módulo } 13.$$

Então, segue que 17^{2002} deixa resto 9 na divisão por 13.

Exemplo 3. Mostre que o número $43^{101} + 23^{101}$ é divisível por 66.

Solução. Ora, como 66 = 6.11, então, um número é divisível por 66 se, e só se, é divisível simultaneamente por 6 e 11. Agora, 43 ≡ 1 mod 6 e 23 ≡ -1 mod 6. Portanto, podemos dizer que, $43^{101} \equiv 1$ mod 6 e $23^{101} \equiv -1$ mod 6. Somando ambas as congruências, obtemos $43^{101} + 23^{101} \equiv 1 + (-1)$ mod 6, que é o mesmo que $43^{101} + 23^{101} \equiv 0$ mod 6. Assim, $43^{101} + 23^{101}$ é divisível por 6. Resta mostrar que $43^{101} + 23^{101}$ é divisível por 11. Para isso, observe que 43 ≡ -1 mod 11 e 23 ≡ 1 mod 11. Portanto, podemos dizer que $43^{101} \equiv -1$ mod 11 e $23^{101} \equiv 1$ mod 11. Logo, $43^{101} + 23^{101} \equiv 0$ mod 11, que é o mesmo que dizer que $43^{101} + 23^{101}$ é divisível por 11. Portanto, como $43^{101} + 23^{101}$ é divisível simultaneamente por 6 e por 11, ou seja, $43^{101} + 23^{101}$ é divisível por 66.

Exemplo 4. Dado um inteiro qualquer n, podemos afirmar que o número $(n^2 + 1)$ não é divisível por 3.

Solução. De fato, na divisão de um número inteiro por 3, os possíveis restos são 0, 1 ou 2. Desse modo, acontece uma, e só uma, das seguintes possibilidades: ou $n \equiv 0 \bmod 3$, ou $n \equiv 1 \bmod 3$, ou $n \equiv 2 \bmod 3$.

Se $n \equiv 0 \bmod 3$, então, $n^2 \equiv 0 \bmod 3$. Daí, segue que $n^2 + 1 \equiv 1 \bmod 3$. Portanto, nesse caso, $n^2 + 1$ deixa resto 1 quando dividido por 3.

Se $n \equiv 1 \bmod 3$, então, $n^2 + 1 \equiv 2 \bmod 3$. Nesse caso, $n^2 + 1$ deixa resto 2 quando dividido por 3.

Se $n \equiv 2 \bmod 3$, então, $n^2 \equiv 2^2 \bmod 3$, que é o mesmo que $n^2 \equiv 1 \bmod 3$. Logo, podemos dizer que $n^2 + 1 \equiv 2 \bmod 3$. Assim, na divisão por 3 o número $n^2 + 1$ deixa resto 1. Logo, para todo n, $n^2 + 1$ não é divisível por 3.

Exemplo 5. Determine os restos das divisões de:

a) 3^{1000} por 101 b) $5^{3^{20}}$ por 13

Solução.

a) Como $3^4 \equiv -20 \bmod 101$, elevando ao quadrado obtêm $3^8 \equiv 400 \bmod 101 \Leftrightarrow 3^8 \equiv -4 \bmod 101$. Multiplicando por 3^2, obtemos $3^{10} \equiv -36 \bmod 101$. Portanto,

$3^{20} \equiv 1296 \bmod 101 \Leftrightarrow 3^{20} \equiv -17 \bmod 101$

$3^{40} \equiv 289 \bmod 101 \Leftrightarrow 3^{40} \equiv -14 \bmod 101$

$3^{80} \equiv 196 \bmod 101 \Leftrightarrow 3^{80} \equiv -6 \bmod 101$

$3^{80}.\ 3^{20} \equiv (-6).(-17) \bmod 101 \Leftrightarrow 3^{100} \equiv 1 \bmod 101$.

Contudo, elevando a última congruência a 10, obtemos $3^{1000} \equiv 1 \bmod 101$, ou seja, 3^{1000} deixa resto 1 na divisão por 101.

b) Note que como $5^4 \equiv 1 \bmod 13$, os restos de 5^n por 13 se repetem com período 4:

$5^0 \equiv 1 \bmod 13$ $5^4 \equiv 1 \bmod 13$ .....

$5^1 \equiv 5 \bmod 13$ $5^5 \equiv 5 \bmod 13$ .....

$5^2 \equiv -1 \bmod 13$ $\quad$ $5^6 \equiv -1 \bmod 13$ $\quad$ .....

$5^3 \equiv -5 \bmod 13$ $\quad$ $5^7 \equiv -5 \bmod 13$ $\quad$ .....

Por outro lado, temos $3 \equiv -1 \bmod 4 \Longrightarrow 3^{20} \equiv 1 \bmod 4$, isto é, 3^{20} deixa resto 1 na divisão por 4. Assim, $5^{3^{20}} \equiv 5^1 \bmod 13$, ou seja, $5^{3^{20}}$ deixa resto 5 na divisão por 13.

Exemplo 6. Vamos determinar o algarismo das unidades do número 7^{7^7}.

Solução. Ora, vamos determinar o algarismo das unidades de todo número da forma 7^{7^α}, onde α é um número natural ímpar. Note que $7 \equiv -3 \bmod 10$ e, portanto, temos que $7^{7^\alpha} \equiv -3^{7^\alpha} \bmod 10$, já que 7^α é ímpar.

Por outro lado, de $3^2 + 1 \equiv 0 \bmod 10$, do fato de $(7^\alpha - 1)/2$ é ímpar, temos que:

$$(3^2)^{\frac{7^\alpha - 1}{2}} + 1 \equiv 0 \bmod 10.$$

Logo, $3^{7^\alpha} + 3 = 3.[(3^2)^{\frac{7^\alpha - 1}{2}} + 1] \equiv 0 \bmod 10$, e, portanto, $7^{7^\alpha} \equiv 7^{7^\alpha} + 3^{7^\alpha} + 3 \equiv 3 \bmod 10$.

Consequentemente, o algarismo das unidades de 7^{7^α} é 3.

Exemplo 7. Mostre que a equação $x^3 - 117y^3 = 5$ não possui soluções inteiras.

Solução. Veja que como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer:

$x^3 - 117y^3 \equiv 5 \bmod 9 \Leftrightarrow x^3 \equiv 5 \bmod 9$.

Porém, x só pode deixar resto 0, 1, ..., 8 na divisão por 9. Analisando estes 9 casos, temos:

$x \bmod 9$	0	1	2	3	4	5	6	7	8
$x^3 \bmod 9$	0	1	8	0	1	8	0	1	8

ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo, $x^3 \equiv 5 \bmod 9$ é impossível e a equação não possui soluções inteiras.

Em 1770, Eduard Waring (1734–1798), matemático inglês, afirmou em seu livro Medidationes algebraicae, que um de seus estudantes, John Wilson (1741 – 1793), conjecturou que, se p é um número inteiro primo, então p divide (p – 1)! + 1. Mas, Wilson não conseguiu provar. O resultado foi provado por Legendre, em 1771, que provou também a recíproca.

Teorema (Wilson) 3.10.2. Seja n > 1. Então n $\mid$ (n – 1)! + 1 se, e só se, n é primo. Mais precisamente,

$$(n-1)! \equiv \begin{cases} -1 \bmod n, & \text{se n é primo} \\ 0 \bmod n, & \text{se n é composto e } n \neq 4. \end{cases}$$

Demonstração. Se n é composto, mas não é o quadrado de um primo podemos escrever n = ab com 1 < a < b < n. Neste caso tanto a quanto b são fatores de (n – 1)! e portanto (n – 1)! ≡ 0 mod n. Se n = p^2, p > 2, então p e 2p são fatores de (n – 1)! e novamente (n – 1)! ≡ 0 mod n; isto demonstra que para todo n ≠ 4 composto temos (n – 1)! ≡ 0 mod n. Se n é primo podemos escrever (n – 1)! ≡ - 2.3....(n – 2) mod n, pois (n – 1) ≡ - 1 mod n; então podemos juntar os inversos aos pares no produto do lado direito, donde (n – 1)! ≡ - 1 mod n.

■

Exemplo 1. Mostrar que se p é um primo ímpar, então 2.(p – 3)! ≡ - 1 mod p.

Solução. Sendo p primo, temos pelo teorema 3.10.2 que (p – 1)! ≡ - 1 mod p; mas, (p – 1)! = (p – 1).(p – 2).(p – 3)!. E, como p – 1 ≡ - 1 mod p e p – 2 ≡ - 2 mod p para p ≠ 2, temos (p – 1).(p – 2).(p – 3)! ≡ (- 1).(- 2).(p – 3)! ≡ 2.(p – 3)! ≡ - 1 mod p.

Exemplo 2. Mostre que p é o menor primo que divide (p – 1)! + 1.

Solução. Pelo teorema 3.10.2 p $\mid$ [(p – 1)! + 1]. Assim, como qualquer primo menor que p divide (p – 1)!, nenhum deles pode dividir (p – 1)! + 1, pois, neste caso, deveria dividir 1. Logo, p é o menor primo tendo esta propriedade.

Numa carta para Bernard Frenicle de Bessy (1605–1675), datada de 18 de outubro de 1640, Pierre de Fermat (1601–1665) deu sua versão do que hoje conhecemos como Pequeno Teorema de Fermat. Ele descobriu algo surpreendente e que foi usado para a criação do sistema RSA. Fermat descobriu que se você, por exemplo, calcular as potências de 2 em uma calculadora comum e verificar o resto na divisão por 7, estes restos têm um padrão: começando com 2^0, após 6 cálculos consecutivos o resto volta e ser 1, veja a tabela a seguir:

Potência de 2	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
Visor da calculadora	1	2	4	8	16	32	64	128	256	512	1024	2048	4096
Resto da divisão por 7	1	2	4	1	2	4	1	2	4	1	2	4	1

Tabela 2. As potências de 2 e seus restos na divisão por 7.

Fermat, ainda viu que este padrão se mantinha se ele substituísse 7 por qualquer número primo, enunciando o seguinte:

Teorema (Pequeno Teorema de Fermat) 3.10.3. Para a, p ∈ $\mathbb{Z}$, com p primo, temos $a^{\mathrm{p}} \equiv a$ mod p. Em particular, se mdc(a, p) = 1, então $a^{\mathrm{p}-1} \equiv 1$ mod p.

Demonstração. Se $a^{\mathrm{p}} \equiv a$ mod p, então p divide $a^{\mathrm{p}} - a = a.(a^{\mathrm{p}-1} - 1)$; Logo, se mdc($a$, p) = 1, $a^{\mathrm{p}-1} \equiv 1$ mod p segue do item a) da proposição 3.8.9. Basta, pois, mostrarmos que $a^{\mathrm{p}} \equiv a$ mod p, para todo $a \in \mathbb{Z}$.

Se p = 2 o resultado é óbvio, uma vez que $a^2 - a = a.(a - 1)$, sendo o produto de dois inteiros consecutivos, é par. Suponhamos, então, que p > 2 e provemos o resultado, primeiramente para $a > 0$, por indução sobre a. Para $a = 1$ nada há a fazer. Suponha, por hipótese de indução, o teorema válido para um certo valor natural de a, isto é, suponha que $\mathrm{k}^{\mathrm{p}} \equiv \mathrm{k}$ mod p, para algum k ∈ $\mathbb{N}$. Para $a = \mathrm{k} + 1$, temos

$$(\mathrm{k}+1)^{\mathrm{p}} - (\mathrm{k}+1) = (\mathrm{k}^{\mathrm{p}} - \mathrm{k}) + \sum_{j=1}^{p-1} \binom{p}{j} \mathrm{k}^{\mathrm{p}-\mathrm{j}}.$$

Mas, como p $\mid (k^p - k)$ pela hipótese e p $\mid \binom{p}{j}$ para $1 \leq j \leq p - 1$, segue que p divide $(k + 1)^p - (k + 1)$, ou seja, que $(k + 1)^p \equiv (k + 1) \bmod p$.

Analisemos, agora, o caso $a \leq 0$; se $a = 0$, nada há a fazer; se $a < 0$, então, uma vez que p é ímpar, segue do que fizemos acima que

$$a^p = -(-a)^p \equiv -(-a) = a \bmod p.$$

■

Exemplo 1. Determinar o resto da divisão de 2^{100000} por 17.

Solução. Pelo teorema 3.10.3 temos $a^{p-1} \equiv 1 \bmod p$ quando p é primo e p ł a. Portanto, como 17 é primo e 17 ł 2, temos $2^{16} \equiv 1 \bmod 17$. Mas $100000 = 6250.16$ e, portanto, $2^{100000} = (2^{16})^{6250} \equiv 1^{6250} \equiv 1 \bmod 17$. Assim, o resto da divisão por 17 de 2^{100000} é 1.

Exemplo 2. Se p e q são primos distintos, prove que p.q divide $p^{q-1} + q^{p-1} - 1$.

Solução. Como p e q são primos distintos, temos mdc(p, q) = 1. Portanto, pelo teorema 3.10.3, q divide $p^{q-1} - 1$. Mas, como q também divide q^{p-1}, segue que q divide $q^{q-1} + (p^{q-1} - 1)$. Analogamente, p divide $p^{q-1} + (q^{p-1} - 1)$. Por fim, como ambos p e q dividem $p^{q-1} + q^{p-1} - 1$ e mdc(p, q) = 1, o item b) da proposição 3.8.9 garante que p.q divide $p^{q-1} + q^{p-1} - 1$.

Exemplo 3. Se p é um número primo ímpar, então p $\mid [2^{p-1} + (p - 1)!]$.

Solução. De fato, sendo p um número primo ímpar, pelo teorema 3.10.3, temos que p $\mid 2^{p-1} - 1$. Por outro lado, pelo teorema 3.10.2, p $\mid (p - 1)! + 1$. Portanto, p $\mid \{(2^{p-1} - 1) + [(p - 1)! + 1]\}$.

Exemplo 4. Verifique que 17 divide $11^{104} + 1$.

Solução. 17 é um número primo e 11 não divide 17. Assim, pelo teorema 3.10.3, $11^{16} \equiv 1 \bmod 17$. Por outro lado, pelo Algoritmo da Divisão, $104 = 16.6 + 8$. Assim, $11^{104} =$

$(11^{16})^6.11^8 \equiv (1)^6.11^8 \bmod 17 \equiv 11^8 \bmod 17$. Agora, observe que: $11^2 = 121 \equiv 2 \bmod 17$ e $11^8 = (11^2)^4 \equiv 2^4 \bmod 17 \equiv -1 \bmod 17$. Portanto, podemos afirmar que $11^{104} \equiv 11^8 \bmod 17 \equiv -1 \bmod 17$, que é o mesmo que afirmar que 17 divide $11^{104} + 1$.

Função de Euler

Dado um número natural n é importante saber a quantidade de números naturais menores do que n e relativamente primos com n. Essa curiosidade nos remete à definição da chamada função de Euler.

$\varphi: \mathbb{N} \rightarrow \mathbb{N}$, tal que $n \in \mathbb{N}$.

$\varphi(n)$ = a quantidade de números naturais $k < n$, tais que k e n são primos entre si. Vejamos o seguinte exemplo. Os valores de:

a) $\varphi(12) = 4$, pois os únicos números naturais que são menores que 12 e relativamente primos com ele são $\{1, 5, 7, 11\}$.

b) $\varphi(17) = 16$, pois os números naturais que são menores que 17 e relativamente primos com ele são $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

Euler observou que se p é um número primo, assim como no item b) do exemplo anterior, então $\varphi(p) = p - 1$. Além disso, descobriu uma generalização do Teorema de Fermat, como veremos a seguir.

Teorema (Euler) 3.10.4. Sejam n e a inteiros positivos primos entre si. Então $a^{\varphi(n)} \equiv 1 \bmod n$.

Demonstração. Observemos que se $r_1, r_2, \ldots, r_{\varphi(n)}$ é um sistema completo de invertíveis módulo n e a é um número natural tal que $mdc(a, n) = 1$, então $ar_1, ar_2, \ldots, ar_{\varphi(n)}$ também é um sistema completo de invertíveis módulo n. De fato, temos que $mdc(ar_i, n) = 1$ para todo i e se $ar_i \equiv ar_j \bmod n$, então $r_i \equiv r_j \bmod n$ pois a é invertível módulo n, logo $r_i = r_j$ e portanto $i = j$. Consequentemente cada ar_i deve ser congruente com algum r_j e, portanto,

$$\prod_{1 \le i \le \varphi(n)} (ar_i) \equiv \prod_{1 \le i \le \varphi(n)} r_i \mod n \iff a^{\varphi(n)} . \prod_{1 \le i \le \varphi(n)} r_i \equiv \prod_{1 \le i \le \varphi(n)} r_i \mod n.$$

Mas como cada r_i é invertível módulo n, simplificando o fator $\prod_{1 \le i \le \varphi(n)} r_i$, obtemos o resultado desejado.

■

Exemplo 1. Encontre o resto da divisão do número 39^{3602} por 14.

Solução. O número ao qual 39^{3602} é congruente é o resto solicitado. Ora, 39 e 14 são primos entre si e $\varphi(14) = \varphi(2.7) = \varphi(2).\varphi(7) = 1.6 = 6$ e $3602 = 600.6 + 2$. Pelo Teorema de 2.10.4, temos $39^{\varphi(14)} = 39^6 \equiv 1 \mod 14$, donde $39^{3600} \equiv 1 \mod 14$, o que nos dá $39^{3602} = 39^{3600}.39^2 \equiv 39^2 \mod 14$. Como $39 \equiv 11 \mod 14$, segue que $39^2 \equiv 11^2 \mod 14 = 121 \mod 14 \equiv 9 \mod 14$. Portanto, 9 é o resto solicitado.

Exemplo 2. Mostre que não existe inteiro x tal que $103 \mid x^3 - 2$.

Solução. Observe que 103 é primo. Agora suponha que $x^3 \equiv 2 \mod 103$, de modo que 103 ł x. Elevando ambos os lados desta congruência a $\frac{103-1}{3} = 34$, obtemos $x^{102} \equiv 2^{34} \mod 103$ e sabemos pelo teorema 3.10.4 que $x^{102} \equiv 1 \mod 103$. Porém, fazendo as contas, obtemos que $2^{34} \equiv 46 \mod 103$, uma contradição. Portanto, não há inteiro x tal que $103 \mid x^3 - 2$.

Exemplo 3. Mostre que existem infinitos números da forma 2000...009 que são múltiplos de 2009.

Solução. O problema é equivalente a encontrar infinitos naturais k tais que $2.10^k + 9 \equiv 0 \mod 2009 \iff 2.10^k + 9 \equiv 2009 \mod 2009 \iff 10^{k-3} \equiv 1 \mod 2009$, pois 2000 é invertível módulo 2009. Como mdc(10, 2009) = 1, pelo teorema 3.10.4 temos que $10^{\varphi(2009)} \equiv 1 \mod 2009 \Longrightarrow 10^{\varphi(2009).t} \equiv 1 \mod 2009$ para todo $t \in \mathbb{N}$, logo basta tomar $k = \varphi(2009).t + 3$.

Observação: Deixaremos para o próximo capítulo, o assunto sobre as congruências lineares, pois este tema é estreitamente relacionado com os estudos das equações diofantinas.

Curiosidade

A **conjectura de Goldbach**, proposta pelo matemático prussiano Christian Goldbach, é um dos problemas não resolvidos da Matemática, mais precisamente da Teoria dos Números, mais antigos atualmente. Ela diz que todo número par maior ou igual a 4 é a soma de dois primos. Por exemplo: 4 = 2 + 2; 6 = 3 + 3; 8 = 5 + 3; 10 = 3 + 7 = 5 + 5; 12 = 5 + 7; etc. Verificações por computador já confirmaram a conjectura de Goldbach para vários números. No entanto, a efetiva demonstração matemática ainda não ocorreu. O melhor resultado até agora foi dado por Olivier Ramaré em 1995: *todo número par é a soma de até 6 números primos*. Em 7 de junho de 1742, o matemático prussiano Christian Goldbach escreveu uma carta a Leonhard Euler, onde ele propôs a seguinte conjectura: *Todo inteiro par maior que 2 pode ser escrito como a soma de 3 números primos.* Ele considerava o número 1 como sendo primo, que uma convenção posterior (e presente até hoje) abandonou. Uma visão moderna da Conjectura (e a mais aceita) é: *Todo inteiro par maior que 5 pode ser escrito como a soma de 3 números primos*. Euler, interessado pelo problema, respondeu que a conjectura era equivalente à outra: *Todo inteiro par maior que 2 pode ser escrito como a soma de 2 números primos*. Euler adicionou, ainda, que estava absolutamente certo sobre isso, porém não era capaz de prová-lo. A versão de Euler é a mais conhecida e divulgada atualmente, também a mais aceita, por ser mais simples e abrangente. Para valores pequenos de n, a conjectura de Goldbach pode ser testada diretamente (método conhecido jocosamente pelos matemáticos como força bruta e ignorância). Em 1938, N. Pipping testou todos os números até 10^5.

4 EQUAÇÕES DIOFANTINAS

"*Não se preocupem com suas dificuldades em Matemática, posso assegurar-lhes que as minhas são bem maiores.*"

(Albert Einstein)

Definição: Equações Diofantinas são equações polinomiais, em várias incógnitas, com coeficientes inteiros (ou racionais) das quais se buscam soluções restritas ao conjunto dos números inteiros.

Então, de modo geral, uma Equação Diofantina é uma equação do tipo $f(x_1, x_2, \ldots, x_n) = 0$, onde f é uma função n-variável com $n \geq 2$ e coeficientes inteiros. As soluções de f são as n-uplas $(a_1, a_2, \ldots, a_n)$ em que $a_i \in \mathbb{Z}$, $1 \leq i \leq n$.

Exemplo. $26x + 18y = 10$; $x^2 = y^2 + 13$.

Chamaremos de Equações Diofantinas lineares as equações do tipo $a_1.x_1 + a_2.x_2 + \ldots + a_n.x_n = b$, sendo $a_1, a_2, \ldots, a_n$ e b números inteiros (ou racionais), cujas soluções são inteiros $x_1, x_2, \ldots, x_n$.

Dada uma equação diofantina, é natural formular as seguintes perguntas:

a) Sob quais condições a equação admite soluções?
b) Se tem solução, o número de soluções é finito ou infinito?
c) Quando existem soluções finitas, como determiná-las?

Nós podemos naturalmente nos perguntar se não existe uma teoria mais geral. Este é em essência o décimo problema de Hilbert: dada uma equação diofantina

com qualquer número de incógnitas e com coeficientes inteiros, descrever um processo que determine, em um número finito de passos, se a equação admite solução inteira. Este problema foi resolvido por Martin Davis, Yuri Matiyasevich, Hilary Putnam e Julia Robinson, não por eles terem descrito um procedimento, mas por eles terem demonstrado que não existe um algoritmo que, dada uma equação diofantina, decida se a equação admite solução inteira.

4.1 Métodos fundamentais para resolução de Equações Diofantinas

Antes de respondermos as perguntas que foram formuladas anteriormente, vejamos sete métodos elementares para se resolver algumas equações diofantinas.

4.1.1 Método da fatoração

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:

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

Agora vejamos alguns exemplos usando o método da fatoração.

Exemplo 1. Determine as soluções inteiras da equação $6x^2 - 2y^2 + xy - 5 = 0$.

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

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

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

Exemplo 2. Determine todas as soluções inteiras não negativas da equação

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

Solução. Reescrevendo a equação temos $(xy - 7)^2 = x^2 + y^2 \Leftrightarrow x^2y^2 - 14xy + 49 = x^2 + y^2 \Leftrightarrow x^2y^2 - 12xy + 36 + 13 = x^2 + 2xy + y^2 \Leftrightarrow (xy - 6)^2 - (x + y)^2 = -13$.
Logo, $(xy - 6)^2 - (x + y)^2 = -13 \Leftrightarrow [(xy - 6) - (x + y)][(xy - 6) + (x + y)] = -13$, o que nos conduz aos sistemas:

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

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

que se assemelham aos sistemas,

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

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

Resolvendo os sistemas, obtemos (− 7, 0), (0, − 7), (3, 4), (4, 3), (− 3, − 4), (− 4, − 3), (0, 7) e (7, 0) como soluções. Portanto, as soluções inteiras e não negativas da equação $(xy - 7)^2 = x^2 + y^2$ são (3, 4), (4, 3), (0, 7) e (7, 0).

Exemplo 3. Determine todas as soluções inteiras da equação $x^2(y - 1) + y^2(x - 1) = 1$.

Solução. Façamos $x = u + 1$ e $y = v + 1$, substituindo na equação dada, temos $(u+1)^2v + (v+1)^2u = 1 \Leftrightarrow u^2v + 2uv + v + uv^2 + 2uv + u = 1 \Leftrightarrow uv(u+v) + 4uv + (u+v) = 1 \Leftrightarrow uv(u+v+4) + (u+v+4) = 5 \Leftrightarrow (uv+1)(u+v+4) = 5$. Assim, a equação $(uv+1)(u+v+4) = 5$ nos leva aos sistemas:

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

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

Estes sistemas são equivalentes aos sistemas:

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

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

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

Exemplo 4. Determine todas as soluções inteiras positivas da equação

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

Solução. Fatorando a equação temos $\frac{1}{x} + \frac{1}{y} = \frac{1}{6} \Leftrightarrow 6(x+y) - xy = 0 \Leftrightarrow 6x + 6y - xy = 0 \Leftrightarrow x(6-y) + 6y - 36 = -36 \Leftrightarrow x(6-y) - 6(6-y) = -36 \Leftrightarrow (x-6)(y-6) = 36$.

Veja que $\frac{1}{x} < \frac{1}{6}$, logo, $x > 6$ e, assim, $x - 6 > 0$. Contudo, a equação $(x-6)(y-6) = 36$ nos conduz aos sistemas:

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

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

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

Exemplo 5. Encontre todas as soluções para a equação $(x^2 + 1).(y^2 + 1) + 2(x - y).(1 - xy) = 4.(1 + xy)$.

Solução. Vamos escrever a equação na forma

$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x - y).(1 - xy) = 4,$$

ou

$$(xy - 1)^2 + (x - y)^2 - 2.(x - y).(xy - 1) = 4.$$

Isto é equivalente a

$$[(xy - 1) - (x - y)]^2 = 4,$$

ou

$$(x + 1).(y - 1) = \pm 2.$$

Se $(x + 1).(y - 1) = 2$, obtêm-se os sistemas de equações

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

obtendo-se as soluções (1, 2), (- 3, 0), (0, 3), (- 2, - 1).

Se (x + 1).(y - 1) = - 2, obtêm-se os sistemas

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

cujas soluções são (1, 0), (- 3, 2), (0, - 1), (- 2, 3).

Todos os oito pares ordenados que determinamos satisfazem a equação dada.

Observação: Vejamos agora um exemplo interessante de uma equação não polinomial, mas que se resolve pelo método da fatoração.

Exemplo. Prove que a equação $2^n + 1 = q^3$ não admite soluções em inteiros positivos n e q.

Solução. Veja que para n = 1, 2, 3 a equação não admite solução, pois $q^3 = 3$, $q^3 = 5$ e $q^3 = 9$ respectivamente, não possuem soluções inteiras positivas. Fatorando obtemos: $2^n = (q - 1).(q^2 + q + 1)$. Como $q - 1 \mid 2^n$ devemos ter q = 2 ou q = 2k + 1 para algum $k \in \mathbb{N}$. Temos que q = 2 não produz solução, pois $2^n = 7$ não admite solução inteira positiva. Então, se q = 2k + 1, temos que $2^n = (2k)[(2k+1)^2 + 2k + 1 + 1] = (2k)(4k^2 + 4k + 1 + 2k + 2) = (2k)(4k^2 + 6k + 3) = 8k^3 + 12k^2 + 6k$. Como n > 3, $8 \mid 2^n$. Mas se k é ímpar, $8k^3 + 12k^2 + 6k$ não é múltiplo de 8. Agora se k é par, $8k^3 + 12k^2 + 6k = 2k.(4k^2 + 6k + 3) = 2^n$. Então, 2^n é igual ao produto de um número par por um ímpar, já que 2k é par e $4k^2 + 6k + 3$ é ímpar. Mas, uma potência de 2 nunca possui um fator ímpar maior que 1 em sua fatoração. Portanto, a equação $2^n + 1 = q^3$ não admite solução.

4.1.2 Utilizando Inequações para Resolver Equações Diofantinas

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. Vejamos alguns exemplos da aplicação deste método.

Exemplo 1. Determine as soluções inteiras da equação

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

Solução. Veja que, devido à simetria da equação, os pares da forma (x, y) = (k, - k) com $k \in \mathbb{Z}$, são soluções. Se $x + y \neq 0$, a equação fica

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

ou ainda, multiplicando por 2, depois somando 2 a ambos os membros e em seguida reordenando os termos, temos:

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

que equivale a

$$(x - y)^2 + (x - 1)^2 + (y - 1)^2 = 2. \qquad \text{(I)}$$

Como $(x - 1)^2 + (y - 1)^2 \leq 2$, segue que, $(x - 1)^2 \leq 1$ e $(y - 1)^2 \leq 1$. Isto restringe os valores das variáveis x e y no intervalo [0, 2]. Se $x = 0$, substituindo na equação (I), temos $y^2 + 1 + y^2 - 2y + 1 = 2 \Leftrightarrow y^2 - y = 0$, que nos dá o par ordenado (0, 1); se $x = 1$, temos $y^2 - 2y = 0$, que nos dá os pares ordenados (1, 0) e (1, 2); e se $x = 2$, temos $y^2 - 3y + 2 = 0$, que nos dá os pares ordenados (2, 2) e (2, 1).

Contudo, obtemos as soluções (0, 1), (1, 0), (1, 2), (2, 2), (2, 1) e (k, - k) com $k \in \mathbb{Z}$.

Exemplo 2. Encontre as soluções inteiras positivas da equação

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

Solução. Por causa da simetria da equação, podemos assumir que $2 \leq x \leq y \leq z$. Isto implica que

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

Se $x = 2$, temos

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

Isso acarreta que

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

Daí segue que

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

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

Se $x = 3$, temos

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

Isto implica que

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

Segue que

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

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

Se $x = 4$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{7}{20}.$$

Isto acarreta que

$$\frac{2}{y} \geq \frac{7}{20} \Longrightarrow y \in \{4, 5\}.$$

Segue que

$$z = \frac{20y}{7y - 20}.$$

Neste caso a única solução é (4, 4, 10).

Se $x = 5$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{2}{5}.$$

Isto acarreta que

$$\frac{2}{y} \geq \frac{2}{5} \Longrightarrow y \in \{5\}.$$

Segue que

$$z = \frac{5y}{2y - 5}.$$

Neste último caso a única solução é (5, 5, 5).
Portanto, as soluções inteiras da equação dada são (2, 11, 110), (2, 12, 60), (2, 14, 35), (2, 15, 30), (2, 20, 20), (3, 4, 60), (3, 5, 15), (3, 6, 10), (4, 4, 10) e (5, 5, 5).

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

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

Seja (x, y) solução para $x \geq 1$. Então $8x^3 < 8x^3 + 8x < 8x^3 + 4x^2 + 4x + 1$, ou seja, $(2x)^3 < y^3 < (2x + 1)^3$, que é uma contradição. Logo, $x < 1$.

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

Exemplo 4. Encontre todas as soluções em inteiros da equação
$x^3 + (x + 1)^3 + (x + 2)^3 + ... + (x + 7)^3 = y^3$.

Solução. Sendo $P(x) = x^3 + (x + 1)^3 + (x + 2)^3 + ... + (x + 7)^3 = 8x^3 + 84x^2 + 420x + 784$. Se $x \geq 0$, então $(2x + 7)^3 = 8x^3 + 84x^2 + 294x + 343 < P(x) < 8x^3 + 120x^2 + 600x + 1000 = (2x + 10)^3$, assim $2x + 7 < y < 2x + 10$; Por conseguinte, y é $2x + 8$ ou $2x + 9$. Mas nenhuma das equações

$$P(x) - (2x + 8)^3 = -12x^2 + 36x + 272 = 0,$$
$$P(x) - (2x + 9)^3 = -24x^2 - 66x + 55 = 0,$$

tem quaisquer raízes inteiras, assim não existe soluções com $x \geq 0$. Agora, veja que P satisfaz $P(-x-7) = -P(x)$, então (x, y) é uma solução se e só se (- x - 7, - y) é uma solução. Portanto não existem soluções com $x \leq -7$. Assim, para (x, y) ser uma solução, devemos ter $-6 \leq x \leq -1$. Para $-3 \leq x \leq -1$, temos P (-1) = 440, não um cubo, P (- 2) = $216 = 6^3$, e P (- 3) = $64 = 4^3$, de modo que (- 2, 6) e (- 3, 4) são as únicas soluções com $-3 \leq x \leq -1$. Portanto (- 4, - 4) e (- 5, - 6) são as únicas soluções com $-6 \leq x \leq -4$. Contudo, as únicas soluções são (- 2, 6), (- 3, 4), (- 4, - 4) e (- 5, - 6).

Exemplo 5. Encontre todos os triplos (x, y, z) de inteiros positivos tais que

$$\left(1+\frac{1}{x}\right).\left(1+\frac{1}{y}\right).\left(1+\frac{1}{z}\right) = 2.$$

Solução. Sem perda de generalidade, podemos assumir $x \geq y \geq z$. Observe que devemos ter $2 \leq (1 + 1/z)^3$, o que implica que $z \leq 3$.

Se $z = 1$, então $\left(1+\frac{1}{x}\right).\left(1+\frac{1}{y}\right) = 1 \Leftrightarrow \frac{1}{x}+\frac{1}{y}+\frac{1}{xy} = 0 \Leftrightarrow \frac{y+x+1}{xy} = 0 \Leftrightarrow x + y = -1$, o que é claramente impossível.

O caso $z = 2$ leva a $\left(1+\frac{1}{x}\right).\left(1+\frac{1}{y}\right) = \frac{4}{3}$. Assim $\frac{4}{3} \leq \left(1+\frac{1}{y}\right)^2$, o que obriga $y < 7$. Desde $1+\frac{1}{x} > 1$, obtemos $y > 3$. Conectando os valores apropriados produz as soluções (7, 6, 2), (9, 5, 2), (15, 4, 2).

Se $z = 3$, então $\left(1+\frac{1}{x}\right).\left(1+\frac{1}{y}\right) = \frac{3}{2}$. Uma análise semelhante leva a $y < 5$ e $y \geq z = 3$. Estes valores produzem as soluções (8, 3, 3) e (5, 4, 3).

Concluímos que as soluções são todas as permutações de (7, 6, 2), (9, 5, 2), (15, 4, 2), (8, 3, 3) e (5, 4, 3).

4.1.3 O método paramétrico

Em muitas situações, as soluções integrais para uma Equação Diofantina $f(x_1, x_2, ..., x_n) = 0$ pode ser representada de um modo paramétrico como se segue: $x_1 = g_1(k_1, k_2, ..., k_l)$, $x_2 = g_2(k_1, k_2, ..., k_l)$, ..., $x_n = g_n(k_1, k_2, ..., k_l)$, onde $g_1, g_2, ..., g_n$ são funções com l variáveis e $k_1, k_2, ..., k_l \in \mathbb{Z}$. O conjunto de soluções para algumas equações diofantinas podem ter múltiplas representações paramétricas. Para a

maioria destas equações não é possível encontrar todas as soluções explicitamente. Em muitos casos o método paramétrico fornece uma prova da existência de um número infinito de soluções.

Exemplo 1. Prove que existem infinitos triplos (x, y, z) de inteiros tais que

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2.$$

Solução. Definindo z = - y, a equação torna-se $x^3 = x^2 + 2y^2$. Tomando y = mx, m ∈ ℤ, teremos $x = 1 + 2m^2$. Obtemos um conjunto infinito de soluções

$$x = 2m^2 + 1, \quad y = m(2m^2 + 1), \quad z = -m(2m^2 + 1), \quad m \in \mathbb{Z}.$$

Exemplo 2. Vejamos este exemplo de uma equação não diofantina. a) Sejam m e n inteiros positivos distintos. Prove que existem infinitos triplos (x, y, z) de inteiros positivos tais que $x^2 + y^2 = (m^2 + n^2)^z$, com
i) z ímpar; ii) z par.
b) Prove que a equação $x^2 + y^2 = 13^z$ tem infinitas soluções nos inteiros positivos x, y, z.

Solução. a) Para i), considere o conjunto

$$x_k = m(m^2 + n^2)^k, \quad y_k = n(m^2 + n^2)^k, \quad z_k = 2k + 1, \quad k \in \mathbb{Z}_+.$$

Para ii), considere o conjunto

$$x_k = |m^2 - n^2|.(m^2 + n^2)^{k-1}, \quad y_k = 2mn(m^2 + n^2)^{k-1}, \quad z_k = 2k, \quad k \in \mathbb{Z}_+.$$

b) Desde $2^2 + 3^2 = 13$, podemos tomar m = 2, n = 3 e obter os conjuntos soluções

$$x_k' = 2.13^k, \quad y_k' = 3.13^k, \quad z_k' = 2k + 1, \quad k \in \mathbb{Z}_+;$$

$$x_k'' = 5.13^{k-1}, \quad y_k'' = 12.13^{k-1}, \quad z_k'' = 2k, \quad k \in \mathbb{Z}_+.$$

Observações.

1) Tendo em conta a identidade de Lagrange

$$(a^2 + b^2).(c^2 + d^2) = (ac - bd)^2 + (ad - bc)^2,$$

podemos gerar um conjunto infinito de soluções, definindo de forma recursiva as sequências $(x_k)_{k \geq 1}$, $(y_k)_{k \geq 1}$ como segue:

$$\begin{cases} x_{k+1} = mx_k - ny_k \\ y_{k+1} = nx_k + my_k \end{cases}, \quad \text{em que } x_1 = m,\ y_1 = n.$$

Não é difícil verificar que $(|x_k|, y_k, k)$, $k \in \mathbb{Z}_+$, são soluções da equação dada.

2) Outra maneira de gerar um conjunto de infinitas soluções é com os números complexos. Seja k um inteiro positivo. Temos $(m + in)^k = A_k + iB_k$, onde A_k, $B_k \in \mathbb{Z}$. Tomando módulos, obtemos,

$$(m^2 + n^2)^k = {A_k}^2 + {B_k}^2,$$

e portanto, $(|A_k|, |B_k|, k)$ é uma solução da equação dada.

Exemplo 3. Encontrar todos os triplos (x, y, z) de inteiros positivos tais que $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$.

Solução. A equação é equivalente a $z = \frac{xy}{x+y}$. Seja d = mdc(x, y). Em seguida temos x = dm, y = dn, com mdc(m, n) = 1. Segue-se que o mdc(m.n, m + n) = 1. Portanto,

$$z = \frac{dmn}{m+n},$$

implicando que (m + n) | d, isto é, d = k(m + n), $k \in \mathbb{Z}_+$.

As soluções para a equação são dadas por x = km(m + n), y = kn(m + n), z = kmn, onde k, m, n ∈ $\mathbb{Z}_+$.

Observações.

1) Se a, b, c são inteiros positivos com nenhum fator comum tais que

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$

temos que a + b é um quadrado perfeito. Com efeito, k = 1, a = m(m + n), b = n(m + n), e portanto, a + b = $(m + n)^2$.

2) Se a, b, c são números inteiros positivos que satisfazem

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$

então $a^2 + b^2 + c^2$ é um quadrado perfeito. De fato,

$$\begin{aligned} a^2 + b^2 + c^2 &= k^2[m^2(m+n)^2 + n^2(m+n)^2 + m^2n^2] \\ &= k^2[(m+n)^4 - 2mn(m+n)^2 + m^2n^2] \\ &= k^2[(m+n)^2 - mn]^2. \end{aligned}$$

Exemplo 4. Prove que para cada inteiro n ≥ 3 a equação $x^n + y^n = z^{n-1}$ tem infinitas soluções nos inteiros positivos.

Solução. Um conjunto infinito de soluções é dado por

$$x_k = k(k^n + 1)^{n-2}, \quad y_k = (k^n + 1)^{n-2}, \quad z_k = (k^n + 1)^{n-1}, \quad k \in \mathbb{Z}_+.$$

4.1.4 O Método Aritmético Modular

Em muitas situações, as considerações aritméticas modulares simples são empregadas em mostrar que determinadas equações diofantinas não são solucionáveis ou em reduzir a escala de suas soluções possíveis.

Exemplo 1. Prove que a equação $(x + 1)^2 + (x + 2)^2 + ... + (x + 2001)^2 = y^2$ não tem solução.

Solução. Seja x = z - 1001. A equação se torna

$$(z - 1000)^2 + ... + (z - 1)^2 + z^2 + (z + 1)^2 + ... + (z + 1000)^2 = y^2,$$

ou

$$2001z^2 + 2(1^2 + 2^2 + ... + 1000^2) = y^2.$$

Daqui resulta que

$$2001z^2 + 2.\frac{1000.1001.2001}{6} = y^2,$$

ou equivalentemente,

$$2001z^2 + 1000.1001.667 = y^2.$$

O lado esquerdo é congruente a 2 mod 3, por isso não pode ser um quadrado perfeito.

Exemplo 2. Encontre todos os pares (p, q) de números primos tais que $p^3 - q^5 = (p + q)^2$.

Solução. A única solução é (7, 3). Primeiro suponha que nem p e nem q são iguais a 3. Em seguida, p ≡ 1 ou 2 mod 3 e q ≡ 1 ou 2 mod 3. Se p ≡ q mod 3, temos que, o lado esquerdo é divisível por três, enquanto que o lado direito não é. Se p ≢ q mod 3, o lado direito é divisível por 3, enquanto que o lado esquerdo não é.

Se p = 3, temos que $q^5 < 27$, o que é impossível.

Se q = 3, obtemos $p^3 - 243 = (p + 3)^2$, cuja única solução inteira é p = 7.

Exemplo 3. Prove que a equação $x^5 - y^2 = 4$ não admite soluções nos números inteiros.

Solução. Consideremos a equação módulo 11. Uma vez que $(x^5)^2 = x^{10} \equiv 0$ ou 1 mod 11 para todo x, temos $x^5 \equiv -1, 0$ ou 1 mod 11. Assim $x^5 - 4$ é congruente a 6, 7 ou 8 módulo 11. No entanto, os resíduos quadrados módulo 11 são 0, 1, 3, 4, 5 e 9, de modo que a equação não tem soluções inteiras.

Exemplo 4. Determine todos os números primos p para os quais o sistema de equações

$$\begin{cases} p + 1 = 2x^2 \\ p^2 + 1 = 2y^2 \end{cases},$$

tem uma solução em números inteiros x, y.

Solução. O único tal primo é p = 7. Suponha sem perda de generalidade que $x, y \geq 0$. Observe que $p + 1 = 2x^2$ é par, então $p \neq 2$. Além disso, $2x^2 \equiv 1 \equiv 2y^2 \bmod p$, o que implica $x \equiv \pm y \bmod p$, uma vez que p é ímpar. Como $x < y < p$, temos $x + y = p$. Em seguida

$$p^2 + 1 = 2(p - x)^2 = 2p^2 - 4px + p + 1,$$

de modo que $p = 4x - 1$, $2x^2 = 4x$, x é 0 ou 2, e p é – 1 ou 7. Naturalmente, - 1 não é primo, mas para p = 7, (x, y) = (2, 5) é uma solução.

4.1.5 O Método de Indução Matemática

Indução matemática é um método poderoso e elegante para provar declarações dependendo de inteiros não negativos. Sobre indução matemática, o leitor pode consultar a seção 3.5.2. Este método de prova é amplamente utilizado em várias áreas da matemática, por exemplo, em teoria dos números. Os exemplos seguintes destinam-se a mostrar como a indução matemática funciona em equações diofantinas.

Exemplo 1. Prove que para todos os inteiros $n \geq 3$, existem inteiros positivos ímpares x, y, tal que $7x^2 + y^2 = 2^n$.

Solução. Vamos provar que existem inteiros positivos ímpares x_n, y_n de tal modo que $7{x_n}^2 + {y_n}^2 = 2^n$, $n \geq 3$.

Para $n = 3$, temos $x_3 = y_3 = 1$. Agora, suponha que para um determinado inteiro $n \geq 3$ temos inteiros ímpares x_n, y_n satisfazendo $7{x_n}^2 + {y_n}^2 = 2^n$. Vamos apresentar um par (x_{n+1}, y_{n+1}) de inteiros positivos ímpares tais que $7{x_{n+1}}^2 + {y_{n+1}}^2 = 2^{n+1}$. De fato,

$$7\left(\frac{x_n \pm y_n}{2}\right)^2 + \left(\frac{7x_n \mp y_n}{2}\right)^2 = 2(7{x_n}^2 + {y_n}^2) = 2^{n+1}.$$

Precisamente um dos números $\frac{x_n + y_n}{2}$ e $\frac{|x_n - y_n|}{2}$ é ímpar (uma vez que a sua soma seja maior do que x_n e y_n, que é ímpar). Se, por exemplo, $\frac{x_n + y_n}{2}$ é ímpar, temos

$$\frac{7x_n - y_n}{2} = 3x_n + \frac{x_n - y_n}{2}$$

também é ímpar (como uma soma de um número ímpar e um número par); portanto neste caso podemos escolher

$$x_{n+1} = \frac{x_n + y_n}{2} \quad \text{e} \quad y_{n+1} = \frac{7x_n - y_n}{2}.$$

Se $\frac{x_n - y_n}{2}$ é ímpar, então

$$\frac{7x_n + y_n}{2} = 3x_n + \frac{x_n + y_n}{2},$$

assim podemos escolher

$$x_{n+1} = \frac{|x_n - y_n|}{2} \quad \text{e} \quad y_{n+1} = \frac{7x_n + y_n}{2}.$$

Exemplo 2. Provar que para todos os inteiros positivos n, a equação $x^2 + y^2 + z^2 = 59^n$ é solúvel em números inteiros positivos.

Solução. Nós usaremos a indução matemática com s = 2 e $n_0 = 1$. Observe que para $(x_1, y_1, z_1) = (1, 3, 7)$ e $(x_2, y_2, z_2) = (14, 39, 42)$, temos

$$x_1^2 + y_1^2 + z_1^2 = 59 \quad \text{e} \quad x_2^2 + y_2^2 + z_2^2 = 59^2.$$

Definimos agora (x_n, y_n, z_n), $n \geq 3$, por

$$x_{n+2} = 59x_n, \quad y_{n+2} = 59y_n, \quad z_{n+2} = 59z_n,$$

para todo $n \geq 1$. Então

$$x^2_{k+2} + y^2_{k+2} + z^2_{k+2} = 59^2(x^2_k + y^2_k + z^2_k);$$

daí $x^2_k + y^2_k + z^2_k = 59^k$ que implica $x^2_{k+2} + y^2_{k+2} + z^2_{k+2} = 59^{k+2}$.

Observação. Podemos escrever as soluções como

$$(x_{2n-1}, y_{2n-1}, z_{2n-1}) = (1.59^{n-1}, 3.59^{n-1}, 7.59^{n-1})$$

e

$$(x_{2n}, y_{2n}, z_{2n}) = (14.59^n, 39.59^n, 42.59^n), \; n \geq 1.$$

Exemplo 3. Prove que, para todo $n \geq 3$ a equação

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$$

é solúvel em inteiros positivos distintos.

Solução. Para o caso básico n = 3 temos

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=\ 1.$$

Assumindo que para algum k ≥ 3,

$$\frac{1}{x_1}+\ \frac{1}{x_2}+\cdots+\ \frac{1}{x_k}=\ 1,$$

em que x_1, x_2, ..., x_k são inteiros positivos distintos, obtemos

$$\frac{1}{2x_1}+\ \frac{1}{2x_2}+\cdots+\ \frac{1}{2x_k}=\ \frac{1}{2}.$$

Daí resulta que

$$\frac{1}{2}+\frac{1}{2x_1}+\ \frac{1}{2x_2}+\cdots+\ \frac{1}{2x_k}=1,$$

onde 2, $2x_1$, $2x_2$, ..., $2x_k$ são distintos.

Exemplo 4. Prove que para todo n ≥ 412 existem inteiros positivos x_1, x_2, ..., x_n de modo que

$$\frac{1}{{x_1}^3}+\ \frac{1}{{x_2}^3}+\cdots+\ \frac{1}{{x_n}^3}=\ 1. \qquad (*)$$

Solução. Temos que

$$\frac{1}{a^3}=\frac{1}{(2a)^3}+\ldots+\frac{1}{(2a)^3}$$

onde o lado direito é composto por oito termos, por isso, se a equação (*) é solúvel em números inteiros positivos, então assim é a equação

$$\frac{1}{{x_1}^3}+\ \frac{1}{{x_2}^3}+\cdots+\ \frac{1}{{x_{n+7}}^3}=\ 1.$$

Utilizando o método de indução matemática com ritmo 7, ele é suficiente para provar a resolubilidade da equação (*) para n = 412, 413, ..., 418. A ideia-chave é construir uma solução em cada um dos casos acima de menores módulo 7. Observe que

$\frac{27}{3^3}$ = 1 e 27 ≡ 412 mod 7,

$\frac{4}{2^3} + \frac{9}{3^3} + \frac{36}{6^3}$ = 1 e 4 + 9 + 36 = 49 ≡ 413 mod 7,

$\frac{4}{2^3} + \frac{32}{4^3}$ = 1 e 4 + 32 = 36 ≡ 414 mod 7,

$\frac{18}{3^3} + \frac{243}{9^3}$ = 1 e 18 + 243 = 261 ≡ 415 mod 7,

$\frac{18}{3^3} + \frac{16}{4^3} + \frac{144}{12^3}$ = 1 e 18 + 16 + 144 = 178 ≡ 416 mod 7,

$\frac{4}{2^3} + \frac{16}{4^3} + \frac{36}{6^3} + \frac{144}{12^3}$ = 1 e 4 + 16 + 36 + 144 = 200 ≡ 417 mod 7.

Finalmente,

$$\frac{4}{2^3} + \frac{9}{3^3} + \frac{81}{9^3} + \frac{324}{18^3} = 1 \text{ e } 4 + 9 + 81 + 324 = 418.$$

4.1.6 Método do descenso infinito de Fermat ou descida de Fermat

Dada uma equação $f(x_1, x_2, ..., x_n) = 0$, 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

$$S = \{(x_1, x_2, ..., x_n) \in \mathbb{Z}^n \diagup\ f(x_1, x_2, ..., x_n) = 0\}$$

é diferente de vazio, então gostaríamos de considerar a solução minimal em certo sentido. Ou seja, queremos construir uma função φ: S → ℕ e considerar a solução $(x_1, x_2, ... , x_n) \in S$ com $\varphi(x_1, x_2, ... , x_n)$ mínimo. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos conduz claramente a uma

contradição, provando que S é de fato vazio. Para trabalharmos este método consideremos os exemplos abaixo.

O método da descida de Fermat consiste então no seguinte esquema:

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 1. Resolva em inteiros não negativos a equação

$$x^3 + 2y^3 = 4z^3.$$

Solução. Observe que (0, 0, 0) é uma solução. Vamos provar que não há outras soluções. Suponhamos o contrário, que a equação possui soluções (x, y, z) nos inteiros positivos. Então, dentre todas as soluções (x, y, z), com x, y e z inteiros positivos, existe uma (x, y, z) = (x_1, y_1, z_1) para a qual $z = z_1$ é o menor possível. Trabalhemos tal solução.

De ${x_1}^3 + 2{y_1}^3 = 4{z_1}^3$ segue-se que $2 \mid x_1$, assim $x_1 = 2x_2$, com $x_2 \in \mathbb{Z}_+$. Daí vem que ${4x_2}^3 + {y_1}^3 = 2{z_1}^3$. Assim $y_1 = 2y_2$, com $y_2 \in \mathbb{Z}_+$, substituindo na equação, chegamos a ${2x_2}^3 + 4{y_2}^3 = {z_1}^3$. Também, $z_1 = 2z_2$, com $z_2 \in \mathbb{Z}_+$, logo a equação fica ${x_2}^3 + 2{y_1}^3 = 4{z_1}^3$. Assim obtemos outra solução (x_2, y_2, z_2) da equação original, com $z_2 = \frac{z_1}{2} < z_1$. Mas isso é uma contradição, pois partimos de uma solução na qual o valor de $z = z_1$ era mínimo possível. Logo, nossa equação não possui soluções inteiras positivas, apenas a única solução (0, 0, 0).

Exemplo 2. Demonstrar que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas.

Solução. Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira com x, y, z > 0. Assim existe uma solução (a, b, c) pela 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 $c > \frac{c}{d^2}$. 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 tais que

$$a^2 = m^2 - n^2,\ b^2 = 2mn \text{ e } c = m^2 + n^2.$$

Temos da primeira equação que (a, n, m) é tripla pitagórica primitiva e assim m é ímpar. Logo, de $b^2 = 2mn$ concluímos que b, e portanto n, é par. Observando ainda que $b^2 = (2n)m$ é um quadrado perfeito e $mdc(2n, m) = 1$, concluímos que tanto 2n como m são quadrados perfeitos, pelo qual podemos encontrar inteiros positivos s e t tais que

$$2n = 4s^2 \quad \text{e} \quad m = t^2.$$

Por outra parte, dado que $a^2 + n^2 = m^2$, então existirão inteiros positivos i e j, primos entre si, tais que

$$a = i^2 - j^2, \quad n = 2ij \quad \text{e} \quad m = i^2 + j^2.$$

Logo, $s^2 = \frac{n}{2} = ij$, assim i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$.
Portanto temos que $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$, assim

$$t^2 = u^4 + v^4,$$

ou seja, (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 solução.

Exemplo 3. Encontrar todas as soluções inteiras positivas da equação

$$m^2 - mn - n^2 = \pm 1.$$

Solução. Observe que $m^2 = n^2 + mn \pm 1 \geq n^2 \Longrightarrow m \geq n$, com igualdade se, e só se, (m, n) = (1, 1), que é claramente uma solução. Agora seja (m, n) uma solução com m > n. Provaremos que (n, m – n) também é solução. Para isto vejamos que

$n^2 - n(m - n) - (m - n)^2 = n^2 - nm + n^2 - m^2 + 2mn - n^2 = n^2 + nm - m^2 = -(m^2 - nm - n^2) = \mp 1$,

Portanto, se temos uma solução (m, n), podemos encontrar uma cadeia descendente de soluções, e este processo terminará quando atingirmos uma solução (a, b) com a = b, isto é, a solução (1, 1). Invertendo o processo, encontraremos assim todas as soluções, ou seja, se (m, n) é solução então (m + n, m) é solução. Logo todas as soluções positivas são

$$(1, 1), (2, 1), (3, 2), ..., (F_{n+1}, F_n), ...$$

onde F_n representa o n-ésimo termo da sequência de Fibonacci.

Observação: Vejamos um exemplo de uma equação não diofantina, mas que se resolve pelo método da descida de Fermat.

Exemplo. Resolva em inteiros não negativos a equação

$$2^x - 1 = xy.$$

Solução. Observe as soluções (0, k), $k \in \mathbb{Z}_+$, e (1, 1). Vamos provar que não há outras soluções usando o método do descenso infinito de Fermat sobre os fatores primos de x. Seja $p_1 > 2$ um divisor primo de x com $p_1 \mid 2^x - 1$ e seja q o menor inteiro positivo tal que $p_1 \mid 2^q - 1$. Pelo pequeno teorema de Fermat temos $p_1 \mid 2^{p_1 - 1} - 1$, e portanto $q \leq p_1 - 1 < p_1$.

Vamos provar agora que $q \mid x$. Se isso não ocorre, então x = kq + r, com 0 < r < q, e

$$2^x - 1 = 2^{kq}. 2^r - 1 = (2^q)^k. 2^r - 1 = (2^q - 1 + 1)^k. 2^r - 1 \equiv 2^r - 1 \bmod p_1.$$

Segue-se que $p_1 \mid 2^r - 1$, o que contradiz a minimalidade de q. Assim $q \mid x$ e $1 < q < p_1$. Agora seja $p_2 \mid 2^x - 1$ um divisor primo de q. É claro que p_2 é um divisor de x e $p_2 < p_1$. Dando continuidade a esse procedimento, construímos uma sequência decrescente infinita de divisores primos de x: $p_1 > p_2 > p_3 > ...$, uma contradição pelo fato de não existir uma sequência de números inteiros não negativos tais que $x_1 > x_2 > ....$

4.1.7 Equações diofantinas variadas

Muitas equações diofantinas elementares não são dos tipos descritos nas seções anteriores. No que se segue, apresentamos alguns exemplos de tais equações.

Exemplo 1. Resolva em inteiros positivos o sistema de equações

$$\begin{cases} x^2 + 3y = u^2 \\ y^2 + 3x = v^2 \end{cases}.$$

Solução. As desigualdades

$$x^2 + 3y \geq (x+2)^2, \quad y^2 + 3x \geq (y+2)^2$$

não podem ser ambas verdadeiras, senão teríamos uma contradição, pois

$$x^2 + 3y \geq (x+2)^2 \Leftrightarrow x^2 + 3y \geq x^2 + 4x + 4 \Leftrightarrow 3y \geq 4x + 4 \Leftrightarrow 3y - 4x \geq 4$$

e

$$y^2 + 3x \geq (y+2)^2 \Leftrightarrow y^2 + 3x \geq y^2 + 4y + 4 \Leftrightarrow 3x - 4y \geq 4,$$

somando as equações obtidas temos $-x - y \geq 8 \Leftrightarrow x + y \leq -8$. Assim, pelo menos uma das desigualdades $x^2 + 3y < (x+2)^2$ e $y^2 + 3x < (y+2)^2$ é verdadeira. Sem perda de generalidade, suponha que $x^2 + 3y < (x+2)^2$. Então $x^2 < x^2 + 3y < (x+2)^2$ implicando em $x^2 + 3y = (x+1)^2$ ou, $3y = 2x + 1$. Obtemos $x = 3k + 1$, $y = 2k + 1$ para algum k inteiro não negativo e $y^2 + 3x = 4k^2 + 13k + 4$. Para $k > 5$, $(2k+3)^2 <$

$4k^2 + 13k + 4 < (2k + 4)^2$; portanto, $y^2 + 3x$ não pode ser um quadrado perfeito. Assim, precisamos apenas considerar $k \in \{0, 1, 2, 3, 4\}$. Apenas $k = 0$ faz $y^2 + 3x$ um quadrado perfeito; portanto, a única solução é

$$x = y = 1, \quad u = v = 2.$$

Exemplo 2. Resolva a equação

$$1 + x_1 + 2x_1x_2 + ... + (n - 1)\, x_1x_2... x_{n-1} = x_1x_2... x_n$$

em inteiros positivos distintos $x_1, x_2, ..., x_n$.

Solução. Escrevendo a equação na forma

$$x_1(x_2... x_n - (n - 1)\, x_2... x_{n-1} - ... - 2x_2 - 1) = 1$$

produz $x_1 = 1$ e

$$x_2(x_3... x_n - (n - 1)\, x_3... x_{n-1} - ... - 3x_3 - 2) = 2.$$

Porque $x_2 \neq x_1$, segue-se que $x_2 = 2$ e que

$$x_3(x_4... x_n - (n - 1)\, x_4... x_{n-1} - ... - 4x_4 - 3) = 3.$$

Nós temos $x_3 \neq x_2$ e $x_3 \neq x_1$; portanto, $x_3 = 3$. Continuando este procedimento (o que equivale a uma "indução finita"), obtemos

$$x_1 = 1, x_2 = 2, ..., x_{n-1} = n - 1.$$

Finalmente, segue-se que $(n - 1).(x_n - (n - 1)) = n - 1$, isto é, $x_n = n$.

Observação. Substituindo na equação fornece a identidade

$$1 + 1.1! + 2.2! + ... + (n - 1).(n - 1)! = n!.$$

Observação: Vejamos agora um exemplo interessante de uma equação não polinomial.

Exemplo. Resolva em inteiros positivos a equação

$$7^x + x^4 + 47 = y^2.$$

Solução. Se x for ímpar, temos que $7^x \equiv -1 \bmod 4$ pela proposição 2.6.12, $x^4 \equiv 1 \bmod 4$ pois $x^2 \equiv 1 \bmod 4$ e $47 \equiv 3 \bmod 4$, portanto $7^x + x^4 + 47 \equiv 3 \bmod 4$, e uma vez em que não existe quadrados perfeitos desta forma, não há soluções neste caso.

Vamos supor que x = 2k, para algum número inteiro positivo k. Para $k \geq 4$, teremos

$$(7^k)^2 < 7^{2k} + (2k)^4 + 47 < (7^k + 1)^2.$$

De fato, a desigualdade esquerda é clara, e a da direita é $7^{2k} + 8k^4 + 47 < 7^{2k} + 2.7^k + 1 \Leftrightarrow 8k^4 + 23 < 7^k$, o que pode ser justificado usando indução matemática.

Basta considerarmos $k \in \{1, 2, 3\}$. Apenas k = 2 produz uma solução. Assim, x = 4, y = 52 é a única solução.

4.2 Equações Diofantinas Lineares de Duas Variáveis

Vamos iniciar com um exemplo.

Vamos supor que só existiam moedas de 15 e de 7 escudos e que eu queria pagar (em dinheiro) uma certa quantia em escudos. Será que é sempre possível? E se só existissem moedas de 12 e de 30 escudos?

No primeiro caso, se conseguirmos pagar 1 escudo, então também sabemos pagar qualquer quantia; basta repetir o pagamento de 1 escudo as vezes que forem necessárias. Para se pagar 1 escudo, podemos usar uma moeda de 15 e receber de troco

duas moedas de 7. Assim, se quisermos pagar 23 escudos podemos usar 23 moedas de 15 e receber de troco 46 moedas de 7. É óbvio que seria mais simples pagar com 2 moedas de 15 e receber 1 moeda de 7 de troco. No fundo estamos a encontrar soluções inteiras da equação 7x + 15y = 1.

No segundo caso é claro que qualquer quantia que se consiga pagar é necessariamente múltipla de 6, porque 12 e 30 são múltiplos de 6. De contra partida, podemos pagar 6 escudos usando uma moeda de 30 e recebendo de troco duas moedas de 12. Deste modo podemos fazer o pagamento de qualquer quantia que seja múltipla de 6.

Definição: Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é dita equação diofantina linear. A resolução de vários problemas de aritmética que exigem soluções inteiras recai, em várias situações, na resolução de equações desta forma. Nem sempre essas equações apresentam soluções, vejamos, por exemplo, a equação $4x + 6y = 5$; veja que não há nenhuma solução inteira para a equação, pois, o primeiro membro da equação é par e, nunca será igual ao segundo membro que é um número ímpar. Sabemos que uma equação do tipo $ax + by = c$, em que se admitem valores reais para as incógnitas x e y, representa uma reta no plano cartesiano. Então, podemos interpretar a resolução da equação diofantina como o problema de determinar os pontos da reta que têm ambas coordenadas inteiras. Ainda existem equações do tipo $ax + by = c$, sem soluções inteiras, que, geometricamente, evitam todos os pontos do produto cartesiano $\mathbb{Z} \times \mathbb{Z} = \{(x, y) / x, y \in \mathbb{Z}\}$. Por exemplo, a equação $12x + 8y = 5$ não tem soluções inteiras, já que mdc(12, 8) = 4 que não divide 5. É natural perguntar-se quais são as condições necessárias e suficientes para que a equação diofantina linear tenha solução e como fazer para encontrá-las. As perguntas serão solucionadas a seguir.

Teorema 4.2.1. Sejam a, b, c $\in \mathbb{Z}$ com a e b não ambos nulos e seja d = mdc(a, b). A equação diofantina linear $ax + by = c$ tem solução em $\mathbb{Z}$ se, e só se, d divide c.

Demonstração. Suponhamos que a equação tenha solução e que existam x e y $\in \mathbb{Z}$ tal que $ax + by = c$. Como d $\mid a$ e d $\mid$ b, temos que d divide qualquer combinação linear formada pelos inteiros a e b, portanto, d $\mid (ax + by)$, ou seja, d $\mid$ c.

E reciprocamente temos por hipótese que d $\mid$ c. Assim, existe k $\in \mathbb{Z}$ tal que kd = c. Usando o teorema 3.8.2, existem α, $\beta \in \mathbb{Z}$ tais que $a\alpha$ + bβ = d. Multiplicando essa igualdade por k obtemos ($a\alpha$)k + (bβ)k = dk, ou seja, a(αk) + b(βk) = c, o que mostra que αk = x e βk = y, e assim (x_0, y_0) = (αk, βk) é solução da equação ax + by = c.

■

Teorema 4.2.2. Sejam a, b, c, k $\in \mathbb{Z}$ e d = mdc(a, b). Se d ł c, então a equação ax + by = c não tem solução inteira. Se d | c a equação possui infinitas soluções e se x = x_0 e y = y_0 é uma solução particular, então todas as soluções são dadas por:

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

Demonstração. Se d ł c, então a equação não possui solução, pois, como d | a e d | b, d deveria dividir c, uma vez que c é uma combinação linear de a e b. Suponhamos, portanto, que d | c. Pelo Teorema 3.8.2, existem inteiros n_0 e m_0, tais que an_0 + bm_0 = d. Como d | c, existe um inteiro k tal que c = kd. Multiplicando an_0 + bm_0 = d por k, teremos a(n_0k) + b(m_0k) = kd = c. Isto nos diz que o par ordenado (x_0, y_0) com x_0 = n_0k e y_0 = m_0k é uma solução de ax + by = c.

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

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

Assim, mostramos que conhecida uma solução particular dada pelo par ordenado (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Resta mostrar que toda solução da equação ax + by = c é da forma x = x_0 + $\left(\frac{b}{d}\right)$k e y = y_0 - $\left(\frac{a}{d}\right)$k. Vamos supor que o par ordenado (x, y) seja uma solução, isto é, ax + by = c. Mas como ax_0 + by_0 = c, obtemos, subtraindo membro a membro, que

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

o que acarreta $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$, segue do Corolário 3.8.8,

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

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

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

Logo, pelo item a) da proposição 3.8.9, $\left(\frac{b}{d}\right) \mid (x - x_0)$. Assim, existe um inteiro k tal que $x - x_0 = k\left(\frac{b}{d}\right)$. Substituindo esse valor na equação (I) temos $y = y_0 - \left(\frac{a}{d}\right)k$ o que completa a demonstração.

■

A solução (x_0, y_0) da equação $ax + by = c$, é chamada de solução minimal se sendo (x_1, y_1) uma solução qualquer da equação, temos que $x_0 \leq x_1$.

Voltemos ao exemplo anterior. Uma vez que a equação $15x + 7y = 17$ tem como solução particular $x = 3$, $y = -4$ (por exemplo), para pagar 17 escudos, basta pagar com 3 moedas de 15 escudos e receber de troco 4 moedas de 7 escudos. Outra hipótese seria pagar com 11 moedas de 7 escudos e receber de troco 4 moedas de 15 escudos. É claro que os teoremas anteriores nos dá um método de encontrar todas as soluções possíveis.

Exemplo 1. A equação $18x + 24y = 5$ não admite solução pois $mdc(18, 24) = 6$ e $6 \nmid 5$.

Exemplo 2. Determine as soluções da equação $28x + 90y = 22$.

Solução. Vamos inicialmente calcular o mdc(28, 90).

	3	4	1	2
90	28	6	4	2
6	4	2	0	

Visto que mdc(28, 90) = 2 e 2 $\mid$ 22, a equação admite soluções. Usando o algoritmo da divisão de trás para frente, temos

$$2 = 6 - 1.4$$
$$4 = 28 - 4.6$$
$$6 = 90 - 3.28$$

Segue-se que $2 = 6 - 1.(28 - 4.6) = (-1).28 + 5.6 = (-1).28 + 5.(90 - 3.28) = (-16).28 + 5.90$

Portanto, $2 = (-16).28 + 5.90$.

Multiplicando ambos os membros desta igualdade por 11, temos

$$22 = (-176).28 + 55.99.$$

Logo, uma solução particular da equação é dada por $(x_0, y_0) = (-176, 55)$. Pelo teorema 4.2.2, a solução geral é

$$x = -176 + 45t$$
$$y = 55 - 14t, \quad \text{com } t \in \mathbb{Z}.$$

Exemplo 3. Encontrar as soluções da equação $-26x + 39y = 65$.

Solução. Dividindo os coeficientes da equação $-26x + 39y = 65$ por 13, obtemos a equação equivalente $-2x + 3y = 5$. Como o mdc(2, 3) = 1, esta última equação possui solução, e, portanto a equação dada também. Temos que encontrar (x_0, y_0), solução de $-2x + 3y = 1$, que gera o par $(5x_0, 5y_0)$, solução da equação original. Aplicando o algoritmo de Euclides para o cálculo de mdc temos:

	1	2
3	2	1
1	0	

Assim, $1 = 3.1 – 2.1$

$1 = - 2.1 + 3.1$

Daí, como $(x_0, y_0) = (1, 1)$, temos que $(5x_0, 5y_0) = (5, 5)$ é uma solução particular da equação dada, e sua solução geral é:

$x = 5 + 3t$

$y = 5 + 2t$, com $t \in \mathbb{Z}$.

Exemplo 4. Determinar todas as soluções inteiras e positivas da equação diofantina $18x + 5y = 48$.

Solução. Determinemos o mdc(18, 5) pelo algoritmo de Euclides:

	3	1	1	2
18	5	3	2	1
3	2	1	0	

Como o mdc(18, 5) = 1 e $1 \mid 48$, a equação dada tem solução. Usando o algoritmo da divisão, temos

$1 = 3 – 1.2$

$2 = 5 – 1.3$

$3 = 18 – 3.5$

Então $1 = 3 – 1.2 = 3 – 1.(5 – 1.3) = (-1).5 + 2.3 = (- 1).5 + 2.(18 – 3.5) = (- 7).5 + 2.18$

Portanto, $2.18 + (- 7).5 = 1$, multiplicando a equação por 48, temos

$$96.18 + (- 336).5 = 48$$

Logo, uma solução particular da equação é dada por $(x_0, y_0) = (96, - 336)$. Pelo teorema 4.2.2, a solução geral é

$$x = 96 + 5t$$
$$y = -336 - 18t, \quad \text{com } t \in \mathbb{Z}.$$

As soluções inteiras e positivas são encontradas escolhendo t de modo que sejam satisfeitas as desigualdades:

$x > 0$ e $y > 0$, então temos que $96 + 5t > 0$ e $-336 - 18t > 0$, ou seja, $t > -19{,}2$ e $t < -18{,}6$

o que implica que $t = -19$ e, portanto,

$$x = 96 + 5.(-19) = 1$$
$$y = -336 - 18.(-19) = 6$$

Contudo, o par de inteiros $x = 1$ e $y = 6$ é a única solução inteira e positiva da equação $18x + 5y = 48$.

4.3 Aplicações das Equações Diofantinas Lineares de Duas Variáveis

Veremos algumas aplicações das equações diofantinas lineares no cotidiano, para isto, dividiremos esta parte em duas seções, Na primeira vamos apresentar algumas situações-problema que os alunos do ensino médio encontram em alguns livros didáticos, provas de vestibulares, Enem e outros. Já na segunda seção, apresentaremos alguns softwares matemáticos para resolver e esboçar o gráfico dessas equações.

4.3.1 Situações-problema envolvendo equações diofantinas lineares

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

Solução. Sejam x o número de canetas e y o número de borrachas com x, y ∈ ℕ. Obtemos a equação 1,7x + 0,9y = 37,4. Multiplicando essa equação por 10, ela se torna 17x + 9y = 374. Como mdc(17, 9) = 1 e 1 | 374 a equação tem solução. Usando o Algoritmo de Euclides, vamos encontrar uma solução para a equação 17x + 9y = 374.

	1	1	8
17	9	8	1
8	1	0	

Verificando o algoritmo podemos escrever 1 = 9 – 1.8 e 8 = 17 – 1.9. Segue que 1 = 9 – 1.8 = 9 – 1.(17 – 1.9) = − 1.17 + 2.9. Multiplicando por 374, teremos

$$374 = -374.17 + 748.9.$$

Assim, temos a solução particular $(x_0, y_0) = (-374, 748)$. A solução geral é, então, dada por

$$x = -374 + 9t$$
$$y = 748 - 17t \quad , \quad \text{com } t \in \mathbb{Z}.$$

Como x > 0 e y > 0, temos −374 + 9t > 0 e 748 − 17t > 0, ou seja, 41,55 < t < 44, o que implica, t = 42 ou t = 43.

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

Problema 2. Quantas quadras de basquete e quantas quadras de vôlei são necessárias para que 80 alunos joguem simultaneamente?

Solução. As equipes de basquete e vôlei são compostas, respectivamente, de 5 e 6 jogadores. Como precisamos de duas equipes por quadra, modelamos o problema com

da seguinte equação diofantina: 12x +10y = 80 onde x e y representam, respectivamente, a quantidade de quadras de vôlei e basquete necessárias para acomodar os 80 jogadores. Simplificando a equação temos 6x + 5y = 40 e mdc(5,6) =1. Como 1 | 40 concluímos que o problema tem solução. Pelo algoritmo de Euclides, 40 = 40.6 − 40.5, então a solução geral é:

$$x = 40 + 5t$$
$$y = -\ 40 - 6t, \quad \text{com } t \in \mathbb{Z}.$$

Assim, como o número de quadras é um número natural, devemos restringir nossa resposta de modo que $x \geq 0$ e $y \geq 0$, logo $x = 40 + 5t \geq 0$ e $y = -40 - 6t \geq 0$, daí temos que $-8 \leq t \leq -7$.

Para $t = -8$, temos 0 quadras de vôlei e 8 quadras de basquete.

Para $t = -7$, temos 5 quadras de vôlei e 2 quadras de basquete.

Problema 3. Exprimir 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.

Solução. Sejam $7x$ e $11y$ esses dois números. Assim, temos $7x + 11y = 100$. Como mdc(7, 11) = 1 e 1 | 100, a equação tem solução. Usando o Algoritmo de Euclides, vamos encontrar uma solução particular para a equação $7x + 11y = 100$.

	1	1	1	3
11	7	4	3	1
4	3	1	0	

Verificando o algoritmo podemos escrever, $1 = 4 - 1.3$, $3 = 7 - 1.4$ e $4 = 11 - 1.7$.

Segue que $1 = 4 - 1.3 = 4 - 1.(7 - 1.4) = 2.4 - 1.7 = 2.(11 - 1.7) - 1.7 = 2.11 - 3.7$. Multiplicando por 100, temos $100 = -300.7 + 200.11$.

Isso implica que a solução particular é $(x_0, y_0) = (-300, 200)$. Então a solução geral é dada por $(x, y) = (-300 + 11t, 200 - 7t)$, com $t \in \mathbb{Z}$. Como $x > 0$ e $y > 0$, temos $-300 + 11t > 0$ e $200 - 7t > 0$, ou seja, $27 < t < 29$. Logo, $t = 28$, o que nos dá $(x, y) = (8, 4)$. Portanto, os números são 56 e 44.

Problema 4. O valor da entrada de um cinema é R$ 8,00 e da "meia" entrada é de R$ 5,00. Qual é o menor número de pessoas que podem assistir a uma sessão de maneira que a bilheteria seja de R$ 500,00?

Solução. Vamos iniciar identificando as variáveis do problema; seja x o número de pessoas que pagarão o valor integral da entrada, e y o número de pessoas que pagarão o valor da meia entrada. Assim, a equação representativa é $8x + 5y = 500$

Vamos encontrar o mdc(8, 5) pelo algoritmo de Euclides:

	1	1	1	2
8	5	3	2	1
3	2	1	0	

Como o mdc(8, 5) = 1, a equação apresenta solução, pois $1 \mid 500$.

Verificando o algoritmo podemos escrever, $1 = 3 - 1.2$, $2 = 5 - 1.3$ e $3 = 8 - 1.5$. Segue que $1 = 3 - 1.(5 - 1.3) = -5 + 2.3 = -5 + 2.(8 - 1.5) = 2.8 + (-3).5$.

Multiplicando a equação por 500, fica:

$$1000.8 + (-1500).5 = 500$$

Isso implica que a solução particular é $(x_0, y_0) = (1000, -1500)$. Logo, a solução geral é dada por

$x = 1000 + 5t$

$y = -1500 - 8t$, com $t \in \mathbb{Z}$.

O problema requer soluções inteiras e positivas, que serão determinadas escolhendo t de modo que sejam satisfeitas as seguintes desigualdades, $x > 0$ e $y > 0$, então temos que $1000 + 5t > 0$ e $- 1500 - 8t > 0$, ou seja, $- 200 < t < - 187,5$

Contudo, para que encontremos o menor número de pessoas, devemos utilizar o maior valor inteiro de t, que é $t = - 188$. Assim, obtemos os valores:

$$x = 1000 + 5.(– 188) = 60 \quad \text{e} \quad y = – \ 1500 – 8.(– 188) = 4.$$

Sendo assim, para a bilheteria ser de R$ 500,00 com o menor número de pessoas possíveis, devem-se ter 60 pessoas que irão pagar R$ 8,00 cada e 4 pessoas que irão pagar R$ 5,00 cada. Portanto, nessas condições o menor número de pessoas será 64.

Problema 5. Um teatro vende ingressos e cobra R$ 18,00 por adulto e R$ 7,50 por criança. Numa noite, arrecada-se R$ 900,00. Quantos adultos e crianças assistiram ao espetáculo, sabendo-se que eram mais adultos do que crianças?

Solução. Sejam x o número de crianças e y o número de adultos que assistiram. Temos que resolver a equação diofantina $7,5.x + 18y = 900$, com a seguinte condição $y > x \geq 0$. Multiplicando a equação por 2, temos $15.x + 36.y = 1800$. Como $mdc(15, 36) = 3$ e $3 \mid 1800$ a equação admite solução. Simplificando a equação, temos $5x + 12y = 600$. Observando que $(x, y) = (120, 0)$ é uma solução da equação, então a solução geral é

$$\begin{aligned} x &= 120 + 12t \\ y &= - 5t \end{aligned} \quad , \quad \text{com } t \in \mathbb{Z}.$$

De $y > x \geq 0$ decorre $- 5t > 120 + 12t \geq 0$ e daí, $- 7,05 = - \frac{120}{17} > t \geq - \frac{120}{12} = - 10$, ou seja, $- 10 \leq t < - 7,05$, o que dá $t \in \{- 10, - 9, - 8\}$.

As três possíveis soluções são:

$$\begin{cases} x = 0 \\ y = 50 \end{cases} \text{ ou } \begin{cases} x = 12 \\ y = 45 \end{cases} \text{ ou } \begin{cases} x = 24 \\ y = 40 \end{cases}$$

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

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

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

Como mdc(8, 15) = 1 e 1 | 7 a equação tem solução. Usando o Algoritmo de Euclides, vamos determinar uma solução particular para a equação 8x − 15y = 7.

	1	1	7
15	8	7	1
7	1	0	

Verificando o algoritmo podemos escrever 1 = 8 – 1.7 e 7 = 15 – 1.8.

Segue-se que, 1 = 8 – 1.7 = 8 – 1.(15 – 1.8) = 2.8 – 1.15. Multiplicando por 7, temos 14.8 + 7.(- 15) = 7.

Isso nos dá a solução particular $(x_0, y_0) = (14, 7)$. A solução geral é, então, dada por (x, y) = (14 − 15t, 7 − 8t), com $t \in \mathbb{Z}$. Como x > 0 e y > 0, temos 14 − 15t > 0 e 7 − 8t > 0, ou seja, $t < \frac{14}{15}$ e $t < \frac{7}{8}$.

Assim, o menor valor de n será obtido ao tomar o menor valor de x e y que satisfaça a equação 8x − 15y = 7 e, isso acontece quando t = 0. Isso implica que (x, y) = (14, 7) e, portanto, n = 118.

Problema 7. Encontrar todos os números naturais N menores do que 10000 tais que, o resto da divisão de N por 37 é 9 e o resto da divisão de N por 52 é 15.

Solução. Pelo algoritmo da divisão, existem x e y inteiros positivos, tais que N = 37x + 9 e N = 52y + 15, segue que:

$$37x + 9 = 52y + 15 \Longrightarrow 37x - 52y = 6$$

Como mdc(37, 52) = 1 e 1 | 6, a equação admite solução inteira. Pelo algoritmo de Euclides, temos:

	1	2	2	7
52	37	15	7	1
15	7	1	0	

Observando o algoritmo de Euclides podemos escrever 1 = 15 – 2.7, 7 = 37 – 2.15 e 15 = 52 – 1.37. Daí, 1 = 15 – 2.7 = 15 – 2.(37 – 2.15) = - 2.37 + 5.15 = – 2.37 + 5.(52 – 1.37) = 5.52 – 7.37, segue que – 7.37 – 5.(– 52) = 1. Multiplicando por 6, segue que (- 42).37 - 30.(- 52) = 6

Temos que a solução particular é $(x_0, y_0) = (- 42, - 30)$. A solução geral é

$x = - 42 - 52t$

$y = - 30 - 37t$, com $t \in \mathbb{Z}$.

Para encontrar as soluções da equação nos naturais, basta determinar t de modo que sejam satisfeitas as desigualdades: $x \geq 0$ e $y \geq 0$, segue que $– 42 – 52t \geq 0$ e $– 30 – 37t \geq 0$, isto é, $t \leq - \frac{21}{26}$ e $t \leq - \frac{30}{37}$.

O que implica que se $t \leq - 1$, temos que a equação $37x – 52y = 6$ possui infinitas soluções no conjunto dos números naturais.

Retomando a pergunta inicial, os números N que estamos procurando são dados, por:

$$N = 37x + 9 = 37.(- 42 - 52t) + 9 = - 1545 - 1924t.$$

Para que $N < 10000$, teremos:

$$- 1545 - 1924t < 10000 \Leftrightarrow t > - \frac{11545}{1924} \approx - 6{,}001$$

Assim, se $t \geq -6$, a equação $N = -1545 - 1924t$ nos fornece um número $N > 10000$. Agora para que o número N seja natural e menor do que 10000, devemos ter $-6 \leq t \leq -1$, o que implica em $t \in \{-6, -5, -4, -3, -2, -1\}$.

Contudo, os seis possíveis valores naturais para N são: 379, 2303, 4227, 6151, 8075 e 9999.

Problema 8. Se o custo de uma postagem é de 83 centavos e os valores dos selos são de 6 e 15 centavos, como podemos combinar os selos para fazer essa postagem?

Solução. Sejam x e y as quantidades de selos de 6 centavos e de 15 centavos respectivamente, então a equação deste problema é $6x + 15y = 83$. Observe que o $mdc(6, 15) = 3$ e $3 \nmid 83$, logo a equação diofantina não possui soluções inteiras, contudo o problema de postagem não tem solução.

Problema 9. Um fazendeiro deseja comprar filhotes de pato e de galinha, gastando um total de R$ 1.770,00. Um filhote de pato custa R$ 31,00 e um de galinha custa R$ 21,00. Quantos de cada um dos dois tipos o fazendeiro poderá comprar?

Solução. Sejam x o número de patos comprados e y o número de galinhas. Assim, podemos modelar o problema do seguinte modo, $31x + 21y = 1770$. Observe que o $mdc(31, 21) = 1$ e que $1 \mid 1770$. Assim, a equação tem solução. Vamos encontrar uma solução particular. Para isso, usamos o Algoritmo da Divisão:

$$31 = 1.21 + 10;$$
$$21 = 2.10 + 1;$$
$$1 = 21 + (-2).10 = 21 + (-2).[31 + (-1).21] = 3.21 + (-2).31.$$

Multiplicando ambos os lados por 1.770, obtemos:

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

Portanto, uma solução particular é $x_0 = -3540$ e $y_0 = 5310$. A solução geral da equação é dada por:

$x = -3540 + 21t$

$y = 5310 - 31t$, com $t \in \mathbb{Z}$.

Observe que estamos interessados somente nas soluções positivas ou nulas, pois representam as quantidades de animais. Assim, temos que impor as seguintes condições:

$$-3540 + 21t \geq 0 \text{ e } 5310 - 31t \geq 0.$$

Portanto, $21t \geq 3540$ e $31t \leq 5310$, que é o mesmo que: $t \geq 168{,}57$ e $t \leq 171{,}29$. Assim, como t é um número inteiro, temos que $169 \leq t \leq 171$. Desse modo, as soluções são:

Para $t = 169$, temos $x = -3540 + 21.169 = 9$ e $y = 5310 - 31.169 = 71$;
para $t = 170$, temos $x = -3540 + 21.170 = 30$ e $y = 5310 - 31.170 = 40$;
para $t = 171$, temos $x = -3540 + 21.171 = 51$ e $y = 5310 - 31.171 = 9$.

Contudo, essas soluções nos dizem que o fazendeiro tem três alternativas para comprar: 9 patos e 71 galinhas, ou 30 patos e 40 galinhas, ou 51 patos e 9 galinhas.

Problema 10. Um parque de diversões cobra R$ 1,00 a entrada de crianças e R$ 3,00 a entrada de adultos. Para que a arrecadação de um dia seja R$ 200,00; qual o menor número de pessoas, entre adultos e crianças, que poderiam estar no parque nesse dia? Quantas crianças? Quantos adultos?

Solução. Considerando o número de crianças por x e o número de adultos por y, de acordo com o enunciado temos a equação $1x + 3y = 200$. Agora, para encontrar a solução desse problema basta resolver a equação diofantina gerada. Como o $mdc(1, 3) = 1$ e $1 \mid 200$ a equação possui solução, logo, $1 = 1.(-2) + 3.1$ então $200 = 1.(-400) + 3.200$. Assim, todos os possíveis valores para x e y se apresentam da seguinte forma:

$$x = -400 + 3t \text{ e } y = 200 - t \text{ com } t \in \mathbb{Z}.$$

Como x e y representam números de pessoas, eles devem ser números naturais, sendo assim, temos:

$$-400 + 3t \geq 0 \text{ e } 200 - t \geq 0 \text{ que geram o intervalo, } 134 \leq t \leq 200.$$

Contudo, devemos encontrar o menor número de pessoas, e para que isso aconteça t deve assumir o menor valor no intervalo, isto é, 134. Portanto, temos que:

$$x = -400 + 3.134 = 2 \text{ e } y = 200 - 134 = 66.$$

Então, o menor número de pessoas que esteve no parque nesse dia foi 68 pessoas, sendo 2 crianças e 66 adultos.

4.3.2 Utilizando o Maple e o Winplot

Vamos utilizar o Maple para solucionar algumas equações diofantinas lineares e em seguida iremos também fazer a construção de alguns gráficos utilizando o Winplot e iremos verificar as suas soluções inteiras nestas construções geométricas. Veremos que o uso desses programas matemáticos computacionais facilitará na melhor compreensão dos problemas.

Exemplo 1. João pediu a Pedro que multiplicasse o dia de seu aniversário por 12 e o mês do aniversário por 31 e somasse os resultados. Pedro obteve 368. Qual é o produto do dia do aniversário de Pedro pelo mês de seu nascimento?

Solução. Sejam x e y o dia e mês, respectivamente, do aniversário de Pedro. Então temos a equação 12x + 31y = 368. Utilizando o Maple temos:

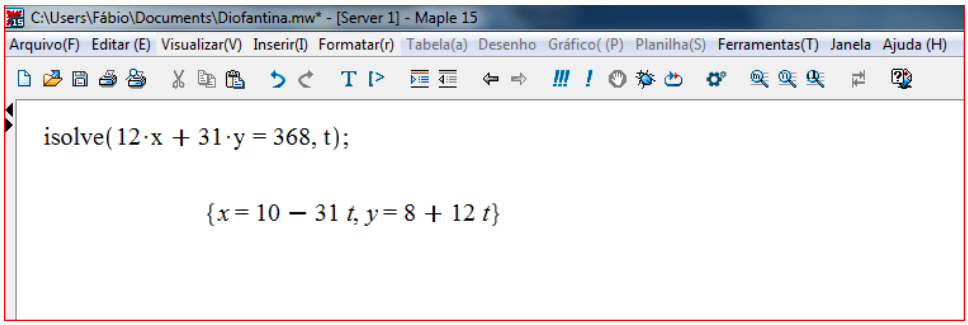

Figura 9. Soluções da equação diofantina com o auxílio do Maple.

É fácil notar que o único valor do parâmetro que satisfaz o problema é t = 0, pois sabemos que $1 \leq x \leq 31$ e $1 \leq y \leq 12$. Então Pedro nasceu no dia 10 de agosto e o produto é 10.8 = 80.

Exemplo 2. Dois irmãos, João e José, pescaram em uma manhã "x" e "y" peixes, respectivamente. Sabendo que 3x + 4y = 61, determine as possíveis quantidades de peixes que eles conseguiram juntos?

Solução. Ora, utilizando o software Maple, vamos determinar todas as soluções inteiras. Para que isso ocorra utilizaremos o comando "isolve" que nos fornece as soluções inteiras da equação em função de um parâmetro, sendo este um número inteiro.
Assim ao abrir o Maple digitamos o comando "isolve" e em seguida digitamos entre parênteses a equação diofantina linear seguida de uma vírgula para colocarmos o parâmetro desejado, encerrando o comando com ponto e vírgula. Veja:

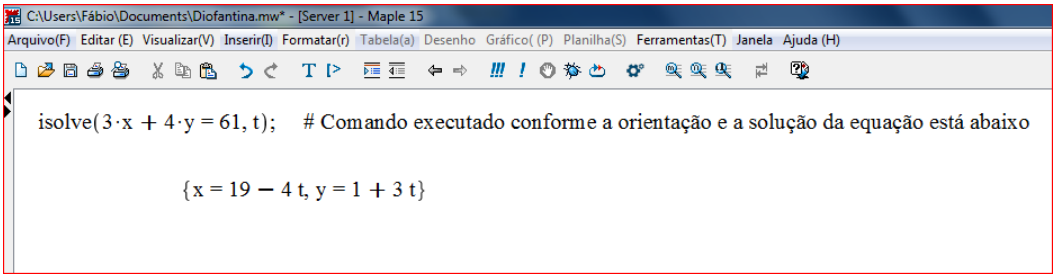

Figura 10. Utilizando o Maple para encontrar as soluções de uma equação diofantina.

Agora, basta determinar t de modo que sejam satisfeitas as desigualdades:

x > 0 e y > 0, segue que 19 – 4t > 0 e 1 + 3t > 0, ou seja,

$$t < \frac{19}{4} = 4{,}75 \quad \text{e} \quad t > -\frac{1}{3} \approx -0{,}33.$$

O que acarreta em $0 \leq t \leq 4$ com $t \in \mathbb{Z}$, logo $t \in \{0, 1, 2, 3, 4\}$, assim existem 5 possibilidades para a pescaria, e a quantidade de peixes que eles conseguiram juntos foi:

Para t = 0, temos que x = 19 e y = 1 e juntos conseguiram 20 peixes ao todo.
Para t = 1, temos que x = 15 e y = 4 e juntos conseguiram 19 peixes ao todo.

Para t = 2, temos que x = 11 e y = 7 e juntos conseguiram 18 peixes ao todo.

Para t = 3, temos que x = 7 e y = 10 e juntos conseguiram 17 peixes ao todo.

Para t = 4, temos que x = 3 e y = 13 e juntos conseguiram 16 peixes ao todo.

Exemplo 3. Represente graficamente as soluções inteiras e positivas da equação 20x + 50y = 510 com a ajuda do Winplot.

Solução. No programa Winplot escolhemos a opção plotar gráfico de "2ª dimensão".

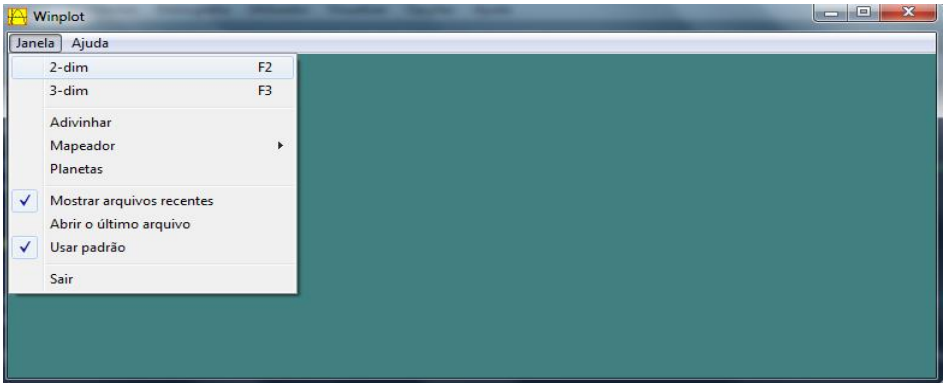

Figura 11. Tela inicial do Winplot.

Na próxima janela selecione "Equação" e depois "Reta".

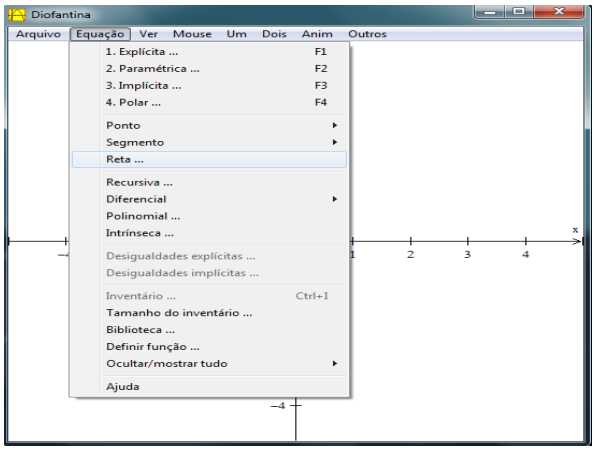

Figura 12. Instruções para a construção do gráfico de uma reta.

Agora para plotar o gráfico da equação ax + by = c, basta digitar seus coeficientes.

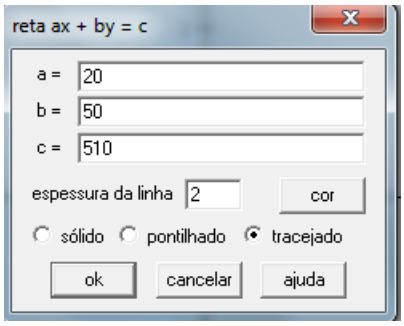

Figura 13. Inserindo os coeficientes de uma equação diofantina que representa uma reta no plano.

Agora vamos visualizar geometricamente o conjunto-solução da equação linear 20x + 50y = 510.

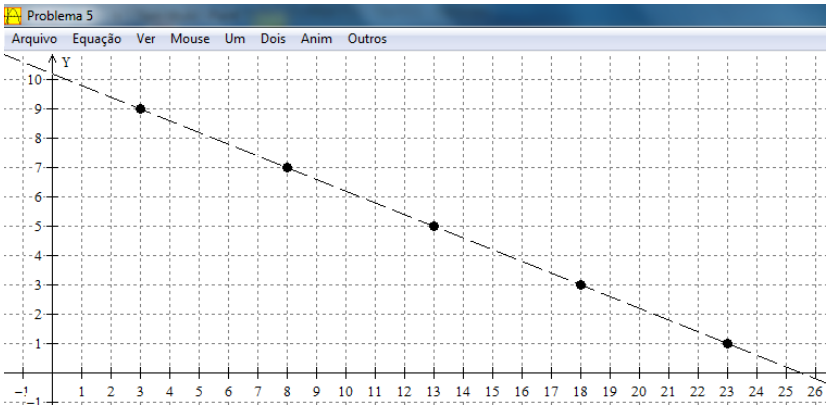

Figura 14. Representação geométrica das soluções inteiras da equação diofantina.

Vemos que a interpretação geométrica desse problema é um conjunto de pontos alinhados que pertencem à reta de equação 20x + 50y = 510, conforme mostra o gráfico acima. Então a partir da solução geral obtida com o Maple, podemos atribuir valores inteiros para t e no Winplot inserirmos alguns pontos com coordenadas inteiras no gráfico que satisfazem a equação. Assim, o exemplo possui apenas 5 soluções com coordenadas inteiras positivas.

Exemplo 4. Ao entrar num bosque, alguns viajantes avistam 37 montes de maçãs. Após serem retiradas 17 frutas, o restante foi dividido igualmente entre 79 pessoas. Qual pode ter sido a menor parte recebida de cada pessoa? Utilize o programa Maple e em seguida represente graficamente as soluções inteiras no programa Winplot.

Solução. Ora, se cada um dos 37 montes tem x maçãs e após serem retiradas 17 maçãs sobraram-nos k maçãs, temos a equação 37x – 17 = k. Como o restante das maçãs será dividido igualmente entre 79 pessoas, temos que k é múltiplo de 79 e assim sendo, é da forma k = 79y, com y ∈ ℤ, onde y é a parte inteira que cabe a cada pessoa. Assim, substituindo temos a seguinte equação diofantina, 37x – 79y = 17.

Solucionado no Maple temos:

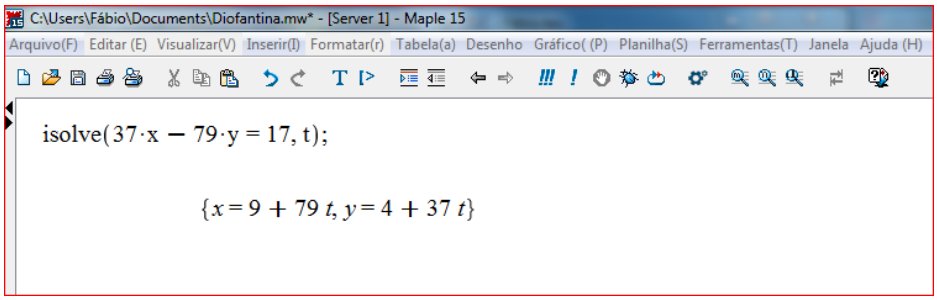

Figura 15. Soluções da equação diofantina do exemplo 4 obtidas com o Maple.

Para que venhamos repartir a menor quantidade possível para cada pessoa, basta, contudo fazer t = 0 na equação y = 4 + 37t. Assim, temos que y = 4, isto é, cada uma das pessoas receberá 4 maçãs.

Visualizando o gráfico da equação diofantina linear 37x – 79y = 17, temos:

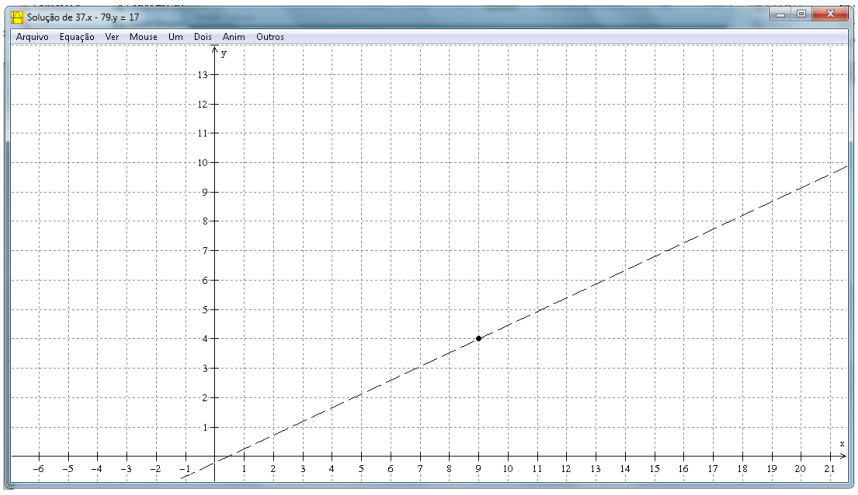

Figura 16. Representação geométrica da única solução que apresenta as menores coordenadas inteiras.

A equação 37x – 79y = 17 possui infinitas soluções, contudo o único par com coordenadas inteiras que nos fornece a menor quantidade de maçãs que podem ser

repartidas igualmente entre as 79 pessoas é (9, 4). Ou seja, cada monte contém 9 maçãs e ao serem retiradas 17 dessas maçãs, cada uma das 79 pessoas ficará com 4 maçãs.

4.4 Utilizando congruência linear para resolver equações diofantinas

Sejam a, b, n $\in \mathbb{Z}$, com n > 0, então chamaremos de congruência linear toda congruência do tipo ax ≡ b mod n. Uma congruência linear ax ≡ b mod n possui uma solução x_0 se n $\mid (a.x_0$ - b), ou seja, se existe um y $\in \mathbb{Z}$, tal que $a.x_0$ - b = n.y, isto é, $a.x_0$ - n.y = b. Logo, as soluções de tais congruências também são soluções de uma equação diofantina. A recíproca dessas implicações é imediata, confirmando o conceito de equação diofantina equivalente a uma congruência linear.

Teorema 4.4.1. Sejam a, b e n inteiros, com n > 1 e d = mdc(a, n).
I) A congruência a.x ≡ b mod n tem solução se, e só se, d $\mid$ b.
II) Se d $\mid$ b, existem exatamente d soluções distintas módulo n, com representantes x_0, $x_0 + \frac{n}{d}$, ..., $x_0 + (d-1).\frac{n}{d}$, onde x_0 é uma solução particular qualquer de a.x ≡ b mod n.

Demonstração.

I) A congruência a.x ≡ b mod n admite solução em x se, e só se, a equação diofantina a.x + n.y = b admite solução em x e y e isto é equivalente, pelo teorema 4.2.1, à condição d $\mid$ b.

II) Seja x_0 uma solução qualquer da congruência a.x ≡ b mod n, assim existe y_0 tal que (x_0, y_0) é uma solução particular da equação diofantina a.x + n.y = b. Pelo teorema 4.2.2, temos que toda solução da equação diofantina a.x + n.y = b é, para algum t $\in \mathbb{Z}$, da forma

$$x = x_0 + t.\frac{n}{d}, \quad y = y_0 - t.\frac{a}{d}.$$

Logo, toda solução da congruência a.x ≡ b mod n é da forma

$$x = x_0 + t.\frac{n}{d}, \quad t \in \mathbb{Z}.$$

As seguintes soluções de $a.x \equiv b \bmod n$, são

$$x_0, x_0 + \frac{n}{d}, \ldots, x_0 + (d-1).\frac{n}{d}, \qquad (*)$$

são claramente duas a duas incongruentes módulo n. Por outro lado, se $x = x_0 + t.\frac{n}{d}$ é uma solução qualquer de $a.x \equiv b \bmod n$, pondo $t = d.q + r$ com $0 \leq r < d$, temos que

$$x \equiv x_0 + t.\frac{n}{d} \equiv x_0 + r.\frac{n}{d} \bmod n.$$

Então, x é congruente módulo n a uma e somente uma das soluções em (*).

■

Corolário 4.4.2. Sejam a, $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então:

a) se o mdc(a, n) = 1 então existe $c \in \mathbb{Z}$, tal que $ac \equiv 1 \bmod n$;

b) (lei do corte) se o mdc(a, n) = 1, $c \in \mathbb{Z}$ e $ac \equiv ab \bmod n$, então $b \equiv c \bmod n$.

Demonstração. Para o item a) basta aplicar o teorema 4.4.1 à congruência $ax \equiv 1 \bmod n$. Para o item b) basta "multiplicar a igualdade $ac \equiv ab \bmod n$ por c" em que c é tal que $ac \equiv 1 \bmod n$. ■

Exemplo 1. Determine a solução geral da equação diofantina 12x + 25y = 331 por congruência linear.

Solução. Como o mdc(12, 25) = 1 e $1 \mid 331$, então a equação diofantina possui solução. Segue que 12x – 331 = 25.(- y), daí $12x \equiv 331 \bmod 25$, como $331 \equiv 12.13 \bmod 25$ temos que $12x \equiv 12.13 \bmod 25$, por fim, $x \equiv 13 \bmod 25$. Portanto, $x_0 = 13$ é uma solução particular da equação diofantina linear. Substituindo este valor na equação diofantina, obtemos, $y_0 = 7$. Contudo, a solução geral da equação é

$$x = 13 + 25t$$
$$y = 7 - 12t \quad , \quad \text{com } t \in \mathbb{Z}.$$

Exemplo 2. Determine a solução geral da equação diofantina $7x + 6y = 9$ por congruência linear.

Solução. Veja que o $mdc(7, 6) = 1$ e $1 \mid 9$, assim a equação diofantina admite solução. Segue que $7x - 9 = 6.(-y)$, daí $7x \equiv 9 \bmod 6$, como $9 \equiv 7.3 \bmod 6$, temos que $7x \equiv 7.3 \bmod 6$, contudo, $x \equiv 3 \bmod 6$. Logo, $x_0 = 3$ é uma solução particular da equação diofantina linear. Substituindo este valor na equação diofantina, obtemos, $y_0 = -2$. Portanto, a solução geral da equação é

$$x = 3 + 6t$$
$$y = -2 - 7t, \quad \text{com } t \in \mathbb{Z}.$$

Teorema chinês do resto

Problemas antigos da astronomia, ligados aos movimentos periódicos dos corpos celestes, deram origem ao hoje conhecido como Teorema Chinês de Restos. O nome veio do fato dos problemas terem sido originários dos antigos matemáticos chineses. Há registros de problemas relacionados ao tema propostos no século terceiro depois de Cristo. O chamado Teorema Chinês dos Restos do século V dá um método sistemático de resolução de sistemas de congruências do tipo $a\,x \equiv b \bmod n$. Aparentemente a ideia surgiu com a necessidade de contar o número de soldados numa parada. Suponhamos que sabemos que o número de soldados é no máximo 1000. Mandamos ordenar os soldados em filas de 7 e depois em filas de 11 e depois em filas de 13 (o que é mais simples do que contar os soldados) e contamos o número de soldados que sobraram em cada um dos casos. Suponhamos que esses números foram 6, 5 e 3. Estamos assim diante do sistema

$$\begin{cases} x \equiv 6 \bmod 7 \\ x \equiv 5 \bmod 11 \\ x \equiv 3 \bmod 13 \end{cases}$$

cuja solução é $x \equiv 874 \bmod 1001$, onde $1001 = 7.11.13$. Deste modo existe $k \in \mathbb{Z}$ tal que o número de soldados é $874 + 1001k$. Como o número pretendido é no máximo 1000 podemos concluir que existem 874 soldados na parada.

O teorema chinês dos restos que veremos a seguir nos diz que, se conseguirmos encontrar (por algum método) uma solução do sistema então passaremos a conhecer todas as suas soluções.

Teorema (Teorema Chinês dos Restos) 4.4.3. Sejam n_1, n_2, ..., n_k naturais maiores que 1 e dois a dois primos entre si. Dados inteiros quaisquer a_1, a_2, ..., a_k, o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ \quad\quad ... \\ x \equiv a_k \bmod n_k \end{cases} \qquad (*)$$

admite uma única solução, módulo n_1, n_2, ..., n_k. De outro modo, existe um único $0 \leq y < n_1 n_2 ... n_k$ tal que $x \in \mathbb{Z}$ satisfaz o sistema acima se, e só se, $x \equiv y \bmod n_1 n_2 ... n_k$.

Demonstração. Veja que se x_1 e x_2 forem duas soluções quaisquer do sistema (*), então $x_1 \equiv a_i \equiv x_2 \bmod n_i$, para todo $1 \leq i \leq k$.

Mas, como n_1, n_2, ..., n_k são dois a dois primos entre si, segue da proposição 2.10.1 que $x_1 \equiv x_2 \bmod n_1 n_2 ... n_k$.

Logo, se o sistema (*) tiver uma solução, esta será única, módulo $n_1 n_2 ... n_k$. Para a existência de solução defina, para $1 \leq j \leq k$,

$$y_j = \prod_{\substack{1 \leq i \leq k \\ i \neq j}} n_i ,$$

de sorte que $mdc(y_j, n_j) = 1$. Seja b_j o inverso de y_j módulo n_j e $x = \sum_{j=1}^{k} a_j b_j y_j$. Fixado $1 \leq t \leq k$, temos que $n_t \mid y_j$ para $j \neq t$ e, daí, módulo n_t temos que

$$x \equiv a_t b_t y_t \equiv a_t . 1 \equiv a_t \bmod n_t .$$

■

Exemplo 1. Seja M um número natural e sejam r_7, r_{11} e r_{13} os seus restos pela divisão por 7, 11 e 13, respectivamente. Tem-se então que $M \equiv 715 . r_7 + 364 . r_{11} + 924 . r_{13} \bmod 1001$.

Solução. De fato, temos N = 7.11.13 = 1001, N_1 = 143, N_2 = 91 e N_3 = 77. Por outro lado, y_1 = 5, y_2 = 4 e y_3 = 12 são soluções de 143.Y ≡ 1 mod 7, 91.Y ≡ 1 mod 11 e 77.Y ≡ 1 mod 13, respectivamente. Assim, o sistema

$$X \equiv r_7 \bmod 7$$
$$X \equiv r_{11} \bmod 11$$
$$X \equiv r_{13} \bmod 13$$

tem por solução $715.r_7 + 364.\ r_{11} + 924.\ r_{13} \bmod 1001$.

Este exemplo serve para a seguinte brincadeira em sala de aula: O professor pede a um aluno que escolha um número menor do que 1001 e que diga os restos r_7, r_{11} e r_{13} desse número quando dividido por 7, 11 e 13, respectivamente. Sem nenhuma outra informação, o professor é capaz de adivinhar o número escolhido pelo aluno. De fato, o número que o aluno escolheu é o resto da divisão de $715.r_7 + 364.\ r_{11} + 924.\ r_{13}$ por 1001.

Exemplo 2. Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7?

Solução. Temos que N = 3.5.7 = 105, N_1 = 35, N_2 = 21 e N_3 = 15. Por outro lado, y_1 = 2, y_2 = 21 e y_3 = 1 são soluções, respectivamente, das congruências 35.Y ≡ 1 mod 3, 21.Y ≡ 1 mod 5 e 15.Y ≡ 1 mod 7. Logo, uma solução módulo N = 105 é dada por
$x = N_1y_1r_1 + N_2y_2r_2 + N_3y_3r_3 = 233$.

Como 233 ≡ 23 mod 105, segue-se que 23 é a solução minimal única módulo 105 e qualquer outra solução é da forma 23 + 105k, com k ∈ ℕ.

Exemplo 3. Mostre que, dado n > 1 inteiro, existem n naturais consecutivos, todos compostos.

Solução. Escolha n primos distintos p_1 , p_2 , ..., p_n e considere o sistema de congruências

$$\begin{cases} x \equiv -1 \bmod {p_1}^2 \\ x \equiv -2 \bmod {p_2}^2 \\ \quad\quad ... \\ x \equiv -n \bmod {p_n}^2 \end{cases}$$

Como p_1, p_2, ..., p_n são dois a dois primos entre si, o teorema chinês dos restos garante a existência de $m \in \mathbb{N}$ satisfazendo o sistema acima. Logo, ${p_i}^2 \mid (m + i)$ para $1 \leq i \leq n$, de maneira que m + 1, m + 2,..., m + n são naturais consecutivos e compostos.

Exemplo 4. Uma senhora transportava um cesto de ovos. Assustada por um cavalo que galopava perto dela, deixou cair o cesto e todos os ovos se partiram. Quando lhe perguntaram quantos ovos tivera o cesto, respondeu dizendo que é muito fraca em aritmética, mas lembra-se de ter contado os ovos de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, e tivera sobra de 1, 2, 3, e 4 ovos, respectivamente. Ache a menor quantidade de ovos que o cesto inicialmente poderia ter.

Solução. Seja x a quantidade de ovos que estavam inicialmente no cesto. Então podemos escrever:

$x \equiv 1 \bmod 2$
$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 4$
$x \equiv 4 \bmod 5$

Na notação do Teorema Chinês de Restos, temos:
$r_1 = 1$, $r_2 = 2$, $r_3 = 3$, $r_4 = 4$;
$n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $n_4 = 5$;

Não podemos aplicar diretamente o Teorema Chinês de Restos, pois mdc(n_1, n_3) = mdc(2, 4) = 2. Para resolver o problema, inicialmente, trabalhamos somente com as congruências lineares

$x \equiv 1 \bmod 2$

$x \equiv 2 \bmod 3$

$x \equiv 4 \bmod 5$

Agora, na notação do Teorema Chinês de Restos o sistema acima tem os seguintes dados:

$r_1 = 1$, $r_2 = 2$, $r_3 = 4$;

$n_1 = 2$, $n_2 = 3$, $n_3 = 5$;

$N = 2.3.5 = 30$,

$N_1 = 3.5 = 15$, $N_2 = 2.5 = 10$, $N_3 = 2.3 = 6$.

As congruências $N_1x_1 \equiv 1 \bmod 2$, $N_2x_2 \equiv 1 \bmod 3$ e $N_3x_3 \equiv 1 \bmod 5$, são:

$15.x_1 \equiv 1 \bmod 2$, que é o mesmo que $1.x_1 \equiv 1 \bmod 2$, cuja solução é $x_1 \equiv 1 \bmod 2$;

$10.x_2 \equiv 1 \bmod 3$, que é o mesmo que $1.x_2 \equiv 1 \bmod 3$, cuja solução é $x_2 \equiv 1 \bmod 3$;

$6.x_3 \equiv 1 \bmod 5$, que é o mesmo que $1.x_3 \equiv 1 \bmod 5$, cuja solução é $x_3 \equiv 1 \bmod 5$.

Logo, a solução do sistema é dada por

$$X = 1.15.1 + 2.10.1 + 4.6.1 \equiv 59 \bmod 30 \equiv 29 \bmod 30.$$

Contudo, X = 29 + 30k, onde k é um número inteiro. Agora, substituímos X na congruência $x \equiv 3 \bmod 4$. Assim, $29 + 30k \equiv 3 \bmod 4$, que é o mesmo que $1 + 2k \equiv 3 \bmod 4$. Ou ainda, $3 + 1 + 2k \equiv 3 + 3 \bmod 4$, que nos leva para $2k \equiv 2 \bmod 4$, que é equivalente a dizer $2k – 2 = 4t$, onde t é um inteiro, isto é, $2.(k – 1) = 4t$. Portanto, k tem de ser um número ímpar, $k = 2s + 1$, onde s é um número inteiro. Logo, $X = 29 + 30.(2s$

+1) = 59 + 60s. Assim, o número mínimo de ovos que a cesta inicialmente poderia conter é 59.

Agora iremos mostrar como encontrar uma solução particular e a solução geral de equações diofantinas lineares com mais de duas variáveis.

4.5 Equações Diofantinas Lineares com n variáveis

Primeiramente veremos o caso em que n = 3. Seja a equação $a_1x + a_2y + a_3z = b$, onde cada a_i, com i = 1, 2, 3, sejam inteiros não nulos simultaneamente. A mesma argumentação usada para provar o Teorema 4.2.1 garante que essa equação admite soluções se, $d = mdc(a_1, a_2, a_3)$ divide b. Se $d_1 = mdc(a_1, a_2)$, então existem $k_1, k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d = mdc(d_1, a_3)$, então existem $k, z_0 \in \mathbb{Z}$ de maneira que $d = d_1k + a_3z_0$. Assim,

$$d = (a_1k_1 + a_2k_2)k + a_3z_0 = a_1(k_1k) + a_2(k_2k) + a_3z_0.$$

Fazendo $k_1k = x_0$ e $k_2k = y_0$, então $a_1x_0 + a_2y_0 + a_3z_0 = d$.

Portanto, se $a_1x + a_2y + a_3z = b$ admite solução e como b = dq, para algum $q \in \mathbb{Z}$, então, $a_1(x_0q) + a_2(y_0q) + a_3(z_0q) = dq = b$, o que mostra que (x_0q, y_0q, z_0q) é uma de suas soluções particulares.

Para encontrar a solução geral de uma equação diofantina linear de três variáveis, utilizaremos os seguintes passos:

I) Por meio de uma substituição, reduziremos a equação original a uma equação com duas variáveis e resolveremos essa equação.

II) A partir dessa solução, retornaremos na substituição feita inicialmente e resolveremos mais uma equação com duas variáveis. Obtendo assim a solução geral.

Reduzindo a equação $a_1x + a_2y + a_3z = b$ para duas variáveis, considerando $a_1x + a_2y = p$, temos $p + a_3z = b$ que possui solução, pois $mdc(1, a_3) = 1$ e $1 \mid b$, e tem como solução geral,

$$S_1 = \left\{\left(p_0 + \frac{a_3}{d_1}t_1, z_0 - \frac{1}{d_1}t_1\right) / \ t_1 \in \mathbb{Z}\right\},$$

e como $mdc(1, a_3) = 1$, segue que

$$S_1 = \{(p_0 + a_3t_1, z_0 - t_1) / \ t_1 \in \mathbb{Z}\}.$$

Daí, a partir dessa solução geral encontrada, escolheremos um valor conveniente para t_1, que satisfaça, $d_2 = mdc(a_1, a_2) \mid (p_0 + a_3t_1)$ e daremos continuidade para encontrar a solução geral da equação $a_1x + a_2y = p = p_0 + a_3t_1$, e a partir dessa, a solução geral da equação original. Agora, basta analisar a equação gerada pela substituição feita, $a_1x + a_2y = p = p_0 + a_3t_1$ que tem com solução geral,

$$S_2 = \left\{\left(x_0 + \frac{a_2}{d_2}t_2, y_0 - \frac{a_1}{d_2}t_2\right) / \ t_2 \in \mathbb{Z}\right\}.$$

Logo, a solução geral da equação original é

$$S = \left\{\left(x_0 + \frac{a_2}{d_2}t_2, y_0 - \frac{a_1}{d_2}t_2, z_0 - t_1\right) / \ t_1, t_2 \in \mathbb{Z}\right\},$$

que é gerada a partir de um valor apropriado, atribuído ao parâmetro t_1 no processo de descoberta dessa solução. Com isso, podemos afirmar que, a cada t_1 apropriado será gerado um novo conjunto solução.

Agora veremos como determinar uma solução particular e a solução geral da equação diofantina linear para n variáveis. Seja a equação $a_1x_1 + a_2x_2 + ... + a_nx_n = b$, onde cada a_i, com i = 1, 2,..., n, sejam inteiros não nulos simultaneamente. A mesma argumentação usada para provar o Teorema 4.2.1 garante que essa equação admite soluções se, $d = mdc(a_1, a_2,..., a_n)$ divide b. Se $d_1 = mdc(a_1, a_2)$, então existem $k_1, k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d_2 = mdc(d_1, a_3)$, então existem $k_3, k_4 \in \mathbb{Z}$

de maneira que $d_2 = d_1k_3 + a_3k_4$. Procedendo de forma análoga n - 1 vezes, chegaremos em d = mdc(d_{n-1}, a_n), então, $a_1(x_{1_0}q) + a_2(x_{2_0}q) + a_3(x_{3_0}q) + ... + a_{n-1}(x_{(n-1)_0}q) + a_n(x_{n_0}q) = dq = b$ para algum $q \in \mathbb{Z}$, o que mostra que ($x_{1_0}q$, $x_{2_0}q$, ..., $x_{(n-1)_0}q$, $x_{n_0}q$) é uma de suas soluções particulares.

Para encontrarmos a equação geral devemos utilizar o processo de reduzi-la a uma equação diofantina linear de duas variáveis. Para isso, faremos uma substituição de n - 1 variáveis, por uma outra variável qualquer, diferente das já existentes. Feito isso, basta encontrar a solução geral desta nova equação gerada. Aplicando esse processo repetidas vezes, encontraremos todos os valores de x_{i_0} com i = 1, 2, 3, ..., n, assim como desenvolvido para encontrar a solução geral das equações diofantinas lineares de três variáveis. Então, a solução geral de uma equação diofantina linear de n variáveis, se apresenta da seguinte forma:

$$S = \left\{\left(x_{1_0} + \frac{a_2}{d_{n-1}}t_{n-1}, x_{2_0} - \frac{a_1}{d_{n-1}}t_{n-1}, x_{3_0} - t_{n-2}, \dots, x_{1_0} - t_1\right) / \; t_i \in \mathbb{Z}, \text{com } i = 1, 2, \dots, n-1\right\}$$ sendo $d_{n-1} = mdc(a_1, a_2)$.

Podemos concluir que o número de parâmetros na solução geral de uma equação diofantina linear se dá da seguinte forma:

I) Se a equação possui duas variáveis, a solução geral estará em função de um parâmetro;

II) Se a equação possui três variáveis, a solução geral estará em função de dois parâmetros;

III) Se a equação possui quatro variáveis, a solução geral estará em função de três parâmetros;

Assim, indutivamente, uma equação diofantina linear com n variáveis, terá sua solução geral em função de n - 1 parâmetros.

Exemplo 1. Determine uma solução particular e a solução geral da equação 100x + 72y + 90z = 6.

Solução. Como o mdc(100, 72, 90) = 2 e $2 \mid 6$, então a equação possui solução. Consideremos agora a equação dada na forma equivalente, 50x + 36y + 45z = 3. Usando o algoritmo de Euclides para o cálculo do mdc(50, 36) temos:

	1	2	1	1	3
50	36	14	8	6	2
14	8	6	2	0	

Assim, 14 = 50 – 36.1

8 = 36 – 14.2

6 = 14 – 8.1

2 = 8 – 6.1

daí, 2 = 8 – 6.1 = 8 - (14 – 8.1) = 8.2 - 14 = (36 – 14.2).2 - 14 = 36.2 – 14.5 = 36.2 - (50 – 36.1).5 = - 50.5 + 36.7 = 50.(- 5) + 36.7.

Aplicando novamente o algoritmo de Euclides para o mdc(2, 45), temos:

	22	2
45	2	1
1	0	

logo, 1 = 45 – 2.22 e como 2 = 50.(- 5) + 36.7 segue que:

1 = 45 - [50.(- 5) + 36.7].22

1 = 45.1 + 50.110 + 36.(- 154)

1 = 50.110 + 36.(- 154) + 45.1

Daí, o terno (110, - 154, 1) é solução de 50x + 36y + 45z = 1, logo ($3x_0$, $3y_0$, $3z_0$) = (330, - 462, 3) é uma solução particular da equação dada.

Agora vamos por partes, encontrar sua solução geral, considerando sua forma equivalente, 50x + 36y + 45z = 3. Seja p = 50x + 36y, que gera a equação, p + 45z = 3, que também possui solução, pois mdc(1, 45) = 1 e 1 $\mid$ 3. Então, conseguimos encontrar uma solução particular para a equação p + 45z = 3, fazendo,

1 = 1.(- 44) + 45.1

3 = 1.(- 132) + 45.3

que nos leva a solução geral de p + 45z = 3 como:

$$S_1 = \{(-132 + 45t_1, 3 - t_1) / t_1 \in \mathbb{Z}\}.$$

Para encontrar a solução geral da equação original, devemos agora encontrar a solução geral da equação 50x + 36y = p = - 132 + $45t_1$. Para que essa equação possua solução, o mdc(50, 36) = 2 deve dividir – 132 + $45t_1$.
Satisfazendo a condição acima, basta encontrar a solução geral, assim pelo algoritmo que resolvemos antes, temos que 2 = 50.(- 5) + 36.7. Portanto,

$$2 = 50.(-5) + 36.7 \Leftrightarrow \left(\frac{-132 + 45t_1}{2}\right).2 = 50.(-5).\left(\frac{-132 + 45t_1}{2}\right) + 36.7.\left(\frac{-132 + 45t_1}{2}\right) \Leftrightarrow$$

$$-132 + 45t_1 = 50.\left(\frac{660 - 225t_1}{2}\right) + 36.\left(\frac{-924 + 315t_1}{2}\right)$$

temos que a equação geral de 50x + 36y = p = - 132 + $45t_1$ é:

$$S_2 = \left\{\left(\frac{660 - 225t_1}{2} + \frac{36}{2}t_2, \frac{-924 + 315t_1}{2} - \frac{50}{2}t_2\right) / \ t_1, t_2 \in \mathbb{Z}\right\}$$

Com isso, podemos concluir que a solução geral da equação diofantina linear de três variáveis é:

$$S = \left\{\left(\frac{660 - 225t_1}{2} + 18t_2, \frac{-924 + 315t_1}{2} - 25t_2, 3 - t_1\right) \ / \ t_1, t_2 \in \mathbb{Z}\right\}.$$

Exemplo 2. Determine a solução geral da equação 120x + 65y + 90z + 45w = 25.

Solução. Como o mdc(120, 65, 90, 45) = 5 e 5 | 25, então a equação possui solução. Dividindo a equação dada por 5 obtemos a equação equivalente, 24x + 13y + 18z + 9w = 5. Sendo p = 24x + 13y + 18z temos que p + 9w = 5, que possui solução, pois mdc(1, 9) = 1 e 1 | 5. Agora devemos encontrar a solução geral de p + 9w = 5. Como o mdc(1, 9) = 1, podemos fazer:

$1 = 1.(-8) + 9.1$

$5 = 1.(-40) + 9.5$

Disso temos que $(p_0, w_0) = (-40, 5)$ é uma solução particular de p + 9w = 5 e

$$S_1 = \{(-40 + 9t_1, 5 - t_1) / t_1 \in \mathbb{Z}\},$$

representa a solução geral de p + 9w = 5.

Voltando para a primeira substituição, temos $24x + 13y + 18z = p = -40 + 9t_1$ que possui solução qualquer que seja o valor de t_1, pois mdc(24, 13, 18) = 1 e 1 | $(-40 + 9t_1)$.

Continuando a procura pela solução geral, devemos fazer uma nova substituição. Assim, seja q = 24x + 13y. Dessa segunda substituição, segue que $q + 18z = -40 + 9t_1$, que também possui solução qualquer que seja o valor de t_1 pois, mdc(1, 18) = 1 e 1 | $(-40 + 9t_1)$.

Agora, devemos encontrar a solução geral de $q + 18z = -40 + 9t_1$. Já sabemos que mdc(1, 18) = 1, então temos:

$1 = 1.(-17) + 18.1$

$-40 + 9t_1 = 1.(-17).(-40 + 9t_1) + 18.1.(-40 + 9t_1)$

$-40 + 9t_1 = 1.(680 - 153t_1) + 18.(-40 + 9t_1)$

daí, concluímos que $(q_0, z_0) = (680 - 153t_1, - 40 + 9t_1)$ e a solução geral de $q + 18z = - 40 + 9t_1$ é:

$$S_2 = \{(680 - 153t_1 + 18t_2, - 40 + 9t_1 - t_2) / t_1, t_2 \in \mathbb{Z}\}.$$

Depois de ter encontrado as soluções de $p + 9w = 5$ e $q + 18z = - 40 + 9t_1$, agora é suficiente encontrar a solução geral de

$$24x + 13y = q = 680 - 153t_1 + 18t_2$$

que possui solução qualquer que sejam os valores de t_1 e t_2, pois mdc(24, 13) = 1 e 1 | $(680 - 153t_1 + 18t_2)$. Utilizando o algoritmo de Euclides para mdc(24, 13), temos

	1	1	5	2
24	13	11	2	1
11	2	1	0	

daí, segue que $11 = 24 – 13.1$

$2 = 13 – 11.1$

$1 = 11 – 2.5$

assim, $1 = 11 – 2.5 = 11 - (13 – 11.1).5 = 11.6 – 13.5 = (24 – 13.1).6 – 13.5 = 24.6 – 13.11 = 24.6 + 13.(- 11)$.

Portanto, multiplicando a equação $1 = 24.6 + 13.(- 11)$ por $680 - 153t_1 + 18t_2$, obtemos,

$680 - 153t_1 + 18t_2 = 24.6.(680 - 153t_1 + 18t_2) + 13.(- 11).(680 - 153t_1 + 18t_2) \Leftrightarrow 680 - 153t_1 + 18t_2 = 24.(4080 - 918t_1 + 108t_2) + 13.(- 7480 + 1683t_1 - 198t_2)$

disso obtemos $(x_0, y_0) = (4080 - 918t_1 + 108t_2, - 7480 + 1683t_1 - 198t_2)$ e a solução geral de $q = 680 - 153t_1 + 18t_2$ é:

$$S_3 = \{(4080 - 918t_1 + 108t_2 + 13t_3, - 7480 + 1683t_1 - 198t_2 - 24t_3) / t_1, t_2, t_3 \in \mathbb{Z}\}.$$

Contudo obtemos a solução geral para a equação $120x + 65y + 90z + 45w = 25$, que é expressa por,

$$S = \{(4080 - 918t_1 + 108t_2 + 13t_3, - 7480 + 1683t_1 - 198t_2 - 24t_3, - 40 + 9t_1 - t_2, 5 - t_1) / t_1, t_2, t_3 \in \mathbb{Z}\}.$$

Tomando $t_1 = 0$, $t_2 = 1$ e $t_3 = 2$, obtemos:

$w = 5$
$z = - 40 + 9.0 – 1 = - 41$
$y = - 7480 + 1683.0 – 198.1 – 24.2 = - 7726$
$x = 4080 – 918.0 + 108.1 + 13.2 = 4214$

isto é, $(4214, - 7726, - 41, 5)$ é uma solução particular de $120x + 65y + 90z + 45w = 25$. Assim, para cada valor atribuído aos parâmetros t_1, t_2 e t_3, será gerada uma nova solução particular.

Exemplo 3. Encontre a solução geral de $32x - 60y - 24z + 42w + 14u = 12$.

Solução. Como o $mdc(32, 60, 24, 42, 14) = 2$ e $2 \mid 12$, então a equação possui solução. Dividindo a equação por 2 obtemos a equação equivalente, $16x - 30y - 12z + 21w + 7u = 6$. Seja $p = 16x - 30y - 12z + 21w$, daí, $p + 7u = 6$, também possui solução, pois $mdc(1, 7) = 1$ e $1 \mid 6$. Assim,

$1 = 1.(- 6) + 7.1$
$6 = 1.(- 36) + 7.6$

então, $(- 36, 6)$ é uma solução particular de $p + 7u = 6$, que nos leva a solução geral

$$S_1 = \{(-36 + 7t_1, 6 - t_1) / t_1 \in \mathbb{Z}\}.$$

Continuando pela busca da solução geral, faremos $16x - 30y - 12z + 21w = p = -36 + 7t_1$ que possui solução, qualquer que seja o valor para t_1, pois mdc(16, 30, 12, 21) = 1.

Considerando $p' = 16x - 30y - 12z$, obtemos $p' + 21w = -36 + 7t_1$ e como o mdc(1, 21) = 1, qualquer que seja o valor de t_1 teremos o mdc(1, 21) dividindo $-36 + 7t_1$. Assim, temos

$$1 = 1.(-20) + 21.1$$
$$-36 + 7t_1 = 1.(-20).(-36 + 7t_1) + 21.1.(-36 + 7t_1)$$
$$-36 + 7t_1 = 1.(720 - 140t_1) + 21.(-36 + 7t_1)$$

que possui $(720 - 140t_1, -36 + 7t_1)$ como uma solução particular e

$$S_2 = \{(720 - 140t_1 + 21t_2, -36 + 7t_1 - t_2) / t_1, t_2 \in \mathbb{Z}\},$$

como solução geral de $p' + 21w = -36 + 7t_1$.

Desta vez, seja $16x - 30y - 12z = p' = 720 - 140t_1 + 21t_2$ que possui solução atribuindo um valor para t_2, de forma que $720 - 140t_1 + 21t_2$ seja divisível pelo mdc(16, 30, 12) = 2. Sendo $p'' = 16x - 30y$, obtemos $p'' - 12z = 720 - 140t_1 + 21t_2$. Portanto, como anteriormente, qualquer que seja o valor de t_2 teremos o mdc(1, 12) dividindo $720 - 140t_1 + 21t_2$, assim,

$1 = 1.13 - 12.1 \Leftrightarrow 720 - 140t_1 + 21t_2 = 1.13.(720 - 140t_1 + 21t_2) - 12.1.(720 - 140t_1 + 21t_2) \Leftrightarrow 720 - 140t_1 + 21t_2 = 1.(9360 - 1820t_1 + 273t_2) - 12.(720 - 140t_1 + 21t_2)$

que possui como uma solução particular $(9360 - 1820t_1 + 273t_2, 720 - 140t_1 + 21t_2)$ e

$$S_3 = \{(9360 - 1820t_1 + 273t_2 - 12t_3, 720 - 140t_1 + 21t_2 - t_3) / t_1, t_2, t_3 \in \mathbb{Z}\},$$

como solução geral de $p'' - 12z = 720 - 140t_1 + 21t_2$.

Finalmente, tomamos 16x - 30y = p'' = 9360 - $1820t_1$ + $273t_2$ - $12t_3$ e como mdc(16, 30) = 2 devemos escolher um valor adequado para t_3 que faça com que 2 divida 9360 - $1820t_1$ + $273t_2$ - $12t_3$. Pelo algoritmo de Euclides para o mdc(16, 30), temos

	1	1	7
30	16	14	2
14	2	0	

assim,

14 = 30 – 16.1

2 = 16 – 14.1

daí, 2 = 16 – 14.1 = 16 - (30 – 16.1).1 = 16.2 – 30.1 assim, temos

2 = 16.2 - 30.1 $\Leftrightarrow$ $2.\left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$ = $16.2.\left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$ - $30.1.\left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$ $\Leftrightarrow$ $9360 - 1820t_1 + 273t_2 - 12t_3$ = $16.(9360 - 1820t_1 + 273t_2 - 12t_3)$ - $30.1.\left(\frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$

que possui solução particular

$$\left(9360 - 1820t_1 + 273t_2 - 12t_3, \frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2}\right)$$

e

$S_4 = \left\{\left(9360 - 1820t_1 + 273t_2 - 12t_3 - \frac{30}{2}t_4, \frac{9360 - 1820t_1 + 273t_2 - 12t_3}{2} - \frac{16}{2}t_4\right) / t_1, t_2, t_3, t_4 \in \mathbb{Z}\right\}$,

como solução geral de p'' = 9360 - $1820t_1$ + $273t_2$ - $12t_3$.

Portanto, podemos concluir que

$$S= \left\{\left(9360 - 1820t_1 + 273t_2 - 12t_3 - 15t_4, \frac{9360-1820t_1+273t_2-12t_3}{2} - 8t_4, 720 - 140t_1 + 21t_2 - t_3, -36 + 7t_1 - t_2, 6 - t_1\right) / t_1, t_2, t_3, t_4 \in \mathbb{Z}\right\},$$

é a solução geral da equação 32x - 60y - 24z + 42w + 14u = 12.

Agora, a partir da solução geral, é possível encontrar uma solução particular qualquer para a equação. Tomando $t_1 = 1$, $t_2 = 0$, $t_3 = 4$ e $t_4 = 10$, obtemos

u = 5
w = - 36 + 7.1 – 0 = - 29
z = 720 – 140.1 + 21.0 – 4 = 576
$y = \frac{9360 - 1820.1 + 273.0 - 12.4}{2} = 3746$
x = 9360 – 1820.1 + 273.0 – 12.4 – 15.10 = 7342

isto é, uma solução particular é S = {(7342, 3746, 576, - 29, 5)}.

Exemplo 4. Determine a solução geral para 45x - 15y - 27z + 36w + 16u - 8v = 43.

Solução. Ora, como o mdc(45, 15, 27, 36, 16, 8) = 1 e 1 $\mid$ 43, então a equação possui solução. Substituindo as cinco primeiras incógnitas por uma, teremos p = 45x - 15y - 27z + 36w + 16u, daí obtemos p - 8v = 43, que também possui solução, pois mdc(1, 8) = 1 e 1 $\mid$ 43. Então,

1 = 1.9 – 8.1
43 = 1.387 - 8.43

e a partir disso, encontramos $(p_0, v_0) = (387, 43)$, que representa uma solução particular de p - 8v = 43 e

$$S_1 = \{(387 - 8t_1, 43 - t_1) / t_1 \in \mathbb{Z}\},$$

como solução geral de p - 8v = 43.

Voltando para a primeira substituição, temos: 45x - 15y - 27z + 36w + 16u = p = 387 - $8t_1$ que possui solução qualquer que seja o valor de t_1, pois mdc(45, 15, 27, 36, 16) = 1 $\mid$ 43. Com uma nova substituição, considerando p' = 45x - 15y - 27z + 36w, obtemos p' + 16u = 387 - $8t_1$, que também possui solução pois mdc(1, 16) = 1 $\mid$ (387 - $8t_1$). Então, como mdc(1, 16) = 1 segue que

$$1 = 1.(-15) + 16.1$$
$$387 - 8t_1 = 1.(-15).(387 - 8t_1) + 16.1.(387 - 8t_1)$$
$$387 - 8t_1 = 1.(-5805 + 120t_1) + 16.(387 - 8t_1)$$

assim, $(p'_0, u_0) = (-5805 + 120t_1, 387 - 8t_1)$ e a solução geral de p' + 16u = 387 - $8t_1$ é

$$S_2 = \{(-5805 + 120t_1 + 16t_2, 387 - 8t_1 - t_2) / t_1, t_2 \in \mathbb{Z}\}.$$

Voltando para a segunda substituição, temos 45x - 15y - 27z + 36w = p' = - 5805 + $120t_1$ + $16t_2$ e para que a equação acima admita solução, devemos atribuir valores a t_1 e t_2, de forma que mdc(45, 15, 27, 36) = 3 $\mid$ (- 5805 + $120t_1$ + $16t_2$).

Prosseguindo em busca da solução geral, faremos uma nova substituição, sendo p'' = 45x - 15y - 27z, obtemos p'' + 36w = - 5805 + $120t_1$ + $16t_2$, que possui solução pois mdc(1, 36) = 1 $\mid$ (- 5805 + $120t_1$ + $16t_2$) qualquer que sejam os valores de t_1 e t_2. Logo,

$$1 = 1.(-35) + 36.1 \Leftrightarrow -5805 + 120t_1 + 16t_2 = 1.(-35).(-5805 + 120t_1 + 16t_2) + 36.1.(-5805 + 120t_1 + 16t_2) \Leftrightarrow -5805 + 120t_1 + 16t_2 = 1.(203175 - 4200t_1 - 560t_2) + 16.(-5805 + 120t_1 + 16t_2)$$

que resulta em, $(p''_0, w_0) = (203175 - 4200t_1 - 560t_2, -5805 + 120t_1 + 16t_2)$ e gera

$$S_3 = \{(203175 - 4200t_1 - 560t_2 + 36t_3, -5805 + 120t_1 + 16t_2 - t_3) / t_1, t_2, t_3 \in \mathbb{Z}\},$$

como solução geral de p'' + 36w = - 5805 + $120t_1$ + $16t_2$.

Agora, devemos voltar na terceira substituição feita, isto é, 45x - 15y - 27z = p'' = 203175 - $4200t_1$ - $560t_2$ + $36t_3$ e para que essa equação tenha solução, devemos atribuir valores acessíveis a t_1, t_2 e t_3 de modo que o mdc(45, 15, 27) = 3 $\mid$(203175 - $4200t_1$ - $560t_2$ + $36t_3$). Com a substituição de duas variáveis por uma, considerando p''' = 45x - 15y, obtemos p''' - 27z = 203175 - $4200t_1$ - $560t_2$ + $36t_3$, que possui solução qualquer que sejam os valores de t_1, t_2 e t_3, pois mdc(1, 27) = 1 $\mid$(203175 - $4200t_1$ - $560t_2$ + $36t_3$). Resolvendo p''' - 27z = 203175 - $4200t_1$ - $560t_2$ + $36t_3$, temos:

1 = 1.28 – 27.1 $\Leftrightarrow$ 203175 - $4200t_1$ - $560t_2$ + $36t_3$ = 1.28.(203175 - $4200t_1$ - $560t_2$ + $36t_3$) – 27.1.(203175 - $4200t_1$ - $560t_2$ + $36t_3$) $\Leftrightarrow$ 203175 - $4200t_1$ - $560t_2$ + $36t_3$ = 1.(5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$) – 27.1.(203175 - $4200t_1$ - $560t_2$ + $36t_3$)

que gera (p'''_0, z_0) = (5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$, 203175 - $4200t_1$ - $560t_2$ + $36t_3$) e tem como solução geral para p''' - 27z = 203175 - $4200t_1$ - $560t_2$ + $36t_3$,

S_4 = {(5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$ - $27t_4$, 203175 - $4200t_1$ - $560t_2$ + $36t_3$ - t_4) / t_1, t_2, t_3, t_4 $\in \mathbb{Z}$}.

Finalmente, basta voltar para a quarta substituição e resolver a equação, isto é, 45x - 15y = p''' = 5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$ - $27t_4$, e para que essa equação possua solução, devemos atribuir valores convenientes a t_1, t_2, t_3 e t_4, de maneira que o mdc(45, 15) = 15 $\mid$(5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$ - $27t_4$). Pelo fato do mdc(45, 15) = 15, temos

$$15 = 45.1 - 15.2 \Leftrightarrow 15.\left(\frac{5688900 - 117600t_1 - 15680t_2 + 1008t_3 - 27t_4}{15}\right) =$$

$$45.1.\left(\frac{5688900 - 117600t_1 - 15680t_2 + 1008t_3 - 27t_4}{15}\right) -$$

$$15.2.\left(\frac{5688900 - 117600t_1 - 15680t_2 + 1008t_3 - 27t_4}{15}\right) \Leftrightarrow 5688900 - 117600t_1 -$$

$$15680t_2 + 1008t_3 - 27t_4 = 45.\left(379260 - 7840t_1 - \frac{3136}{3}t_2 + \frac{336}{5}t_3 - \frac{9}{5}t_4\right) - 15.\left(758520 - 15680t_1 - \frac{6272}{3}t_2 + \frac{672}{5}t_3 - \frac{18}{5}t_4\right).$$

Com isso, obtemos (x_0, y_0) como sendo

$$\left(379260 - 7840t_1 - \frac{3136}{3}t_2 + \frac{336}{5}t_3 - \frac{9}{5}t_4, 758520 - 15680t_1 - \frac{6272}{3}t_2 + \frac{672}{5}t_3 - \frac{18}{5}t_4\right)$$

e

$$S_5 = \left\{\left(379260 - 7840t_1 - \frac{3136}{3}t_2 + \frac{336}{5}t_3 - \frac{9}{5}t_4 - \frac{15}{15}t_5, 758520 - 15680t_1 - \frac{6272}{3}t_2 + \frac{672}{5}t_3 - \frac{18}{5}t_4 - \frac{45}{15}t_5\right) / t_1, t_2, t_3, t_4, t_5 \in \mathbb{Z}\right\}$$

como solução geral de p''' = 5688900 - $117600t_1$ - $15680t_2$ + $1008t_3$ - $27t_4$.

Portanto, a solução geral da equação original é:

$$S = \left\{\left(379260 - 7840t_1 - \frac{3136}{3}t_2 + \frac{336}{5}t_3 - \frac{9}{5}t_4 - t_5, 758520 - 15680t_1 - \frac{6272}{3}t_2 + \frac{672}{5}t_3 - \frac{18}{5}t_4 - 3t_5, 203175 - 4200t_1 - 560t_2 + 36t_3 - t_4, -5805 + 120t_1 + 16t_2 - t_3, 387 - 8t_1 - t_2, 43 - t_1\right) / t_1, t_2, t_3, t_4, t_5 \in \mathbb{Z}\right\}.$$

Para determinar uma solução particular, basta atribuir valores convenientes aos parâmetros, então, se $t_1 = 1$, $t_2 = 3$, $t_3 = -1$, $t_4 = -4$ e $t_5 = 2$, temos:

v = 43 – 1 = 42

u = 387 – 8.1 – 3 = 376

w = - 5805 + 120.1 + 16.3 –(- 1) = - 5636

z = 203175 – 4200.1 – 560.3 + 36.(- 1) – (- 4) = 197263

$y = 758520 - 15680.1 - \frac{6272}{3}.3 + \frac{672}{5}.(-1) - \frac{18}{5}.(-4) - 3.2 =$ 736442

$x = 379260 - 7840.1 - \frac{3136}{3}.3 + \frac{336}{5}.(-1) - \frac{9}{5}.(-4) - 2 = 368222$

isto é,

S = {(368222, 736442, 197263, - 5636, 376, 42)}.

4.6 Situações-problema envolvendo equações diofantinas lineares com n variáveis

Observando o fato de que atualmente, com a aplicação das provas do Enem, a interpretação de situações problema tem sido de fundamental importância para um desempenho eficaz, juntamente com os conhecimentos científicos adquiridos durante a vida estudantil, ampliando o senso crítico, a visão de mundo e atualidades. Sendo assim, entendemos que é de grande valia a abordagem dessa questão. Como a observância, a interpretação e resolução de problemas estão presentes em situações do nosso cotidiano, devem ser trabalhadas efetivamente com os alunos da educação básica, mostrando ao aluno a aplicação de tais conhecimentos nessas situações, por isso, além de simplesmente mostrar como resolver equações diofantinas lineares, também resolveremos problemas cuja interpretação matemática gera uma equação diofantina linear. Portanto, veremos alguns problemas que serão solucionados através dos conceitos previstos.

Problema 1. Deseja-se sacar R$ 1000,00 em notas de R$ 2,00, R$ 5,00 e R$ 10,00. Apresente um método para encontrar formas distintas de efetuar esse saque?

Solução. De acordo com o enunciado, geramos a seguinte equação diofantina, $2x + 5y + 10z = 1000$, onde x representa o número de notas de 2, y o número de notas de 5 e z o número de notas de 10, onde é obrigatório o saque de pelo menos uma nota de cada tipo. Para resolvermos o problema basta encontrar a solução geral da equação gerada. Como $mdc(2, 5, 10) = 1$ e $1 \mid 1000$, segue que a equação possui solução. Tomando $2x + 5y = p$, temos que $p + 10z = 1000$ e como $mdc(1, 10) = 1$ e $1 \mid 1000$, podemos fazer:

$$1 = 1.(-9) + 10.1$$
$$1000 = 1.(-9000) + 10.1000$$

daí, $p = -9000 + 10t_1$ e $z = 1000 - t_1$, e como p e z devem ser números naturais, temos,

$$-9000 + 10t_1 > 0 \Leftrightarrow 10t_1 > 9000 \Leftrightarrow t_1 > 900$$

e

$$1000 - t_1 > 0 \Leftrightarrow - t_1 > - 1000 \Leftrightarrow t_1 < 1000$$

gerando, $900 < t_1 < 1000$, com $t_1 \in \mathbb{Z}$.

Para determinar x e y devemos escolher um valor conveniente para t_1, de modo que o mdc(2, 5) divida p. Como o mdc(2, 5) = 1, então t_1 pode assumir qualquer valor no intervalo. Seja $t_1 = 901$, então, $2x + 5y = p = - 9000 + 10t_1 = - 9000 + 10.901 = 10$. Utilizando o algoritmo de Euclides para o mdc(2, 5), temos:

$1 = 5.1 – 2.2$
$1 = 2.(- 2) + 5.1$
$10 = 2.(- 20) + 5.10$

assim, $x = - 20 + 5t_2$ e $y = 10 - 2t_2$ e como x e y devem ser números inteiros positivos, devemos ter,

$$- 20 + 5t_2 > 0 \Leftrightarrow 5t_2 > 20 \Leftrightarrow t_2 > 4$$

e

$$10 - 2t_2 > 0 \Leftrightarrow - 2t_2 > - 10 \Leftrightarrow t_2 < 5$$

que gera, $4 < t_2 < 5$, assim, para $t_1 = 901$, não existe $t_2 \in \mathbb{Z}$ satisfazendo, isto é, nenhuma maneira de efetuar o saque.

Agora, seja $t_1 = 902$, logo, $2x + 5y = p = - 9000 + 10t_1 = - 9000 + 10.902 = 20$. Como já vimos, temos que

$$1 = 2.(- 2) + 5.1 \Leftrightarrow 20 = 2.(- 40) + 5.20$$

então, $x = - 40 + 5t_2$ e $y = 20 - 2t_2$ e como x e y devem ser números naturais, devemos ter $8 < t_2 < 10$, que resulta em $t_2 = 9$, que representa um modo de efetuar o saque.

Para $t_1 = 903$, temos $2x + 5y = p = -9000 + 10t_1 = -9000 + 10.903 = 30$, que pode ser representada assim,

$$1 = 2.(-2) + 5.1 \Leftrightarrow 30 = 2.(-60) + 5.30$$

assim, $x = -60 + 5t_2$ e $y = 30 - 2t_2$ e como x e y devem ser números inteiros positivos, segue que, $12 < t_2 < 15$, ou seja, dois modos de efetuar o saque.

Tomando qualquer valor para t_1 no referido intervalo, teremos também uma determinada quantidade de t_2, com isso encontraremos todos os modos de efetuar o saque.

Com $t_1 = 950$, temos $2x + 5y = p = -9000 + 10t_1 = -9000 + 10.950 = 500$, daí,

$$1 = 2.(-2) + 5.1 \Leftrightarrow 500 = 2.(-1000) + 5.500,$$

assim, $x = -1000 + 5t_2$ e $y = 500 - 2t_2$ e como x e y devem ser números naturais, devemos ter $200 < t_2 < 250$, ou seja, $250 - 200 - 1 = 49$ modos de efetuar o saque.

Contudo que foi exposto, podemos concluir que existem vários modos distintos de se efetuar o saque. Para encontrarmos todos esses modos, devemos analisar os intervalos de t_1 e t_2, e para fazer esta análise de maneira eficaz, basta colocar t_2 em função de t_1, pois a partir da escolha de um valor conveniente para t_1, encontraremos o intervalo apropriado para t_2. Para encontrar t_2 em função de t_1, faremos $2x + 5y = p = -9000 + 10t_1$. Então, temos:

$$1 = 5.1 - 2.2$$
$$1 = 2.(-2) + 5.1$$
$$-9000 + 10t_1 = 2.(-2).(-9000 + 10t_1) + 5.1.(-9000 + 10t_1)$$
$$-9000 + 10t_1 = 2.(18000 - 20t_1) + 5.(-9000 + 10t_1)$$

assim, $x = 18000 - 20t_1 + 5t_2$ e $y = -9000 + 10t_1 - 2t_2$ e como x e y devem ser números naturais, devemos ter:

$$18000 - 20t_1 + 5t_2 > 0 \Leftrightarrow t_2 > 4t_1 - 3600$$

e

$$-9000 + 10t_1 - 2t_2 > 0 \Leftrightarrow t_2 < 5t_1 - 4500,$$

isto é, $4t_1 - 3600 < t_2 < 5t_1 - 4500$ que representa o intervalo desejado, pois gera, juntamente com o intervalo de t_1, cada um dos distintos modos de efetuar o saque.

Façamos alguns testes.

Se $t_1 = 901$, temos

$4t_1 - 3600 < t_2 < 5t_1 - 4500$
$4.901 - 3600 < t_2 < 5.901 - 4500$
$4 < t_2 < 5$

isto é, para $t_1 = 901$ não existe t_2, gerando assim, nenhum modo de efetuar o saque, tal como vimos anteriormente.

Seja agora, $t_1 = 902$, assim,

$4t_1 - 3600 < t_2 < 5t_1 - 4500$
$4.902 - 3600 < t_2 < 5.902 - 4500$
$8 < t_2 < 10$

isto é, para $t_1 = 902$, temos $10 - 8 - 1 = 1$ modo de efetuar o saque.

Se $t_1 = 950$, temos

$4t_1 - 3600 < t_2 < 5t_1 - 4500$
$4.950 - 3600 < t_2 < 5.950 - 4500$
$200 < t_2 < 250$

isto é, para $t_1 = 950$, temos $250 - 200 - 1 = 49$ modos de efetuar o saque.

Contudo, fica provado que o intervalo encontrado para t_2 nos dá de maneira eficiente, todos os possíveis modos de efetuar o saque, baseados no intervalo de t_1, ou seja, o método apresentado é verdadeiro.

Problema 2. Deseja-se sacar R$ 40,00 em notas de R$ 2,00, R$ 5,00 ou R$ 10,00. De quantas maneiras é possível efetuar esse saque?

Solução. Percebemos que este problema é semelhante ao anterior, exceto pelo fato de que podemos considerar também, os saques com notas apenas de um tipo ou saques com notas de dois tipos. Pelo enunciado a equação diofantina gerada é $2x + 5y + 10z = 40$, onde x representa o número de notas de 2, y o número de notas de 5 e z o número de notas de 10. Para responder a pergunta basta encontrar a solução geral da equação gerada. Aproveitando os cálculos realizados do problema anterior, temos $2x + 5y = p$, assim, $p + 10z = 40$ e como $mdc(1, 10) = 1$, podemos fazer:

$$1 = 1.(-9) + 10.1$$
$$40 = 1.(-360) + 10.40$$

então, $p = -360 + 10t_1$ e $z = 40 - t_1$ e como p e z devem ser números naturais, devemos ter,

$$-360 + 10t_1 \geq 0 \Leftrightarrow 10t_1 \geq 360 \Leftrightarrow t_1 \geq 36$$

e

$$40 - t_1 \geq 0 \Leftrightarrow -t_1 \geq -40 \Leftrightarrow t_1 \leq 40$$

gerando $36 \leq t_1 \leq 40$ com $t_1 \in \mathbb{Z}$.

Para determinar os valores para x e y, faremos $2x + 5y = p = -360 + 10t_1$ e como o $mdc(2, 5) = 1$, qualquer que seja o valor de t_1 sempre teremos 1 dividindo $p = -360 + 10t_1$, assim,

$1 = 2.(-2) + 5.1$

$-360 + 10t_1 = 2.(-2).(-360 + 10t_1) + 5.1.(-360 + 10t_1)$

$-360 + 10t_1 = 2.(720 - 20t_1) + 5.(-360 + 10t_1)$

logo, $x = 720 - 20t_1 + 5t_2$ e $y = -360 + 10t_1 - 2t_2$ e como x e y devem ser números naturais, teremos

$$720 - 20t_1 + 5t_2 \geq 0 \Leftrightarrow t_2 \geq 4t_1 - 144$$

e

$$-360 + 10t_1 - 2t_2 \geq 0 \Leftrightarrow t_2 \leq 5t_1 - 180$$

gerando, $4t_1 - 144 \leq t_2 \leq 5t_1 - 180$ com $t_2 \in \mathbb{Z}$.

Portanto, para determinar todos os possíveis modos de efetuar o saque, faremos as escolhas para t_1 no intervalo $36 \leq t_1 \leq 40$. Vejamos cada caso:

I) Se $t_1 = 36$, temos que, $4.36 - 144 = 0 \leq t_2 \leq 5.36 - 180 = 0$, isto é, $t_2 = 0$, que representa **um** modo de efetuar o saque. Para determinar a configuração desse saque, basta substituirmos os valores encontrados para t_1 e t_2 em x, y e z, assim,

$z = 40 - t_1 = 40 - 36 = 4$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.36 - 2.0 = 0$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.36 + 5.0 = 0$

ou seja, o saque será feito somente com quatro notas de dez.

II) Se $t_1 = 37$, temos que, $4.37 - 144 = 4 \leq t_2 \leq 5.37 - 180 = 5$, isto é, dois modos de efetuar o saque. Assim, para encontrar essa configuração, faremos como no caso anterior, mas, devendo analisar, $t_2 = 4$ e $t_2 = 5$;

a) para $t_1 = 37$ e $t_2 = 4$

$z = 40 - t_1 = 40 - 37 = 3$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.37 - 2.4 = 2$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.37 + 5.4 = 0$

isto é, o saque será feito apenas com duas notas de cinco e três notas de dez;

b) para $t_1 = 37$ e $t_2 = 5$

$z = 40 - t_1 = 40 - 37 = 3$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.37 - 2.5 = 0$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.37 + 5.5 = 5$

assim, o saque será feito apenas com cinco notas de dois e três notas de dez.

III) Se $t_1 = 38$, temos que, $4.38 - 144 = 8 \leq t_2 \leq 5.38 - 180 = 10$, ou seja, três modos de efetuar o saque. Portanto, analisaremos os casos $t_2 = 8$, $t_2 = 9$ e $t_2 = 10$.

a) para $t_1 = 38$ e $t_2 = 8$

$z = 40 - t_1 = 40 - 38 = 2$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.38 - 2.8 = 4$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.38 + 5.8 = 0$

logo, o saque será feito apenas com quatro notas de cinco e duas notas de dez;

b) para $t_1 = 38$ e $t_2 = 9$

$z = 40 - t_1 = 40 - 38 = 2$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.38 - 2.9 = 2$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.38 + 5.9 = 5$

assim, o saque será feito com cinco notas de dois, duas notas de cinco e duas notas de dez;

c) para $t_1 = 38$ e $t_2 = 10$

$z = 40 - t_1 = 40 - 38 = 2$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.38 - 2.10 = 0$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.38 + 5.10 = 10$

então, o saque será feito apenas com dez notas de dois e duas notas de dez.

IV) Se $t_1 = 39$, temos que, $4.39 - 144 = 12 \leq t_2 \leq 5.39 - 180 = 15$, ou seja, quatro modos de efetuar o saque;

a) para $t_1 = 39$ e $t_2 = 12$

$z = 40 - t_1 = 40 - 39 = 1$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.39 - 2.12 = 6$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.39 + 5.12 = 0$

assim, o saque será feito apenas com seis notas de cinco e uma nota de dez;

b) para $t_1 = 39$ e $t_2 = 13$

$z = 40 - t_1 = 40 - 39 = 1$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.39 - 2.13 = 4$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.39 + 5.13 = 5$

logo, o saque será feito com cinco notas de dois, quatro notas de cinco e uma nota de dez;

c) para $t_1 = 39$ e $t_2 = 14$

$z = 40 - t_1 = 40 - 39 = 1$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.39 - 2.14 = 2$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.39 + 5.14 = 10$

então, o saque será feito com dez notas de dois, duas notas de cinco e uma nota de dez;

d) para $t_1 = 39$ e $t_2 = 15$

$z = 40 - t_1 = 40 - 39 = 1$

$y = -360 + 10t_1 - 2t_2 = -360 + 10.39 - 2.15 = 0$

$x = 720 - 20t_1 + 5t_2 = 720 - 20.39 + 5.15 = 15$

neste, o saque será feito apenas com quinze notas de dois e uma nota de dez.

V) Se $t_1 = 40$, temos que, $4.40 - 144 = 16 \leq t_2 \leq 5.40 - 180 = 20$, ou seja, cinco modos de efetuar o saque;

a) para $t_1 = 40$ e $t_2 = 16$

$z = 40 - t_1 = 40 - 39 = 0$

$$y = -360 + 10t_1 - 2t_2 = -360 + 10.40 - 2.16 = 8$$

$$x = 720 - 20t_1 + 5t_2 = 720 - 20.40 + 5.16 = 0$$

isto é, o saque será feito somente com oito notas de cinco;

b) para $t_1 = 40$ e $t_2 = 17$

$$z = 40 - t_1 = 40 - 39 = 0$$

$$y = -360 + 10t_1 - 2t_2 = -360 + 10.40 - 2.17 = 6$$

$$x = 720 - 20t_1 + 5t_2 = 720 - 20.40 + 5.17 = 5$$

ou seja, o saque será feito apenas com cinco notas de dois e seis notas de cinco;

c) para $t_1 = 40$ e $t_2 = 18$

$$z = 40 - t_1 = 40 - 39 = 0$$

$$y = -360 + 10t_1 - 2t_2 = -360 + 10.40 - 2.18 = 4$$

$$x = 720 - 20t_1 + 5t_2 = 720 - 20.40 + 5.18 = 10$$

então, o saque será feito apenas com dez notas de dois e quatro notas de cinco;

d) para $t_1 = 40$ e $t_2 = 19$

$$z = 40 - t_1 = 40 - 39 = 0$$

$$y = -360 + 10t_1 - 2t_2 = -360 + 10.40 - 2.19 = 2$$

$$x = 720 - 20t_1 + 5t_2 = 720 - 20.40 + 5.19 = 15$$

neste, o saque será feito apenas com quinze notas de dois e duas notas de cinco;

e) para $t_1 = 40$ e $t_2 = 20$

$$z = 40 - t_1 = 40 - 39 = 0$$

$$y = -360 + 10t_1 - 2t_2 = -360 + 10.40 - 2.20 = 0$$

$$x = 720 - 20t_1 + 5t_2 = 720 - 20.40 + 5.20 = 20$$

logo, o saque será feito somente com vinte notas de dois.

Contudo, somando todas as possibilidades verificadas, podemos concluir que é possível efetuar o saque de quinze modos distintos.

Problema 3. Com pacotes de papel higiênico contendo 8 unidades, de sabonete, 16 unidades, de pasta de dente, 12 unidades e de shampoo, 4 unidades. Quantas maneiras

distintas existem, para montar quites com 56 unidades, que contenham pelo menos um pacote de cada item?

Solução. Interpretando o problema, temos 8x + 16y + 12z + 4w = 56, onde, x representa o número de pacotes de papel higiênico, y o número de pacotes de sabonete, z o número de pacotes de pasta de dente e w o número de pacotes de shampoo. Em primeiro lugar, vamos analisar se a equação possui solução. Como mdc(8, 16, 12, 4) = 4 e 4 $\mid$ 56, o problema possui solução, devemos agora, encontrá-la, calculando sua solução geral.
Seja, 8x + 16y + 12z = p, então, p + 4w = 56, como mdc(1, 4) = 1 e 1 $\mid$ 56, temos

1 = 1.(- 3) + 4.1
56 = 1.(- 168) + 4.56

assim, p = - 168 + $4t_1$ e w = 56 - t_1 e como p e w devem ser números naturais, devemos ter 42 < t_1 < 56 com $t_1 \in \mathbb{Z}$. Escolhendo um valor conveniente para t_1, de maneira que o mdc(8, 16, 12) divida p, temos:

$$8x + 16y + 12z = p = - 168 + 4t_1$$

fazendo uma nova substituição em 8x + 16y + 12z = - 168 + $4t_1$, considerando 8x + 16y = p', segue que,

$$p' + 12z = - 168 + 4t_1$$

e como mdc(1, 12) = 1 e 1 $\mid$ (- 168 + $4t_1$) , qualquer que seja o valor de t_1 no intervalo encontrado, podemos continuar nossa procura pela solução, do seguinte modo:

1 = 1.(- 11) + 12.1
- 168 + $4t_1$ = 1.(- 11).(- 168 + $4t_1$) + 12.1.(- 168 + $4t_1$)
- 168 + $4t_1$ = 1.(1848 - $44t_1$) + 12.(- 168 + $4t_1$)

assim, p' = (1848 - $44t_1$) + $12t_2$ e z = (- 168 + $4t_1$) - t_2 e como p' e z devem ser inteiros positivos, devemos ter:

$(1848 - 44t_1) + 12t_2 > 0 \Leftrightarrow 12t_2 > -1848 + 44t_1 \Leftrightarrow t_2 > \frac{-1848 + 44t_1}{12} \Leftrightarrow t_2 > -154 + \frac{11}{3}t_1$

e

$$(-168 + 4t_1) - t_2 > 0 \Leftrightarrow -t_2 > -(-168 + 4t_1) \Leftrightarrow t_2 < -168 + 4t_1$$

que gera, $-154 + \frac{11}{3}t_1 < t_2 < -168 + 4t_1$ com $t_2 \in \mathbb{Z}$.

Prosseguindo, devemos escolher um valor adequado para t_2 de modo que o mdc(8, 16) divida p', temos então,

$$8x + 16y = p' = 1848 - 44t_1 + 12t_2$$

assim, como mdc(8, 16) = 8, vem:

$8 = 8.(-1) + 16.1 \Leftrightarrow 8.\left(\frac{1848 - 44t_1 + 12t_2}{8}\right) = 8.(-1).\left(\frac{1848 - 44t_1 + 12t_2}{8}\right) + 16.1.\left(\frac{1848 - 44t_1 + 12t_2}{8}\right) \Leftrightarrow 1848 - 44t_1 + 12t_2 = 8.\left(-231 + \frac{11}{2}t_1 - \frac{3}{2}t_2\right) + 16.\left(231 - \frac{11}{2}t_1 + \frac{3}{2}t_2\right)$

assim, temos:

$$x = -231 + \frac{11}{2}t_1 - \frac{3}{2}t_2 + \frac{16}{8}t_3 = -231 + \frac{11}{2}t_1 - \frac{3}{2}t_2 + 2t_3$$

$$y = 231 - \frac{11}{2}t_1 + \frac{3}{2}t_2 - t_3$$

com x e y números naturais, portanto, devemos proceder da seguinte maneira:

$-231 + \frac{11}{2}t_1 - \frac{3}{2}t_2 + 2t_3 > 0 \Leftrightarrow 2t_3 > 231 - \frac{11}{2}t_1 + \frac{3}{2}t_2 \Leftrightarrow t_3 > \frac{231}{2} - \frac{11}{4}t_1 + \frac{3}{4}t_2$

e

$231 - \frac{11}{2}t_1 + \frac{3}{2}t_2 - t_3 > 0 \Leftrightarrow -t_3 > -231 + \frac{11}{2}t_1 - \frac{3}{2}t_2 \Leftrightarrow t_3 < 231 - \frac{11}{2}t_1 + \frac{3}{2}t_2$

gerando, $\frac{231}{2} - \frac{11}{4}t_1 + \frac{3}{4}t_2 < t_3 < 231 - \frac{11}{2}t_1 + \frac{3}{2}t_2$ com $t_3 \in \mathbb{Z}$.

Depois de ter analisado todas as restrições de t_1, t_2 e t_3, encontramos:

$$42 < t_1 < 56$$

e

$$-154 + \frac{11}{3}t_1 < t_2 < -168 + 4t_1$$

e

$$\frac{231}{2} - \frac{11}{4}t_1 + \frac{3}{4}t_2 < t_3 < 231 - \frac{11}{2}t_1 + \frac{3}{2}t_2 \text{ com } t_1, t_2, t_3 \in \mathbb{Z}.$$

Para responder a pergunta do problema, analisaremos os seguintes casos:

I) Se $t_1 = 43$, temos $-154 + \frac{11}{3}.43 = 3{,}6667 < t_2 < -168 + 4.43 = 4$, assim como não existe $t_2 \in \mathbb{Z}$ neste caso, então $t_1 = 43$ não gera formas de montar o quite.

II) Se $t_1 = 44$, temos $-154 + \frac{11}{3}.44 = 7{,}3333 < t_2 < -168 + 4.44 = 8$, assim como não existe $t_2 \in \mathbb{Z}$ neste caso, então $t_1 = 44$ não gera formas de montar o quite.

III) Se $t_1 = 45$, temos $-154 + \frac{11}{3}.45 = 11 < t_2 < -168 + 4.45 = 12$, como não existe $t_2 \in \mathbb{Z}$, assim como nos casos anteriores, então $t_1 = 45$ não gera formas de montar o quite.

IV) Se $t_1 = 46$, temos $-154 + \frac{11}{3}.46 = 14{,}667 < t_2 < -168 + 4.46 = 16$, isto é, $t_2 = 15$, para determinar t_3, primeiro devemos analisar se o mdc(8, 16) = 8 divide $1848 - 44t_1 + 12t_2$, caso divida, continuaremos o processo, caso não divida, concluímos

o processo, sem encontrar formas de montar o quite para os respectivos valores de t_1 e t_2. Como 1848 – 44.46 + 12.15 = 4 e 8 ł 4 segue que t_1 = 46 não gera formas de montar o quite.

V) Se t_1 = 47, temos - 154 + $\frac{11}{3}$.47 = 18,333 < t_2 < - 168 + 4.47 = 20, isto é, t_2 = 19, para determinar t_3, faremos como no caso anterior, 1848 – 44.47 + 12.19 = 8 e como 8 $\mid$ 8, continuaremos o processo para encontrar valor de t_3, caso exista, logo, $\frac{231}{2} - \frac{11}{4}.47 + \frac{3}{4}.19 = 0{,}5 < t_3 < 231 - \frac{11}{2}.47 + \frac{3}{2}.19 = 1$ e como não existe $t_3 \in \mathbb{Z}$, t_1 = 47 não gera formas de montar o quite.

VI) Se t_1 = 48, temos - 154 + $\frac{11}{3}$.48 = 22 < t_2 < - 168 + 4.48 = 24, isto é, t_2 = 23 assim, 1848 – 44.48 + 12.23 = 12 e como 8 ł 12 segue que t_1 = 48 não gera formas de montar o quite.

VII) Se t_1 = 49, temos - 154 + $\frac{11}{3}$.49 = 25,667 < t_2 < - 168 + 4.49 = 28, verificando cada caso, temos:

a) para t_2 = 26, obtemos 1848 – 44.49 + 12.26 = 4 e como 8 ł 4 não é possível encontrar valor para t_3;

b) para t_2 = 27, obtemos 1848 – 44.49 + 12.27 = 16 e como 8 $\mid$ 16, segue que, $\frac{231}{2} - \frac{11}{4}.49 + \frac{3}{4}.27 = 1 < t_3 < 231 - \frac{11}{2}.49 + \frac{3}{2}.27 = 2$, que não gera valor para t_3.

Portanto, para t_1 = 49, não encontramos formas de montar o quite.

VIII) Se t_1 = 50, temos - 154 + $\frac{11}{3}$.50 = 29,333 < t_2 < - 168 + 4.50 = 32, verificando cada caso, temos:

a) para t_2 = 30, obtemos 1848 – 44.50 + 12.30 = 8 e como 8 $\mid$ 8 segue que, $\frac{231}{2} - \frac{11}{4}.50 + \frac{3}{4}.30 = 0{,}5 < t_3 < 231 - \frac{11}{2}.50 + \frac{3}{2}.30 = 1$, que não gera t_3;

b) para t_2 = 31, obtemos 1848 – 44.50 + 12.31 = 20 e como 8 ł 20 não é possível determinar valor para t_3.

Assim, t_1 = 50 não gera formas de montar o quite.

IX) Se t_1 = 51, temos - 154 + $\frac{11}{3}$.51 = 33 < t_2 < - 168 + 4.51 = 36, verificando cada caso, temos:

a) para t_2 = 34, obtemos 1848 – 44.51 + 12.34 = 12 e como 8 ł 12 não é possível encontrar valor para t_3;

b) para t_2 = 35, obtemos 1848 – 44.51 + 12.35 = 24 e como 8 $\mid$ 24 segue que, $\frac{231}{2} - \frac{11}{4}.51 + \frac{3}{4}.35 = 1{,}5 < t_3 < 231 - \frac{11}{2}.51 + \frac{3}{2}.35 = 3$, que gera t_3 = 2.

Portanto, para t_1 = 51, temos **uma** forma de montar o quite.

X) Se t_1 = 52, temos - 154 + $\frac{11}{3}$.52 = 36,667 < t_2 < - 168 + 4.52 = 40, verificando cada caso, temos:

a) para t_2 = 37, obtemos 1848 – 44.52 + 12.37 = 4 e como 8 ł 4 não é possível encontrar valor para t_3;

b) para t_2 = 38, obtemos 1848 – 44.52 + 12.38 = 16 e como 8 $\mid$ 16 segue que, $\frac{231}{2} - \frac{11}{4}.52 + \frac{3}{4}.38 = 1 < t_3 < 231 - \frac{11}{2}.52 + \frac{3}{2}.38 = 2$, que não gera valor para t_3.

c) para t_2 = 39, obtemos 1848 – 44.52 + 12.39 = 28 e como 8 ł 28 não é possível encontrar valor para t_3.

Logo, t_1 = 52 não gera formas de montar o quite.

XI) Se t_1 = 53, temos - 154 + $\frac{11}{3}$.53 = 40,333 < t_2 < - 168 + 4.53 = 44, verificando cada caso, temos:

a) para t_2 = 41, obtemos 1848 – 44.53 + 12.41 = 8 e como 8 $\mid$ 8 segue que, $\frac{231}{2} - \frac{11}{4}.53 + \frac{3}{4}.41 = 0{,}5 < t_3 < 231 - \frac{11}{2}.53 + \frac{3}{2}.41 = 1$, que não gera valor para t_3.

b) para t_2 = 42, obtemos 1848 – 44.53 + 12.42 = 20 e como 8 ł 20 não é possível encontrar valor para t_3.

c) para t_2 = 43, obtemos 1848 – 44.53 + 12.43 = 32 e como 8 $\mid$ 32 segue que, $\frac{231}{2} - \frac{11}{4}.53 + \frac{3}{4}.43 = 2 < t_3 < 231 - \frac{11}{2}.53 + \frac{3}{2}.43 = 4$, isto é, t_3 = 3.

Portanto, para $t_1 = 53$, temos **uma** forma de montar o quite.

XII) Se $t_1 = 54$, temos $-154 + \frac{11}{3}.54 = 44 < t_2 < -168 + 4.54 = 48$, verificando cada caso, temos:

a) para $t_2 = 45$, obtemos $1848 - 44.54 + 12.45 = 12$ e como $8 \nmid 12$ não é possível encontrar valor para t_3;

b) para $t_2 = 46$, obtemos $1848 - 44.54 + 12.46 = 24$ e como $8 \mid 24$ segue que, $\frac{231}{2} - \frac{11}{4}.54 + \frac{3}{4}.46 = 1{,}5 < t_3 < 231 - \frac{11}{2}.54 + \frac{3}{2}.46 = 3$, isto é, $t_3 = 2$;

c) para $t_2 = 47$, obtemos $1848 - 44.54 + 12.47 = 36$ e como $8 \nmid 36$ não é possível encontrar valor para t_3.

Assim, para $t_1 = 54$, temos **uma** forma de montar o quite.

XIII) Se $t_1 = 55$, temos $-154 + \frac{11}{3}.55 = 47{,}667 < t_2 < -168 + 4.55 = 52$, verificando cada caso, temos:

a) para $t_2 = 48$, obtemos $1848 - 44.55 + 12.48 = 4$ e como $8 \nmid 4$ não é possível encontrar valor para t_3;

b) para $t_2 = 49$, obtemos $1848 - 44.55 + 12.49 = 16$ e como $8 \mid 16$ segue que, $\frac{231}{2} - \frac{11}{4}.55 + \frac{3}{4}.49 = 1 < t_3 < 231 - \frac{11}{2}.55 + \frac{3}{2}.49 = 2$, que não gera valor para t_3;

c) para $t_2 = 50$, obtemos $1848 - 44.55 + 12.50 = 28$ e como $8 \nmid 28$ não é possível encontrar valor para t_3;

d) para $t_2 = 51$, obtemos $1848 - 44.55 + 12.51 = 40$ e como $8 \mid 40$ segue que, $\frac{231}{2} - \frac{11}{4}.55 + \frac{3}{4}.51 = 2{,}5 < t_3 < 231 - \frac{11}{2}.55 + \frac{3}{2}.51 = 5$, isto é, $t_3 = 3$ e $t_3 = 4$.

Então, para $t_1 = 55$, temos **duas** formas de montar o quite.

Contudo, basta somar todas as possibilidades acima para determinar o total de modos, M, de montar o quite. Logo,

$$M = 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 0 + 1 + 1 + 2 = 5.$$

Enfim, existem 5 modos distintos de montar o quite.

5 CONCLUSÃO

Neste trabalho apresentamos como é possível determinar soluções de uma Equação Diofantina que contenha várias variáveis, e também, mostramos que é possível a aplicação desse tipo de equação em situações do nosso cotidiano. Assim trabalhamos objetivamente o conceito mais geral de máximo divisor comum, da divisão euclidiana e de congruência e que os mesmos não se resumem apenas em descobrir qual é o maior divisor entre números inteiros, ou se dois números inteiros deixam o mesmo resto, mas também, que suas aplicabilidades, auxiliadas pelo algoritmo de Euclides, possuam uma significativa importância no processo de resolução das Equações Diofantinas. Contudo, deseja-se que o leitor seja capaz de identificar problemas, não só matemáticos, mas também de outros ramos do conhecimento, que possam ser modelados e em seguida solucionados por meio dessas equações. É possível reparar a contribuição de Diofanto para a história da matemática, contribuindo para a abertura de novos horizontes, e que sirva de incentivo e inspiração para um melhor entendimento da importância da matemática atual, em particular á álgebra, pois foi pioneiro no desenvolvimento da notação algébrica em que algumas operações eram representadas por suas abreviações. 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. Por isso a importância fundamental de se fazer um estudo acerca das equações, visando às aplicações das mesmas na resolução dos problemas algébricos. Diante do que foi abordado, percebemos a importância desse conteúdo que poderia estar no currículo do Ensino Médio, sabendo que a base necessária para trabalhá-lo é transmitida desde o Ensino Fundamental. O material pode ser desenvolvido a partir dos últimos anos do Ensino Fundamental, trabalhando às aplicações das Equações Diofantinas Lineares com duas variáveis. Já para o Ensino Médio, seriam abordadas as aplicações das Equações Diofantinas lineares com várias variáveis e a resolução por meio dos métodos fundamentais, tais como a fatoração, a indução matemática entre outros. Assim cabe ao professor explorá-lo da forma que lhe pareça mais adequado, de modo a levar os estudantes à investigação e à pesquisa por meio de situações-problema instigadoras e curiosas. Contudo, desejo que este trabalho possa contribuir para uma melhor compreensão do processo de ensino-aprendizagem

dos temas relativos à Teoria Elementar dos Números no Ensino Fundamental e Médio, em particular das Equações Diofantinas ajudando discentes e/ou docentes a aprimorar seus conhecimentos sobre este assunto.

REFERÊNCIAS

[1] Abramo Hefez, *Curso de Álgebra Volume 1*, IMPA, RJ (2013)

[2] Abramo Hefez, *Elementos de Aritmética*, SBM, RJ (2011)

[3] Abramo Hefez, *Iniciação à Aritmética*, SBM/IMPA/MEC, RJ (2009)

[4] Antônio Caminha Muniz Neto, *Tópicos de Matemática Elementar Volume 5 Teoria dos Números*, SBM, RJ (2012)

[5] Asger Aaboe, *Episódios da História Antiga da Matemática*, SBM, RJ (2013)

[6] BARROS, Alayde Ferreira dos Santos, *Equações Diofantinas e suas Aplicações*, Monografia (Especialista em Matemática), UESB-BA (1998)

[7] Carl B. Boyer, *História da Matemática*, Ed. Da Universidade de São Paulo, SP (1974)

[8] Carlos Correia de Sá e Jorge Rocha, *Treze Viagens pelo Mundo da Matemática*, SBM, RJ (2012)

[9] Clifford A. Pickover, *O Livro da Matemática: De Pitágoras à 57ª Dimensão, 250 Marcos da História da Matemática*, Librero, China (2011)

[10] Daniel Cordeiro de Morais Filho, *Um Convite à Matemática*, SBM, RJ (2013)

[11] Dmitri Fomin e Sergey Genkin e Ilia Itenberg, *Círculos Matemáticos A experiência Russa*, IMPA, RJ (2012)

[12] Edward R. Sheinerman, *Matemática Discreta*, Thomson, SP (2003)

[13] E. L. Lima e P. C. P. Carvalho e E. Wagner e A. C. Morgado, *A Matemática do Ensino Médio*, SBM, RJ (2009)

[14] F. B. Martinez e C. G. Moreira e N. Saldanha e E. Tengan, *Teoria dos Números: Um Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro*, IMPA, RJ (2013)

[15] Gilberto Geraldo Garbi, *A Rainha das Ciências*, Livraria da Física, SP (2010)

[16] Ian Stewart, *Incríveis Passatempos Matemáticos*, Zahar, RJ (2010)

[17] José Carlos Admo Lacerda, *Praticando a Aritmética*, Issonnarte, RJ (2013)

[18] José Plínio de Oliveira Santos, *Introdução à Teoria dos Números*, IMPA, RJ (2014)

[19] LA ROQUE, G. PITOMBEIRA, J.B., *Uma Equação Diofantina e Suas Resoluções*, Revista do Professor de Matemática, SP (1991)

[20] Paulo Ribenboim, *Números Primos Velhos Mistérios e Novos Recordes*, IMPA, RJ (2012)

[21] POMMER, Wagner Marcelo, *Equações Diofantinas Lineares: Um Desafio Motivador para Alunos de Ensino Médio*, Dissertação (Mestrado em Educação Matemática), PUC-SP (2008)

[22] Rogério S. Mol, *Introdução à História da Matemática*, CAED-UFMG, BH (2013)

[23] S. C. Coutinho, *Números Inteiros e Criptografia RSA*, IMPA & SBM, RJ (1997)

[24] Simon Singh, *O Último Teorema de Fermat*, Record, RJ (2005)

[25] Tatiana Roque, *História da Matemática: uma Visão Crítica, Desfazendo Mitos e Lendas*, Zahar, SP (2012)

[26] T. Andreescu e D. Andrica e I. Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser, NY (2010)

[27] Terence Tao, *Como Resolver Problemas Matemáticos*, SBM, RJ (2013)