UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

NÚMEROS PRIMOS E CONGRUÊNCIAS: TÓPICOS DE TEORIA DOS NÚMEROS NA EDUCAÇÃO BÁSICA

JOSÉ SIMÃO OLIVEIRA DOS SANTOS

CRUZ DAS ALMAS
Dezembro - 2015

NÚMEROS PRIMOS E CONGRUÊNCIAS: TÓPICOS DE TEORIA DOS NÚMEROS NA EDUCAÇÃO BÁSICA

JOSÉ SIMÃO OLIVEIRA DOS SANTOS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática, ofertado pelo Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Profº MsC. Gilberto da Silva Pina

CRUZ DAS ALMAS
Dezembro - 2015

FICHA CATALOGRÁFICA

S237n

Santos, José Simão Oliveira dos.
Números primos e congruências: tópicos de teoria dos números na educação básica / José Simão Oliveira dos Santos._ Cruz das Almas, BA, 2015.
61f.; il.

Orientador: Gilberto da Silva Pina.

Dissertação (Mestrado) – Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas.

1.Matemática – Estudo e ensino. 2.Matemática – Teoria dos números. 3.Números primos. I.Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas. II.Título.

CDD: 511

Ficha elaborada pela Biblioteca Universitária de Cruz das Almas - UFRB.

NÚMEROS PRIMOS E CONGRUÊNCIAS: TÓPICOS DE TEORIA DOS NÚMEROS NA EDUCAÇÃO BÁSICA

JOSÉ SIMÃO OLIVEIRA DOS SANTOS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática, ofertado pelo Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia, como requisito parcial para obtenção do título de Mestre em Matemática.

Banca Examinadora:

Orientador: Gilberto da Silva Pina
Profº MsC. Gilberto da Silva Pina (UFRB)

Membro: Maria Amélia de P. B. Hohlenwerger
Profª Drª. Maria Amélia de Pinho Barbosa Hohlenwerger (UFRB)

Membro: Yuri Tavares dos Passos
Profº MsC. Yuri Tavares dos Passos (UFRB)

Cruz das Almas, 17 de dezembro de 2015.

Aos meus pais,
à minha esposa, Rejiane e,
aos meus filhos, Lucas, Breno e Thaíc
com muito amor.

"A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."
Albert Einstein

Agradecimentos

Que bom chegar até aqui! Nada seria possível se não fosse da vontade Dele: Deus Pai Misericordioso, a quem primeiramente agradeço por me dar forças, saúde e permissão para que esse feito fosse realizado.

Agradeço, em especial, ao meu orientador professor Gilberto da Silva Pina que aceitou fazer parte desse trabalho, com sua generosidade e paciência.

A todo corpo docente do PROFMAT pela dedicação e incentivo nas horas difíceis. Em especial, aos professores Erikson e Gilberto que compartilharam conosco, vários momentos vividos, na maioria das disciplinas oferecidas.

Agradeço à Sociedade Brasileira de Matemática pela oportunidade concedida.

À CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela concessão da bolsa durante o curso.

A todos da banca examinadora por aceitar fazer parte e contribuir para este trabalho.

À minha família da qual muitas vezes me isolei para focar nos estudos.

Aos colegas de curso que sempre trouxeram motivação e fizeram parte dessa conquista, em especial a Leila e Alexandro pelos diversos feriados e fins de semanas compartilhados juntos estudando.

Aos meus alunos e colegas de trabalho pela compreensão da minha ausência em determinados momentos, especialmente ao professor Leonardo pelos incentivos constantes.

Enfim, a todos que colaboraram direta e indiretamente para que tudo ocorresse da melhor maneira possível, meus sinceros agradecimentos.

José Simão O. dos Santos

Resumo

Este trabalho propõe a abordagem de conceitos complementares sobre a teoria dos números na educação básica, como uma alternativa a corroborar na resolução de situações envolvendo tópicos sobre números primos e divisibilidade de inteiros, bem como, reafirmar a importância desse ramo da Matemática para o desenvolvimento de habilidades básicas primordiais ao estudo e compreensão de conceitos essenciais dessa ciência. Nesse contexto, serão apresentados os principais resultados sobre números primos, propriedades relevantes sobre a divisibilidade e a aritmética modular, a resolução de congruências lineares e equações diofantinas. Por fim, buscaremos apresentar resultados de propostas experimentais em sala de aula com a finalidade de verificação e sugestão prática de aplicabilidade da teoria proposta nesse projeto.

Palavras-chave: Educação básica, números primos, divisibilidade, congruências lineares.

Abstract

This work proposes the approach of complementary concepts about the numbers' theory in basic education, as an alternative to corroborate in the resolution of situations involving topics about prime numbers and divisibility of integers, as well as, reaffirm the importance of this branch of Mathematics for the development of basic skills primordial to the study and understanding of essential concepts this science. In this context, the main results will be presented about prime numbers, relevant properties about the divisibility and modular arithmetic, the resolution of linear congruences and diophantine equations. At last, we will search to show results of experimental proposals in classroom with the purpose of verification and practical suggestion the applicability of the theory proposed in this project.

Keywords: Basic education, prime numbers, divisibility , linear congruences.

Sumário

Lista de Figuras

Introdução

A abordagem sobre teoria dos números em Educação Básica, no tangente ao que se refere a conjunto dos números primos e divisibilidade, é feita de forma mecânica e superficial, e pouca relevância é dada a conceitos e propriedades necessárias à compreensão desse tema e de outros importantes em todo o percurso escolar do aluno. Proposições e teoremas imprescindíveis são poucos explorados ou quase que esquecidos, a exemplos do teorema fundamental da aritmética que, mesmo sendo utilizado para o cálculo do *máximo divisor comum (mdc)* e *mínimo múltiplo comum (mmc*), muitas das vezes fica implícito no processo e nenhuma associação é feita sobre A sua importância ao expressar todos os números inteiros maiores do que um, de forma semelhante, como produto de números primos.

Em relação às dificuldades apresentadas pelos estudantes, em Matemática, observamos que apenas uma pequena parte daqueles que concluíram o ensino fundamental e cursam o ensino médio, no país, apresentam habilidades necessárias à resolução de problemas relacionados ao seu nível de estudo e estão aptos a prosseguir no nível posterior (10 % em 2009; 12% em 2011 e 11% em 2013 dos concluintes do 9º ano), conforme dados da Prova Brasil [1] colhidos e apresentados pelo portal QEdu [2] . Esses argumentos e as experiências fortalecem a crença de que grande parte dos nossos estudantes não conseguem compreender as noções fundamentais às operações de aritmética dos inteiros para resolver problemas articulados a outras áreas da Matemática como a geometria e a álgebra. Por outro lado, também observamos que está cada vez mais presente a exploração de situações envolvendo equações diofantinas e aritmética modular nas avaliações externas, a exemplo das Olimpíadas Brasileiras de Matemática das Escolas Públicas (OBMEP), carecendo, o tema, de maior atenção por parte de professores e alunos da educação básica.

Acreditamos que a compreensão de conceitos complementares sobre aritmética dos núme-

[1] Avaliação, em larga escala, desenvolvidas pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep/MEC) para diagnóstico da qualidade do ensino oferecido pelo sistema educacional brasileiro.

[2] http://www.qedu.org.br/brasil/proficiencia.

ros inteiros poderá favorecer o desenvolvimento de habilidades e competências que serão o alicerce para potencializar toda a aprendizagem matemática, e permitir que o aluno aumente a sua capacidade de argumentar, conjecturar, generalizar e de investigar. Nesse trabalho, propomos o aprofundamento dos conhecimentos sobre a teoria dos números na educação básica por meio de estudo especial dos números primos e divisibilidade, destacando congruências e equações diofantinas como alternativas auxiliares na resolução de situações que envolvam cálculo de divisibilidade. Consideramos que essa iniciativa pode ser feita de forma diversificada, seja no momento sala de aula, como em atividades de reforço, ou estudos complementares em horário extra, e não discutimos aqui a melhor metodologia para sua aplicação. Apresentaremos uma sequência de atividades desenvolvidas, as quais qualificamos como oficinas, para mostrar os possíveis resultados verificados com determinado grupo de estudantes.

A estrutura desse trabalho está dividida em quatro capítulos subdivididos em seções. O primeiro deles faz uma abordagem preliminar contando fatos históricos do surgimento da teoria dos números, os principais percussores, desenvolvimento e perspectivas para a atualidade, além de relacionar o ensino dessa teoria nas escolas. O segundo capítulo é dedicado a apresentação de conceitos importantes sobre a teoria dos números como definições, proposições e teoremas demonstrados, algoritmos e outros resultados que constituirão o embasamento teórico às questões preteridas. No terceiro, serão descritas as atividades desenvolvidas para alcançar os objetivos pretendidos com essa proposta. Por fim, o quarto capítulo, está reservado às considerações finais sobre os resultados esperados e conclusões.

Esperamos despertar no leitor a curiosidade pelo tema para uma reflexão e disseminação das ideias centrais nesse texto.

Capítulo 1

Preliminares

NESTE capítulo abordaremos sobre fatos históricos que proporcionaram, ao longo dos séculos, o desenvolvimento desse importante ramo da Matemática e como tem sido tratado esse tema diante de sua importância para o desenvolvimento das ciências, e seu aprimoramento para o progresso nas diversas relações necessárias à sociedade atual.

1.1 Um pouco de história

Fatos que comprovam os primeiros estudos sobre números inteiros remontam a Antiguidade, através de documentos deixados pelos povos egípcios e babilônios.

As figuras mostram dois documentos antigos que chegaram até nós e que revelam esse interesse pelos números e a aritmética:

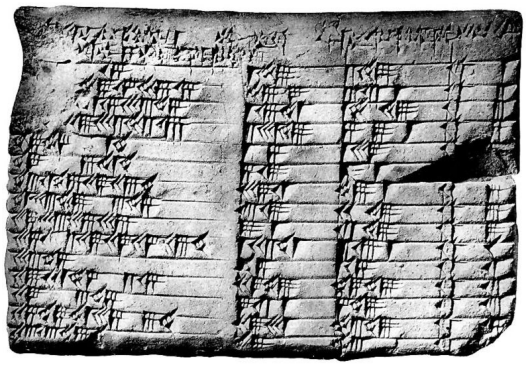

Figura 1.1: Plimptom 322 - Universidade de Columbia

Figura 1.2: Papiro Rhind

A primeira imagem [1] é do *Plimpton 322* (da Coleção G.A. Plimpton na Universidade de Columbia), uma tabuleta de argila escrita em 1800 a.C. composta por uma tabela de quatro colunas e 15 linhas de números em cuneiforme escrita do tempo. Nela está o que hoje é chamado trios pitagóricos, ou seja, inteiros a , b , c satisfazendo $a^2 + b^2 = c^2$. A outra figura [2] mostra parte do *Papiro de Rhind ou papiro de Ahmes*, um documento egípcio de cerca de 1650 a.C., onde um escriba de nome Ahmes detalha a solução de 80 problemas de aritmética, frações, cálculo de áreas, volumes, progressões, repartições proporcionais, regra de três simples, equações lineares, trigonometria básica e geometria.

Sautoy (2007), afirma que os números primos podem ter sido descobertos muito antes da Era Cristã:

> O primeiro indício impreciso do momento em que a humanidade se deu conta das qualidades especiais dos números primos é um osso datado de 6500 a.C., conhecido como o osso de Ishango, que foi descoberto em 1960 nas montanhas da África Central Equatorial. Nele estão inscritas três colunas contendo quatro série de entalhes. Em uma dessas colunas encontramos 11, 13, 17 e 19 entalhes, uma lista de todos os primos entre 10 e 20 (Sautoy, 2007, p.27).

As mais antigas referências gregas atribuem a *Tales de Mileto* (624 - 548 a.C) e a *Pitágoras de Samos* (580 - 500 a.C.) muitas descobertas matemáticas, mas nada que tenha documento

[1] Disponível em: <https://pt.wikipedia.org/wiki/Plimpton_322#/media/File:Plimpton_322.jpg> Acesso em out. 2015.

[2] Disponível em: <https://en.wikipedia.org/wiki/Rhind_Mathematical_Papyrus> Acesso out. 2015.

histórico. Os primeiros registros matemáticos datam, aproximadamente, o ano 300 a.C. quando *Euclides de Alexandria* escreveu o livro titulado de *"Os Elementos"*, aquela que foi a mais antiga e influente obra da Matemática grega deixada para nós [3]. Foi a partir dessa obra de Euclides que a Matemática passou a ser posta como ciência.

"Os Elementos" é uma obra, quase sempre, associada à geometria, mas dentre os treze livros que a compõe, três deles (Livro VII, VIII e IX) são dedicados a teoria dos números [3]. E, são neles que estão as mais importantes contribuições de Euclides para o desenvolvimento desse ramo da Matemática, como a prova da *infinitude dos números primos*, o resultado conhecido atualmente como o *teorema fundamental da aritmética*, o *algoritmo da divisão* e o *cálculo do máximo divisor comum* entre dois números, dentre outras que são utilizadas até hoje no estudo da divisibilidade. Não tão distante a essa época, outro matemático também merece destaque. Trata-se de *Diofanto de Alexandria* (séc. III a.C.) que escreveu o livro *"Arithmetica"* apresentando cerca de 150 problemas, dentre eles resoluções de equações com uma ou mais incógnitas de coeficientes e soluções inteiras [3].

Na nossa era a Aritmética voltou a ter espaço com o movimento conhecido como *Renascença*, um movimento europeu que revolucionou a arte, a ciência e a cultura, e que, mais tarde, alcançou a Matemática com a tradução para o latim do tratado *Aritmética*, de Diofanto, em 1575 por Regiomanto e, posteriormente, em 1621 *Bachet Méziriac* publicou uma tradução francesa dessa obra que promoveu grande transformação na história da Matemática, quando passam a ser divulgadas as demonstrações dos resultados, e propostos desafios entre os estudiosos. Aí, um nome ganha espaço na época, o jurista francês *Pierre Fermat* (1601 - 1665) [6]. Esse jurista foi atraído por um dos mistérios que tem atravessado séculos, desde Euclides até os dias atuais: descobrir uma fórmula para encontrar todos os números primos, e Fermat chegou a afirmar ter encontrado um padrão para descrever uma lista de números primos através da expressão $2^{2^n} + 1$. Foi responsável por vários resultados importantes para a evolução da Matemática como o *Pequeno Teorema de Fermat* para os números primos, e *o último teorema de Fermat* que afirma não haver soluções inteiras para a expressão $x^n + y^n$, para $n \geq 2$, só provado em 1995 pelo inglês *Andrew Wiles* [6]. Fermat tinha seus trabalhos divulgados por meio do padre *Marin Mersenne*(1588 - 1648), grande divulgador das descobertas científicas da época que, através dos contatos que mantinha com Fermat [6] [14], também foi influenciado para o interesse em encontrar uma fórmula que descrevesse os números primos levando-o a afirmar que $2^p - 1$ gerava números primos para valores de p iguais a $2, 3, 5, 7, 13, 19, 31, 67, 127, 257$. Lista parcialmente correta, já que foram omitidos valores $61, 89$ e 107 para p, e incluído indevidamente os

valores 67 e 257 que geram números compostos nessa expressão.

Em 1707 nasce aquele que foi considerado maior matemático de seu tempo: *Lehonard Euler (1707 - 1783)*, responsável pelas demonstrações de quase todos os resultados deixados por Fermat[6], incluindo a negação da fórmula acima para encontrar números primos, mostrando que era falsa para $n = 5$. Também estabeleceu teoremas importantes como aquele que recebe o seu nome. Antes de encerrar os relatos do século XVIII, não podemos esquecer *Cal F. Gauss* nascido na Alemanha em 1777, que publicou em 1801 o livro *"Disquisitiones Arithmetical"* sobre teoria dos números introduzindo os conceitos de congruência[14].

O século XX também chamou a atenção sobre os estudos desse segmento da Matemática, como pela já mencionada prova do último teorema de Fermat, e o aparecimento das máquinas de enigmas da segunda guerra mundial dando origem aos primeiros computadores. Esse avanço da tecnologia e da era digital que depende de códigos secretos para manter em sigilos as trocas de informações confidenciais nas diversas relações mantidas entre as pessoas abriu espaço para *criptografia*[3] baseada em chaves compostas por números primos escolhidos com centenas de casas decimais. Ela garantiu a comunicação através de códigos secretos onde apenas o receptor possa ter condições de decodificar a mensagem, já que depende da fatoração desses números. Essa tem sido uma das grandes aplicações da teoria dos números, da qual depende todo o sistema de comunicação universal.

1.2 Algumas reflexões sobre o ensino de teoria dos números nas escolas

A aritmética é parte integrante dos currículos de todos os países. Quando pensamos nela, logo associamos à ideia de números, quatro operações elementares, e na educação matemática os conceitos têm correspondido a relações de quantitativos sobre coleções de objetos, como afirma Lins e Gimenez (1997). Ainda, segundo os autores:

[3]Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário , o que a torna difícil de ser lida por alguém não autorizado.

> ...Tem se esquecido frequentemente que a aritmética inclui também: a) representações e significações diversas (pontos de referência e núcleos, que ampliam a ideia simples do manipulativo); b) análise do porquê dos algoritmos e divisibilidade (elementos conceituais); c) uso adequado e racional de regras (técnicas, destrezas e habilidades); e d) descobertas ou "teoremas" (descobertas, elaboração de conjecturas e processos de raciocínio) (Lins e Gimenez, 1997, p.33).

Referindo-se a proposta curricular expressa para o ensino médio nos parâmetros curriculares nacionais, pesquisadores [9] concluíram não haver nenhuma referência a conteúdos como equação diofantina, e que coleções de livros didáticos aprovados pelo Plano Nacional do Livro Didático (PNLD) também não continham indicação sobre o assunto, embora o autor destaque em seu texto situações que são concernentes ao tema como exemplo das equações de retas com ambas coordenadas inteiras.

Observamos que o tratamento dado a certos tópicos fundamentais na aritmética escolar, não contempla tamanha importância do assunto para o desenvolvimento da matemática e sua compreensão. Os estudos sobre a teoria dos números primos podem ser citados como exemplos, visto que princípios básicos como a infinitude desses números, a falta de um padrão que os definam, quando abordados, são feitos de forma superficial, e, que poderiam ser explorados com maior rigor apresentando argumentos acessíveis como as adaptações da prova do teorema de Euclides. Outra observação importante refere-se ao abandono às propriedades sobre divisibilidade de números inteiros, que são um alicerce para compreensão de toda esta teoria da divisibilidade que procede.

Em relação a conexão com outras áreas dentro da própria Matemática, Lins e Gimenez (1997) defende que haja uma coexistência entre a álgebra e a aritmética. Que a primeira fosse vista como aritmética falando de afirmações que envolvem números, operações e igualdades, enquanto a outra fosse vista como a álgebra, que constitua ferramenta parte do processo de organização da atividade humana, e não como ferramenta auxiliar, que precede os conhecimentos de outras áreas.

Sobre o *porquê promover uma ampliação desses conceitos na educação básica*, alguns autores defendem que constitui-se ferramentas essenciais para criar argumentação e promover investigação.

> ... a Teoria Elementar dos Números, ao ter como foco o estudo dos números inteiros, é um campo propício para desenvolvimento de atividades investigativas, pois a exploração de padrões e de relações numéricas, o uso da recursão e da indução matemática, envolvendo os inteiros, a divisibilidade e números primos estiveram e estão presentes na matemática e podem ser explorados nas atividades escolares, em qualquer nível (Resende, 2007, p.209).

Além disso, muitos temas abordados oportunizam o desenvolvimento de estratégias e competências, como afirma Pommer (2010) sobre as equações diofantinas.

> O tema das Equações Diofantinas Lineares permite articular, a partir da estratégia da tentativa e erro, outras estratégias de enfoque aritmético, que possibilitam a evolução para o uso da escrita algébrica, como condição otimizadora das condições dadas no enunciado (Pommer, 2010, p.2).

Queremos deixar claro que não estamos discutindo, nem esse é o propósito aqui, qual a melhor maneira de ensinar e aprender aritmética nas escolas, tampouco debater sua relação com a aplicabilidade no cotidiano do aluno, ou propor mudança curricular. Queremos apenas enfatizar, no ensino dessa área, a importância de priorizar os conceitos básicos inerentes a construção dessa teoria, os quais tem relação direta também com outras áreas como a álgebra e a geometria.

Finalizamos essa seção reafirmando a necessidade de uma maior atenção dada a tópicos pouco explorados na educação básica, de modo a permitir condições, ao aluno, de potencializar suas habilidades de criação, manipulação e escolha de estratégias adequadas à compreensão e resolução de problemas matemáticos, possibilitando superação das dificuldades apresentadas pelos alunos no processo de aprendizagem refletidos, atualmente, nos sistemas de avaliações de larga escala aos quais são submetidos.

Capítulo 2

Conceitos Importantes sobre a Teoria dos Números

ESTE capítulo será dedicado à abordagem de conceitos fundamentais ao desenvolvimento desse trabalho. Não será esgotada, aqui, toda a teoria sobre os conteúdos em destaque, mas serão apresentados tópicos necessários à fundamentação e compreensão do propósito estabelecido. Para isso, em todo o capítulo estaremos utilizando resultados, proposições, teoremas e demonstrações de autores consagrados no ramo da aritmética [6, 4, 13, 8, 5].

Ao longo deste trabalho, algumas demonstrações farão uso do Princípio da Indução Matemática. Por isso, abriremos o capítulo com sua apresentação.

Teorema 2.1. ***Princípio da Indução Matemática:***
Seja P(n) uma proposição associada a cada inteiro n e que satisfaz às duas seguintes condições:
(i) P(1) é verdadeira;
(ii) $\forall n$ *positivo, se P(n) é verdadeira então* $P(n+1)$ *é verdadeira.*
Nestas condições, a proposição P(n) é verdadeira para todo inteiro n positivo.

Demonstração*:*
Seja S o conjunto de todos os inteiros positivos n para os quais a proposição P(n) é verdadeira, isto é:
$S = \{n \in \mathbb{N}; P(n)$ *é verdadeira}*
Pela condição (i), P(1) é verdadeira e, portanto, $1 \in S$*. Pela condição (2), para todo inteiro positivo n, se* $n \in S$*, então* $n+1 \in S$*. Logo, o conjunto S satisfaz às condições (1) e (2) do "Princípio da indução finita" e, portanto,* $S = \mathbb{N}$*, isto é, a proposição P(n) é verdadeira para todo inteiro positivo n.*

2.1 Algumas noções sobre divisibilidade

NESTA seção apresentaremos algumas definições, teoremas e proposições que formarão a fundamentação e o embasamento necessários para alcançar os objetivos propostos nesse projeto.

2.1.1 Divisibilidade

Dados dois números inteiros a e b, diz-se que a divide b, e escrevemos $a|b$ quando existe um número inteiro c tal que $b = a \cdot c$. A negação será indicada por $a \nmid b$.

Quando $\boldsymbol{a}$ divide b, dizemos que a é um **divisor** ou um fator de b, ou, ainda, que b é um **múltiplo** de a.

Exemplo 2.1. $3|15$, *pois* $15 = 3 \cdot 5$;

Exemplo 2.2. $3 \nmid 10$, *pois não existe* $c \in \mathbb{Z}$ *tal que* $10 = 3 \cdot \boldsymbol{c}$.

Proposição 2.1. *Dados* $a, b, c \in \mathbb{Z}$, *temos que:*

i) $1 \mid a$, $a \mid a$ *e* $a|0$. *(Todo número inteiro é divisível por 1 e por si mesmo, e todo número inteiro divide* 0*).*
ii) *se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração*:*
i) *Consequências das igualdades* $a = a \cdot 1$, $a = 1 \cdot a$ *e* $0 = 0 \cdot a$.
ii) *Se* $a|b$ *e* $b|c$, *então existem* $k_1, k_2 \in \mathbb{Z}$, *tais que* $b = k_1 \cdot a$ *e* $c = k_2 \cdot b$. *Daí,*
$c = k_2 \cdot b = k_2 \cdot (k_1 \cdot a) = (k_1 \cdot k_2) \cdot a = k_3 \cdot a$, *onde* $k_3 = k_1 \cdot k_2$.

Proposição 2.2. *Sejam* $a, b \in \mathbb{Z}$.

i) *Se* $a|1$, *então* $a = \pm 1$.
ii) *Se* $a|b$, $b|a$ *então* $a = \pm b$.

***Demonstração**:*
***i)** De fato, se $a|1$, existe $k \in \mathbb{Z}$, tal que $1 = a \cdot k$. Daí, temos que $a = 1$ e $k = 1$, ou que $a = -1$ e $k = -1$, isto é, $a = \pm 1$.*
***ii)** Com efeito, se $a|b$ exite $q \in \mathbb{Z}$ tal que $b = a \cdot q$; e, se $b|a$ existe $q_1 \in \mathbb{Z}$ tal que $a = b \cdot q_1$. Daí, segue que $a \cdot b = a \cdot b \cdot q \cdot q_1$, logo $a = aq \cdot q_1$ o que implica $q \cdot q_1 = 1$, e por sua vez implica que $q_1|1$, isto é, $q_1 = \pm 1$. Portanto, de $a = b \cdot q_1$ resulta que $a = \pm b$.*

Proposição 2.3. *Sejam $a, b \in \mathbb{Z}$. Se $a|b$, com $b \neq 0$, então $|a| \leq |b|$.*

***Demonstração**:*
$a|b$, $b \neq 0$ implica que $b = a \cdot k$, $k \in \mathbb{Z}$ e $k \neq 0$. Segue que $|b| = |a| \cdot |k|$. Como $k \neq 0$, temos $|k| \geq 1$ e, portanto, $|b| \geq |a|$.

Proposição 2.4. *Sejam $a, b, c, d \in \mathbb{Z}$. Se $a \mid b$ e $c|d$, então $a \cdot c \mid b \cdot d$.*

***Demonstração**:*
Se $a|b$ e $c|d$, então existem $k, t \in \mathbb{Z}$ tais que $b = k \cdot a$ e $d = t \cdot c$. Daí,
$b \cdot d = (k \cdot a) \cdot (t \cdot c) = (k \cdot t) \cdot (a \cdot c)$. Logo, $a \cdot c|b \cdot d$.

Proposição 2.5. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então*
$a|b \iff a|c$

***Demonstração**:*
Supondo que $a|(b + c)$, existe $k \in \mathbb{Z}$ tal que $b + c = k \cdot a$. Se $a|b$, existe $t \in \mathbb{Z}$ tal que $b = t \cdot a$. Das duas igualdades concluímos que $t \cdot a + c = k \cdot a$, e, daí, segue que $c = (k - t) \cdot a$, logo $a|c$;
Analogamente, se $a|c$, existe $q \in \mathbb{Z}$ tal que $c = q \cdot a$. Daí, de $b + c = k \cdot a$ temos $b + q \cdot a = k \cdot a$, que implica $b = (k - q) \cdot a$, logo $a|b$.
Por outro lado, se $a|(b - c)$ e $a|b$, pelo caso anterior, $a| - c$, o que implica $a|c$. De forma análoga, mostra-se a implicação contrária, ou seja, que $a|b$.

Proposição 2.6. *Se $a, b, c \in \mathbb{Z}$ são tais que $a|b$ e $a|c$, então $a|(x \cdot b + y \cdot c)$, $\forall\ x, y \in \mathbb{Z}$.*

***Demonstração**:*
Se $a|b$ e $a|c$, existem $q, t \in \mathbb{Z}$ tais que $b = q \cdot a$ e $c = t \cdot a$. Logo,$\forall\ x, y \in \mathbb{Z}$
$x \cdot b + y \cdot c = x \cdot (q \cdot a) + y \cdot (t \cdot a) = (x \cdot q + y \cdot t) \cdot a$,
o que prova o resultado.

Proposição 2.7. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tem-se que $a - b$ divide $a^n - b^n$.*

***Demonstração**:*
Por indução sobre n, tem-se:
A afirmação é verdadeira para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.
Suponhamos que a afirmação $a - b|a^n - b^n$ seja verdadeira para algum $n \in \mathbb{N}$.
Escrevemos $a^{n+1} - b^{n+1} = a \cdot a^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n)$.
Como $a - b|a - b$ e, pela hipótese de indução, $a - b|a^n - b^n$, segue da proposição anterior (2.6), e da igualdade acima, que $a - b|a^{n+1} - b^{n+1}$. Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$.

Proposição 2.8. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tem-se que $a + b$ divide $a^{2n-1} + b^{2n-1}$.*

***Demonstração**:*
Por indução sobre n, temos que:
A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^1 + b^1 = a + b$.
Suponhamos que a afirmação $a + b|a^{2n-1} + b^{2n-1}$ seja verdadeira para algum $n \in \mathbb{N}$.
Escrevemos $a^{2(n+1)-1} - b^{2(n+1)-1} = a^2a^{2n-1} - b^2a^{2n-1} + b^2a^{2n-1} + b^2b^{2n-1} = (a^2 - b^2)a^{2n-1} + b^2(a^{2n-1} + b^{2n-1})$.
Como $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$ e, pela hipótese de indução, $a + b|a^{2n-1} + b^{2n-1}$, segue da igualdade acima e da proposição (2.6) que $a + b|a^{2(n+1)-1} + b^{2(n+1)-1}$. Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$.

Proposição 2.9. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.*

***Demonstração**:*
Por indução sobre n, temos que:
A afirmação é verdadeira para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$.

Suponhamos que a afirmação $a+b|a^{2n}-b^{2n}$ seja verdadeira para algum $n \in \mathbb{N}$.
Escrevemos $a^{2(n+1)}-b^{2(n+1)} = a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} = (a^2-b^2)a^{2n} + b^2(a^{2n}-b^{2n})$.
Como $a+b$ divide $a^2-b^2 = (a+b)(a-b)$ e, pela hipótese de indução, $a+b|a^{2n}-b^{2n}$, segue da igualdade acima e da proposição (2.6) que $a+b|a^{2(n+1)}-b^{2(n+1)}$.
Logo, a afirmação é verdadeira para todo $n \in \mathbb{N}$.

2.1.2 Divisão Euclidiana

É interessante observar que, em sua obra, Euclides só tratava de números positivos quando se referia aos números inteiros.

Teorema 2.2. ***Divisão Euclidiana:***

Se a e b são dois números inteiros, com $b \neq 0$, então existem e são únicos os inteiros q e r que satisfazem as condições:

$$a = b \cdot q + r \qquad\qquad 0 \leq r < |b| \tag{2.1}$$

***Demonstração**:*
Consideremos um conjunto K formado por todos os números inteiros não negativos da forma $a-bx$, com $x \in \mathbb{Z}$, ou seja, $K = \{a-bx | x \in \mathbb{Z},\ a-bx \geq 0\}$. Note que $b > 0$, logo $b \geq 1$, e para $x = -|a|$, resultam que:
$a - bx = a + b|a| \geq a + |a| \geq 0$. Segue que K não é vazio, assim, pelo Princípio da Boa Ordenação [1], K possui elemento mínimo $r \geq 0$ e, $r = a - bq$ ou $a = bq + r$, com $q \in \mathbb{Z}$.

E, além do mais, $r < b$, pois caso contrário ter-se-ia
$0 \leq r - b = (a - bq) - b = a - b(q+1) < r$, e r não seria elemento mínimo de K, o que contradiz a afirmação acima.
Unicidade: suponhamos que existam outros dois números inteiros r_1 e q_1, tais que $a = b \cdot q_1 + r_1$ e $0 \leq r_1 < b$, então $a = b \cdot q_1 + r_1 = bq + r$, daí $r_1 - r = (q - q_1) \cdot b$, e portanto, $|b| \cdot |q - q_1| = |r_1 - r|$.
Mas, $-b < -r \leq 0$ e $0 < r_1 < b$, o que implica $-b < r_1 - r < b$, ou seja $|r_1 - r| < b$, Logo, $|b| \cdot |q - q_1| = |r_1 - r| < |b|$, o que só ocorre se $q_1 = q$ e consequentemente, $r = r_1$.

Exemplo 2.3. *Encontre o quociente (q) e o resto (r) da divisão de 17 por 5.*

[1] Principio da Boa Ordenação: em todo subconjunto $K \in \mathbb{N}$, existe $t \in K$ tal que $t \leq x$, $\forall x \in K$, isto é, t é elemento mínimo de K.

Solução:
$17 = 5 \cdot 3 + 2$. *Logo,* $q = 3$ *e* $r = 2$.

2.1.3 Divisor comum

Dados dois números inteiros a e b, não simultaneamente nulos, dizemos que o número inteiro $d \in \mathbb{Z}$ é um *divisor comum* de a e b se $d|a$ e $d|b$.

Exemplo 2.4. *O número* 4 *é divisor comum de* 12 *e* 20, *pois* $12 = 4 \cdot 3 \quad e \quad 20 = 4 \cdot 5$.

2.1.4 Máximo divisor comum (mdc) e o Algorítmo de Euclides

Definição 2.1. *Um número natural d é um* ***máximo divisor comum*** *(mdc) de a e b, não simultaneamente nulos, se:*

i) d é um divisor comum de a e de b, e

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

ii') Se c é um divisor comum de a e de b, então $c|d$.
O mdc de dois números a e b quando existe é único e será denotado por (a, b).

Exemplo 2.5. *O número* 5 *é o máximo divisor comum de* 15 *e* 20, *indicamos* $(15, 20) = 5$.

Para todo inteiro a não nulo é imediato que:
$(0, a) = |a|$;
$(a, a) = |a|$;
$(1, a) = 1$.
Se $a|b$ então $(a, b) = |a|$.

E, para todo $b \in \mathbb{Z}$, tem-se:

$$a|b \iff (a,b) = |a| \tag{2.2}$$

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

A seguir, enunciaremos um importante resultado dado por Euclides, cerca de 300 a.C., muito útil para calcular o mdc de dois números inteiros quaisquer. Logo após, um caso mais elementar que justificará o Algorítmo, também criado por Euclides, para expressar esse mesmo mdc de dois inteiros.

Lema 2.1 (Lema de Euclides)**.** *Sejam a, b, c e $n \in \mathbb{Z}$. Se existe $(a, b - n \cdot a)$, então (a,b) existe e $(a,b) = (a, b - n \cdot a)$.*
Demonstração:
Seja $d = (a, b - n \cdot a)$. Como $d|a$ e $d|(b - n \cdot a)$, segue que d divide $b = b - n \cdot a + n \cdot a$. Logo, d é divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c|d$. Isso prova que $d = (a,b)$.

Como resultado imediato podemos enunciar o seguinte lema:

Lema 2.2. *Se $a = bq + r$, então $(a,b) = (b,r)$.*

***Demonstração**:*
Se $(a,b) = d$, então $d|a$ e $d|b$, o que implica $d|(a - bq) = r$, ou seja, d é divisor comum de b e r.
Se c é um divisor comum de b e r, então $c|bq + r = a$, ou seja, c é um divisor de a e b e, daí, $c \leq d$. Logo, $(b,r) = d$.

Exemplo 2.6. *Calcular o mdc de 117 e 35.*
$117 = 3 \cdot 35 + 12$
$35 = 2 \cdot 12 + 11$
$12 = 1 \cdot 11 + 1$

$11 = 11 \cdot 1 + 0$

Logo, $(117, 35) = (35, 12) = (12, 11) = (11, 1) = (1, 0) = 1$

O Algoritmo de Euclides ou processo das divisões sucessivas:

Dados a, $b \in \mathbb{N}$, suponhamos que $a > b$. Pela aplicação repetida da divisão euclidiana, escrevemos as seguintes igualdades:

$a = bq_1 + r_1, \qquad 0 < r_1 < b$

$b = r_1q_2 + r_2, \qquad 0 < r_2 < r_1$

$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2$

$r_2 = r_3q_4 + r_4, \quad 0 < r_4 < r_3$

$\ldots \qquad\qquad \ldots$

Como os restos $r_1, r_2, r_3, r_4, ...$ são inteiros positivos tais que $b > r_1 > r_2 > r_3 > r_4 > ...$ e existem apenas $b - 1$ inteiros positivos menores do que b, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, isto é, tem-se que:
$r_{n-2} = r_{n-1} \cdot q_n + r_n, \qquad 0 < r_n < r_{n-1}$
$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}, \qquad r_n = 0$
O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o mdc de a e b, ou seja, $(a, b) = r_n$, já que pelo lema anterior, $(a, b) = (b, r) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$.

É utilizado o seguinte dispositivo para realização das divisões:

	q_1	q_2	q_3		q_{n+1}	q_n
a	b	r_1	r_2	...	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	

Exemplo 2.7. *Calcular o mdc de 117 e 35.*

	3	3	1	11
117	35	12	11	1
12	11	1	0	

Portanto, $(117, 35) = 1$.

Assim, o Algoritmo de Euclides também nos fornece o mdc de a e b como uma combinação linear de dois números. Essa combinação linear é o resultado do teorema seguinte.

Teorema 2.3 (Bachet-Bézout)**.** *Seja d o máximo divisor comum de a e b, então existem inteiros n_0 e m_0 tais que $d = m_0 \cdot a + n_0 \cdot b$.*

Demonstração:
Seja S o conjunto de todas as combinações lineares $(m \cdot a + n \cdot b)$, onde m e n são inteiros. Este conjunto contém, claramente, números negativos, positivos e também o zero. Vamos escolher n_0 e m_0 tais que $c = n_0 \cdot a + m_0 \cdot b$ seja o menor inteiro positivo pertencente ao conjunto S. Vamos provar que $c|a$ e $c|b$. Como as demonstrações são similares, mostraremos apenas que $c|a$. A prova é por contradição. Suponhamos que $c \nmid a$. Neste caso, existem q, r tais que $a = q \cdot c + r$, com $0 < r < c$. Portanto, $r = a - q \cdot c = a - q(n_0 \cdot a + m_0 \cdot b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in S$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de S. Logo, $c|a$ e de forma análoga se prova que $c|b$.
Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$ e, portanto, $c = n_0 \cdot a + m_0 \cdot b = n_0 \cdot k_1 \cdot d + m_0 \cdot k_2 \cdot d = d \cdot (n_0 \cdot k_1 + m_0 \cdot k_2)$ o que implica $d|c$. De $d|c$, temos que $d \leqslant c$ (ambos positivos) e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = c = n_0 \cdot a + m_0 \cdot b$.

Veja no exemplo anterior que:
$1 = 12 - 1 \cdot 11$
$11 = 35 - 2 \cdot 12$
$12 = 117 - 3 \cdot 35$
Comparando as expressões se chega a $1 = 3 \cdot 117 - 10 \cdot 35$.
Ou seja, temos $m_0 = 3$ *e* $n_0 = -10$.

Teorema 2.4 (Euclides)**.** *Sejam a, b e c números inteiros. Se $a|b \cdot c$ e $(a, b) = 1$, então $a|c$.*

***Demonstração**:*
$a|b \cdot c$, implica que existe $t \in \mathbb{Z}$ tal que $b \cdot c = a \cdot t$. E, se $(a, b) = 1$, então existem x e $y \in \mathbb{Z}$, tais que $xa + yb = 1$.
Multiplicando por c ambos os lados da igualdade acima, tem-se que $c = xac + ybc$, substituindo bc por at nessa última igualdade, resulta $c = xac + yat = a(xc + yt)$ e, portanto, $a|c$.

2.1.5 Mínimo múltiplo comum (mmc)

Um número inteiro é múltiplo comum de dois números naturais se ele é, simultaneamente, múltiplo de ambos os números.
Diremos que um número natural m é **mínimo múltiplo comum (mmc)** dos números inteiros a e b, ambos não nulos, se atender às condições:
(i) m é múltiplo comum de a e b; e
(ii) se c é um múltiplo de comum de a e b, então $m|c$.

Notação: $[a, b]$ ou mmc (a, b).

2.2 Tópicos importantes sobre números primos

Nesta seção abordaremos alguns tópicos importantes sobre os números primos. Números que fascinam matemáticos de todos os tempos, os quais Sautoy (1997) chama de átomos da aritmética por gerar todos os outros números inteiros. Apresentaremos a sua definição, alguns fatos, proposições, e o teorema fundamental da aritmética, que serão necessários à compreensão dos conteúdos abordados.

Definição 2.2. ***Número Primo***
Um número natural $p > 1$ é dito ***número primo*** *se ele só possui como divisores positivos o número* 1 *e ele próprio.*
São exemplos de primos os números 2, 3, 11, 29. Já os números maiores que 1 que não são primos serão ditos compostos, como 6, 10 e 27.

Consequências da definição: Dados dois números primos p, q e um inteiro a, qualquer:

i) Se $p|q$, então $p = q$.
De fato, se $p|q$, como q é primo, tem-se $p = 1$ ou $p = q$. Mas, p é primo, logo $p > 1$, o que implica $p = q$.

ii) Se $p \nmid a$, então $(p, a) = 1$.
De fato, se $(p, a) = d$, tem-se que $d|p$ e $d|a$. Como p é primo, $d = p$ ou $d = 1$. Mas, $d \neq p$, pois $p \nmid a$, resulta que $d = 1$.

Proposição 2.10. *Sejam os números inteiros a, b, p, com p primo. Se $p|a \cdot b$, então $p|a$ ou $p|b$.*

***Demonstração**:*
Se $p|a$, nada há que demonstrar, e se, ao invés, $p \nmid a$, então $(p, a) = 1$. Logo, pelo teorema anterior (Euclides), concluímos que $p|b$.

Teorema 2.5 (TEOREMA FUNDAMENTAL DA ARITMÉTICA - (TFA)). *Todo número natural n maior que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto*

de números primos.

***Demonstração**:*
Se n é primo não há o que demonstrar. Suponhamos n composto. Seja $p_1(p_1 > 1)$ *o menor dos divisores positivos de n. Afirmamos que* p_1 *é primo, pois caso contrário existiria* $p, 1 < p < p_1$ *com* $p|n$*, contradizendo a escolha de* p_1*. Logo,* $n = p_1 \cdot n_1$*.*
Se n_1 *for primo a prova se completa. Se* n_1 *não é primo, tomamos* p_2 *como o menor fator de* n_1*. Pelo argumento anterior,* p_2 *é primo e temos que* $n = p_1.p_2.n_2$*.*
Repetindo esse processo obtém-se uma sequência decrescente de inteiros positivos $n_1, n_2, \cdots, n_r$*. Como todos esses inteiros são maiores do que* 1*, esse procedimento deve terminar. Como os primos da sequência* $p_1, p_2, \cdots, p_k$ *não são, necessariamente, distintos, n terá, em geral, a forma:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \quad \cdots \quad p_k^{\alpha_k}$$

Unicidade: Por indução em n, tem-se para $n = 2$ *que a afirmação é verdadeira. Assumindo, que é válida para todos os inteiros maiores do que* 1 *e menores do que n, provamos que ela é válida para n. De fato, se n é primo não há o que provar. Suponhamos que n é composto e que admite duas fatorações,*
$n = p_1 \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_r$*.*
Devemos provar que $s = r$ *e que cada* p_i *é igual a algum* q_j*. Como* p_1 *divide o produto* $q_1 \cdot q_2 \cdots q_r$ *ele divide pelo menos um dos fatores* q_j*. Sem perda de generalidade, podemos supor que* $p_1|q_1$*. Como são ambos primos, isto acarreta em* $p_1 = q_1$*. Logo,* $(n/p_1) = p_2 \cdots p_s = q_2 \cdots q_r$*. Como* $1 < n/p_1 < n$ *a hipótese de indução leva a concluir que as duas fatorações são idênticas, isto é,* $s = r$ *e, a menos da ordem, as fatorações* $p_1 \cdot p_2 \cdots p_s$ *e* $q_1 \cdot q_2 \cdots q_r$ *são iguais.*

É importante destacarmos que a decomposição de números naturais em fatores primos torna-se, de certo modo, impossível quando se tem números com quantidade de algarismos extremamente grande, o que levaria muitos anos com o processo manual e não suportado, até então, pelas capacidades dos atuais processadores nos mais avançados computadores existentes. Esse tem garantido a eficiência dos métodos de *criptografia* baseada em números primos.

Proposição 2.11. *Seja* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *um número natural escrito em sua forma fatorada. Se* n_0 *é um divisor positivo de n, então*

$n_0 = p_1^{\beta_1} \cdots p_r^{\beta_r}$, *onde* $0 \leq \beta_i \leq \alpha_i$, *para* $i = 1, \cdots r$.

Demonstração:
Seja n_0 um divisor positivo de n e seja p^β a potência de um primo p que figura na decomposição de n_0 em fatores primos. Como $p^\beta | n$, segue que p^β divide algum $p_i^{\alpha_i}$ por ser primo com os demais $p_j^{\alpha_j}$, e, consequentemente, $p = p_i$ e $\beta \leq \alpha_i$.

Teorema 2.6. *Se dois números inteiros positivos a e b possuem as fatorações*

$$a = \pm p_1^{\alpha_1} \quad \cdots \quad p_n^{\alpha_n} \qquad e \qquad b = \pm p_1^{\beta_1} \quad \cdots \quad p_n^{\beta_n}$$

então o máximo divisor comum de a e b é dado por $(a, b) = p_1^{\lambda_1} \cdots p_n^{\lambda_n}$, onde $\lambda_i = min\{\alpha_i, \beta_i\}$, $i = 1, \cdots, n$.

Demonstração:
Pela proposição anterior (2.11), é claro que $p_1^{\lambda_1} \cdots p_n^{\lambda_n}$ é um divisor comum de a e b. Seja c um divisor comum de a e b; então, temos que $c = \pm p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$, onde $\varepsilon_i \leq min\ \{\alpha_i, \beta_i\}$, $i = 1, \cdots, n$. Como cada $p_i^{\varepsilon_i} | p_i^{\lambda_i}$, pois $\varepsilon_i \leq \lambda_i$, segue que $c | p_1^{\lambda_1} \cdots p_n^{\lambda_n}$, $i = 1, \cdots, n$.

2.2.1 Distribuição dos números primos

Quando é apresentado o conjunto de números primos para alguém, uma das primeiras perguntas que surge é a seguinte: quantos são os números primos? Quem respondeu a essa pergunta foi nada menos que Euclides no Livro IX de *Os Elementos*, por volta de 300 a.C.. Esse fato resultou no seguinte teorema:

Teorema 2.7 (Teorema de Euclides). *Existem infinitos números primos.*

Demonstração
Euclides deu a seguinte prova para esse resultado, usando a técnica da redução ao absurdo.
Suponhamos que exista apenas um número finito de números primos $p_1, p_2, \cdots, p_r$. Tomando o número natural $n = p_1 \cdot p_2 \cdot \cdots \cdot p_r + 1$, pelo teorema (2.5), o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \cdots, p_r$ e, consequentemente, divide o produto, $p_1 \cdot p_2 \cdot \cdots \cdot p_r$. Mas

isto implica que p divide 1, o que é uma contradição.

Outra pergunta pertinente é sobre a determinação dos números primos entre os dispostos em uma lista ordenada com os números naturais. Sobre essa questão, Eratóstenes (cerca de 230 a.C.) desenvolveu um método prático o qual é chamado de *Crivo de Eratóstenes*, em sua homenagem, que permite determinar todos os números primos até certa ordem, porém não muito eficiente pra ordens muito elevadas devido ser um método exaustivo [6]. Esse método consiste em escrever numa tabela em ordem crescente todos os números naturais iniciando do 2 até o número da ordem n que se quer determinar os primos. A seguir são riscados todos os múltiplos dos números primos da lista, a começar pelos múltiplos de 2, depois todos os múltiplos de 3, depois de 5, e assim sucessivamente. Mas quando saber se já pode parar? O Teorema a seguir dá uma resposta para esse questionamento.

Teorema 2.8. *Se um número natural $n > 1$ é composto, então n possui, necessariamente, um fator primo $p \leq \sqrt{n}$.*

***Demonstração**:*

Sendo n composto então $n = n_1 \cdot n_2$ onde $1 < n_1 < n$, e $1 < n_2 < n$. Sem perda de generalidade suponhamos $n_1 \leq n_2$. Notamos que, $n_1 \leq \sqrt{n}$, pois caso contrário teríamos $n = n_1 \cdot n_2 > \sqrt{n} \cdot \sqrt{n} = n$, o que é uma contradição. Logo, pelo TFA, n_1 possui algum fator primo p, tal que $p \leq \sqrt{n}$. Como p, sendo um fator de n_1, também p é um fator de n, conclui-se a demonstração.

Assim, além de determinar quando parar o método de eliminação de primos no Crivo de Eratóstenes, esse teorema é um teste de primalidade que fornece um método para saber se um número é primo ou não. Basta apenas testar a divisibilidade de um número natural $n > 1$ pelos primos $p \leq \sqrt{n}$.

Exemplo 2.8. *Testar se o número 127 é primo.*

Observa-se que $11 < \sqrt{127} < 12$. Logo, os primos que não excedem a $\sqrt{127}$ são 2, 3, 5, 7 e 11. Como nenhum deles é divisor de 127, tem-se que o número 127 é primo.

Exemplo 2.9. *Determinar todos os números primos menores que 45.*

Os primos menores que $\sqrt{45}$ são 2, 3 e 5. Logo, pelo teorema acima deve-se riscar no Crivo de Eratóstenes todos os números que são múltiplos desses primos, os que sobrarem na lista serão primos procurados. Assim, na lista

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45.

Riscamos: inicialmente, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42 e 44, que são os múltiplos de 2; a seguir, os múltiplos de 3, isto é: 9, 15, 21, 27, 33, 39, 45 (nota-se: 45 não é primo); por fim, os múltiplos de 5 que são os números 25 e 35.
Restaram os primos procurados: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 e 43.

Percebe-se que se trata de processos muito exaustivos e inviáveis quando o número n considerado é muito grande.

2.2.2 Em busca de padrões para os primos: Fermat e Mersenne

Autores [6, 14] destacam que foram muitas as tentativas para encontrar uma fórmula, regularidade, ou padrão que descrevesse todos os números primos ou ao menos uma lista deles. Essas especulações possibilitaram, ao longo da história, o surgimento de grandes nomes da matemática e de muitos problemas que se traduziram em conjecturas e hipóteses ainda esperando por soluções, cujos temas e discussões vão muito além do propósito desse trabalho. Dentre os grandes feitos, destacaremos as descobertas realizadas pelo jurista francês *Pierre Fermat (1601 - 1665)* e seu contemporâneo, e interlocutor, o padre *Marin Mersenne (1588 — 1648)*, que apresentaram, cada um, fórmulas que acreditavam expressar padrões para listar números primos, as quais discutiremos a seguir.
Em suas tentativas, Fermat afirmou ter encontrado uma fórmula para escrever uma lista com

todos os números primos e, para isso, acreditava que eles eram gerados pela forma $F_n = 2^{2^n} + 1$, o que ficou conhecido como **números de Fermat**. Talvez, pelo fato de o tamanho dos números de Fermat aumentar muito rapidamente, ele não tenha verificado o quinto deles, que possui dez algarismos, não ser um número primo. Esse fato só foi comprovado mais tarde em 1732, quando *Leonhard Euler(1707 - 1783)* mostrou que $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$.
Os números de Fermat primos são conhecidos como os **primos de Fermat**. Acerca desse fato existe uma importante conjectura sobre o número de primos de Fermat: os primos de Fermat são em número finito [6].
Grande divulgador das descobertas, Marin Mersenne também ficou entusiasmado pela busca de um padrão para os números primos e, mesmo não conseguindo encontrar um método padrão que gerasse todos os números primos, ele descreveu uma fórmula mais eficaz na busca de primos do que a criada por Fermat [14]. Os números descritos pela fórmula $M_p = 2^p - 1$, sendo p um número primo, são conhecidos como **números de Mersenne**. Destes, os que representam números primos são chamado de **primos de Mersenne**. Ele chegou a afirmar que para os valores de p até 257 eram primos aqueles atribuídos os valores $2, 3, 5, 7, 13, 19, 31, 67, 127, 257$, omitindo nessa lista os valores $61, 89$ e 107 de p e, incluindo valores indevidos 67 e 257.

> Da mesma forma que Fermat, Mersenne começou considerando potências de 2. Porém, em vez de adicionar 1, como fizera Fermat, Mersenne decidiu subtrair 1 da resposta. Assim, por exemplo, $2^3 - 1 = 8 - 1 = 7$, um número primo. É possível que a intuição musical de Mersenne o tenha ajudado. Ao duplicarmos a frequência de uma nota, ela se eleva uma oitava, portanto potências de 2 produzem notas harmônicas. Poderíamos esperar que um desvio de 1 gerasse uma nota muito dissonante, incompatível com qualquer frequência prévia — uma "nota prima". (Sautoy, 2007, p.41 e 42).

O maior primo de Mersenne conhecido é $M_{43112609}$, descoberto pelo *Great Internet Mersenne Prime Search (GIMPS)*, em 2008, e possui no sistema decimal 12 978 189 dígitos.
Será que os números de primos de Mersene são em quantidade infinita? Essa é uma conjectura deixada até nós [14].
As contribuições trazidas com as descobertas desses números são de grandezas imensuráveis e responsáveis por surgimento de importantes proposições no estudo da teoria dos números, e formulação de conjecturas que sobrevivem ao tempo fascinando matemáticos de diversas gerações.

2.3 Pequeno Teorema de Fermat

Constitui-se um dos mais importantes resultados sobre teoria dos números, e muito útil na resolução de problemas relacionados a divisibilidade e números primos. Antes de enunciá-lo, é necessário destacar um lema útil na demonstração desse teorema.

Lema 2.3. *Dado um número primo p, os números $\left(\begin{array}{c} p \\ i \end{array} \right)$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração
Se $i = 1$ não há o que provar. Seja $1 < i < p$. Temos que $i!|p(p-1)\cdots(p-i+1)$, e como $(i!, p) = 1$, ou seja, $i \nmid p$, implica $i!|(p-1)\cdots(p-i+1)$, logo garante que

$$\left(\begin{array}{c} p \\ i \end{array} \right) = p.\frac{(p-1)\cdots(p-i+1)}{i!} \quad \text{equivale a} \quad \left(\begin{array}{c} p \\ i \end{array} \right) = p.k\,, \quad k = \frac{(p-1)\cdots(p-i+1)}{i!},$$

$k \in \mathbb{N}$.

Teorema 2.9 (Pequeno Teorema de Fermat - (PTF)). *Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração
Prova por indução sobre a e para $a \geq 0$.
Para $a = 0$ temos $p|0$. Suponhamos o resultado ser válido para a, devemos provar para $a+1$. Pela fórmula de binômio de Newton,

$$(a+1)^p - (a+1) = \left(\begin{array}{c} p \\ 0 \end{array} \right) a^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1} + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) a + \left(\begin{array}{c} p \\ p \end{array} \right) a^0 \cdot 1 - (a+1)$$

$$= \quad a^p - a + \left(\begin{array}{c} p \\ 1 \end{array} \right) a^{p-1} + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) a$$

Pela hipótese de indução $p|a^p - a$ e pelo lema anterior p divide $\left(\begin{array}{c} p \\ i \end{array} \right)$, $0 < i < p$, segue que o resultado vale para $a+1$. Portanto, conclui-se a demonstração.

Corolário 2.1. *Se p é um número primo e se a é um número inteiro não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração
A prova é uma consequência do PTF, pois $p|a^p - a = a(a^{p-1} - 1)$, e como $p \nmid a$, segue que $p|a^{p-1} - 1$.

Exemplo 2.10. $3|10^3 - 10$ *ou* $3|10^2 - 1$.

2.4 Equações Diofantinas

Essa seção será dedicada aos estudos das equações diofantinas, que recebe esse nome devido a Diofanto de Alexandria (por volta 300 d.C.), um dos Matemáticos de mais destaque na Teoria dos Números por sua obra o Livro *Arithmetica* [3] que trata, dentre outros problemas, da resolução de equações com uma ou mais incógnitas de coeficientes e soluções inteiras.

Equações diofantinas lineares são equações do tipo $aX + bY = c$, com $a, b, c \in \mathbb{Z}$.

Exemplo 2.11. $2X + 8Y = 5$

Proposição 2.12 (Existência de soluções)**.** *Sejam $a, b \in \mathbb{Z} - \{0\}$ e $c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em números inteiros se, e somente se, $(a, b)|c$.*

Demonstração
($\Longrightarrow$) Suponhamos que sejam x_0 e y_0 um par de solução da equação diofantina acima, ou seja, $ax_0 + by_0 = c$. Sendo $(a, b) = d$, então $a = dr$ e $b = ds$ para r, s inteiros, e, $c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$. Portanto, segue que $d|c$.
($\Longleftarrow$) Agora, seja $d = (a, b)$ e suponhamos que $d|c$. Logo, existe t inteiro tal que $c = d \cdot t$. Como

$(a,b) = d$, pelo teorema (2.3), existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$ o que implica:
$c = dt = t(ax_0 + by_0) = a(tx_0) + b(ty_0)$, o que fornece o par $x = tx_0 = (c/d)x_0$ e $y = ty_0 = (c/d)y_0$ como uma solução da equação $aX + bY = c$.

Proposição 2.13 (Solução da equação diofantina)**.** *Seja $(a,b) = d$. Se $d|c$, e se o par de inteiros x_0, y_0 é uma solução particular da equação diofantina linear $aX + bY = c$, então todas as outras soluções desta equação são dadas pelas fórmulas:*
$x = x_0 + (b/d)t$ e $y = y_0 - (a/d)t$, onde t é um inteiro arbitrário.

***Demonstração**:*
Suponhamos que o par x_0, y_0 é uma solução particular da equação $ax + by = c$, e seja x_1, y_1 uma outra solução qualquer desta equação. Então, temos:
$ax_0 + by_0 = c = ax_1 + by_1$ e, portanto, $a(x_1 - x_0) = b(y_0 - y_1)$.
Por ser $(a,b) = d$, existem inteiros r e s, primos entre si, tais que $a = dr$ e $b = ds$. Substituindo na igualdade anterior, obtém-se: $r(x_1 - x_0) = s(y_0 - y_1)$. Logo, $r|s(y_0 - y_1)$, e como $(r,s) = 1$, segue-se que $r|(y_0 - y_1)$ e implica que $y_0 - y_1 = rt$ e $x_1 - x_0 = st$, para algum t inteiro.
Portanto,
$x_1 = x_0 + st = x_0 + (b/d)t$
$y_1 = y_0 - rt = y_0 - (a/d)t$,
são as soluções procuradas.

NOTAS:
***i)** Percebemos que se $(a,b) = d$ e $d|c$, a equação $ax + by = c$ admite infinitas soluções. E se $(a,b) = d = 1$, temos $b/d = b$ e $a/d = a$ e as soluções são do tipo $x = x_0 + bt$ e $y = y_0 - at$.*
***ii)** Uma solução particular pode ser determinada por inspeção quando os valores absolutos de a, b, c são pequenos. Caso contrário, escrevemos (a,b) como combinação linear de a e b, usando o algoritmo euclidiano.*

Exemplo 2.12. *Um cachecol custa, na Rússia, 19 rublos, mas o caso é que o comprador só tem notas de 3, e o caixa, só de 5. Nessas condições, será possível pagar a importância da compra, e de quantos modos?*

Solução:

Do enunciado, escrevemos a equação $3X - 5Y = 19$. De $(3,5) = 1$ e $1|19$, concluímos que a equação admite infinitas soluções inteiras. A solução particular pode ser achada por inspeção, pois os números 3, 5 e 19 são pequenos, ou utilizando o algoritmo de Euclides podemos escrever $3 \cdot 2 - 5 \cdot 1 = 1$ e, assim, multiplicando ambos os membros da igualdade por 19, teremos $3 \cdot 38 - 5 \cdot 19 = 19$.
Logo, $x_0 = 38$ e $y_0 = 19$ é solução particular da equação que tem as demais soluções inteiras positivas dadas por:

$X = 38 - 5t$ e $Y = 19 - 3t$, com $t \in \mathbb{Z}$ e $t \leq 6$.

2.5 Congruências

O conceito de congruência foi introduzido por Gauss em seu livro *Disquisitiones Arithmeticae*, em 1801. Muitos problemas que parecem complexos por suas dimensões de cálculos não imediatos tornam-se resolvíveis com o auxílio da congruência e suas propriedades.

Definição 2.3. *Sejam a e b inteiros quaisquer e m um inteiro positivo. Dizemos que a é congruente a b módulo m se, e somente se, $m|a - b$. Em outras palavras, a é congruente a b módulo m se, e somente se, existe $k \in \mathbb{Z}$, tal que $a - b = km$.*

Notação: $a \equiv b \ mod \ m \quad ou \quad a \equiv b \ (mod \ m)$.

Portanto, $a \equiv b \ (mod \ m) \iff m|(a - b)$.

Exemplo 2.13. $24 \equiv 4 \ (mod \ 5), \quad pois \quad 5|(24 - 4)$
$-3 \equiv 7 \ (mod \ 10), \quad pois \quad 10|(-3 - 7)$.

Proposição 2.14. *Dois números inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

***Demonstração**:*
($\Longrightarrow$) Suponha que $a \equiv b \ (mod\ m)$. Então, da definição decorre que $a - b = km$, com $k \in \mathbb{Z}$. Seja r o resto da divisão de b por m; pelo algoritmo da divisão, $b = mq + r$, onde $0 \leq r < m$
Logo, de $a - b = km$, $a = km + b = km + mq + r = m(k + q) + r$,
Isso mostra que r também é resto da divisão de a por m.
($\Longleftarrow$) Reciprocamente, suponha que a e b divididos por m deixam o mesmo resto. Então, sejam $a = mq_1 + r$ e $b = mq_2 + r$, onde $0 \leq r < m$.
Logo, $a - b = (q_1 - q_2)m \Longrightarrow m|(a - b) \Longrightarrow a \equiv b(mod\ m)$.

Exemplo 2.14. $18 \equiv 4(mod\ 7)$, *pois pelo algoritmo da divisão* $18 = 7 \cdot 2 + 4$ *e* $4 = 7 \cdot 0 + 4$.

Proposição 2.15. *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, temos que*

i) $a \equiv a(mod\ m)$.

ii) Se $a \equiv b(mod\ m)$, *então* $b \equiv a(mod\ m)$.

iii) Se $a \equiv b(mod\ m)$ *e* $b \equiv c(modm)$, *então* $a \equiv c(mod\ m)$.

***Demonstração**:*
i) De fato, como $m|0$, $m|(a - a)$.

ii) se $a \equiv b(mod\ m)$, então $a - b = km$, com $k \in \mathbb{Z}$. Portanto, $b - a = -km = (-k)m \Longrightarrow b \equiv a(mod\ m)$.

iii) Com efeito, dadas as condições acima, existem inteiros k e t tais que $a - b = tm$ e $b - c = km$. Logo, $a - c = b + tm - b + km = (t + k)m$ que implica $a \equiv c(mod\ m)$.

Proposição 2.16. *Seja m um inteiro positivo $(m > 1)$. Sejam a e b números inteiros quaisquer, então:*

i) Se $a \equiv b(mod\ m)$ e se $n|m$, $n > 0$, então $a \equiv b(mod\ n)$.

ii) Se $a \equiv b(mod\ m)$ e se $c > 0$, então $ac \equiv bc(mod\ mc)$.

iii) Se $a \equiv b(mod\ m)$ e se a, b, m são todos divisíveis pelo inteiro $d > 0$, então $a/d \equiv b/d(mod\ m/d)$.

***Demonstração**:*
i) Se $a \equiv b(mod\ m)$, então $a - b = km$, e de $n|m$ tem-se $m = n.q$, com k, q inteiros e $q > 0$. Portanto $a - b = (kq)n$ que implica $a \equiv b(mod\ n)$.

ii) Como $a \equiv b(mod\ m)$, existe inteiro k, tal que $a - b = km$. Sendo $c > 0$, segue que $ac - bc = k(mc)$, daí resulta que $ac \equiv bc(mod\ mc)$.

iii) Se $a \equiv b(mod\ m)$, existe inteiro k, tal que $a - b = km$. Sendo $d > 0$, segue que $a/d - b/d = k \cdot m/d$, daí resulta que $a/d \equiv b/d(mod\ m/d)$.

Proposição 2.17. *Sejam $a, b, c, m \in \mathbf{Z}$, com $m > 1$.*

i) Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a + c \equiv b + d(mod\ m)$ e, $ac \equiv bd(mod\ m)$.

ii) Se $a \equiv b(mod\ m)$, então $a^n \equiv b^n(mod\ m)$ para todo $n > 0$.

***Demonstração**:*
i) Supondo que $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$. Logo, tem-se $m|a - b$ e $m|c - d$. Portanto, $m|(a - b) + (c - d)$, isto é, $m|(a + c) - (b + d)$ que implica $a + c \equiv b + d(mod\ m)$.
E, por outro lado, temos que $a - b = km$ e $c - d = qm$, com $k, q \in \mathbb{Z}$. Multiplicando ambas as igualdades anteriores por c e b, respectivamente, e somando membro a membro uma com a outra, obtemos $ac - bd = (ck + bq)m$, o que mostra $m|ac - bd$ e implica $ac \equiv bd(mod\ m)$.
É imediato, desse último argumento, que se $a \equiv b(mod\ m)$ então $ac \equiv bc(mod\ m)$, pois $c \equiv c(mod\ m)$.
ii) Por indução sobre n:
Para $n = 1$ a proposição é verdadeira. Supondo ser válida para um inteiro positivo $n = k$, temos então, $a^k \equiv b^k(mod\ m)$ e $a \equiv b(mod\ m)$.
Portanto, pelo item (i), $a^k.a \equiv b^k.b(mod\ m)$ ou $a^{k+1} \equiv b^{k+1}(mod\ m)$, logo a proposição é verdadeira para $n = k + 1$ e, portanto válida para todo n positivo.

Proposição 2.18. *Sejam $a, b, c, m \in \mathbf{Z}$, com $m > 1$. Temos que*
$a + c \equiv b + c(mod\ m) \iff a \equiv b(mod\ m)$.

***Demonstração**:*
Se $a \equiv b(mod\ m)$ segue da proposição anterior que $a + c \equiv b + c(mod\ m)$, pois $c \equiv c(mod\ m)$. Reciprocamente, se $a + c \equiv b + c(mod\ m)$, então $m|b + c - (a + c)$, o resulta $m|b - a$ e, consequentemente, $a \equiv b(mod\ m)$.

Proposição 2.19. *Sejam $a, b \in \mathbf{Z}$. Se $m, m_1, \cdots, m_r$ são inteiros maiores do que 1, temos que:*

i) $a \equiv b(mod\ m_i)$, para todo $i = 1, \cdots, r \iff a \equiv b(mod\ [m_1, \cdots, m_r])$;

ii) Se $a \equiv b(mod\ m)$, então $(a, m) = (b, m)$.

***Demonstração**:*

i) Se $a \equiv b(mod\ m_i)$, $i = 1, \cdots, r$, então $m_i|b - a$ para todo i. Sendo $b - a$ um múltiplo de cada m_i, segue que $[m_1, \cdots, m_r]|b - a$, o que prova que $a \equiv b(mod\ [m_1, \cdots, m_r])$. A recíproca decorre da proposição 2.16(i), isto é, se $a \equiv b(mod\ [m_1, \cdots, m_r])$ tem-se que cada $m_i|[m_1, \cdots, m_r]$ para $i = 1, \cdots, r$. Logo, $a \equiv b(mod\ m_i)$.

ii) Se $a \equiv b(mod\ m)$, então $m|b - a$ e, portanto, $b = a + tm$, com $t \in \mathbf{Z}$. Logo, pelo Lema 2.1 tem-se $(a, m) = (a + mt, m) = (b, m)$.

Proposição 2.20. *Sejam $a, b, c, m \in \mathbf{Z}$, com $c \neq 0$ e $m > 1$. Seja $(c, m) = d$. Temos que*
$ac \equiv bc(mod\ m) \iff a \equiv b(mod\ \frac{m}{d})$.

***Demonstração**:*
Como $\frac{m}{d}$ e $\frac{c}{d}$ são coprimos [2], então
$ac \equiv bc(mod\ m) \iff m|(b - a)c \iff \frac{m}{d}|(b - a)\frac{c}{d}$.

[2]Números primos entre si (coprimos ou, ainda, relativamente primos) são conjuntos de números onde o máximo divisor comum entre eles é o número 1.

É imediato que, se $(c, m) = 1$, *temos* $ac \equiv bc(mod\ m) \iff a \equiv b(mod\ m)$.

Na sequência, definiremos um sistema completo módulo m, que será base para outros pontos importantes deste material.

Definição 2.4 (Sistema completo de restos). *Chamamos sistema completo de restos módulo m* ***todo conjunto*** $S = \{r_1, \cdots, r_m\}$ *de m inteiros tal que um inteiro qualquer a é congruente módulo m a um único elemento de S.*

Exemplo 2.15. *Cada um dos conjuntos* $\{0, 1, 2, 3\}$, $\{1, 2, 3, 4\}$, $\{-3, -2, -1, 0\}$ *é um sistema completo de restos módulo 4.*

Definição 2.5 (Função de Euler). *Se n é um número inteiro positivo, a função* ϕ *de Euler, denotada por* $\phi(n)$, *é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Antes de passarmos ao cálculo de $\phi(n)$, é necessário compreender as seguintes formulações:

Proposição 2.21. *Sejam m e n inteiros positivos tais que* $(m, n) = 1$. *Então,* $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Demonstração:
O resultado é trivial para $m = 1$, *ou* $n = 1$. *Portanto, vamos supor* $m > 1$ *e* $n > 1$. *Neste caso, os inteiros de 1 a* $m \cdot n$ *podem ser dispostos em m colunas com n inteiros em cada uma delas, do seguinte modo:*

$$\begin{array}{ccccccc} 1 & & 2 & \cdots & h & \cdots & m \\ m+1 & & m+2 & & m+h & & 2m \\ 2m+1 & & 2m+2 & & 2m+h & & 3m \\ \vdots & & \vdots & & & \vdots & \\ (n-1)m+1 & & (n-1)m+2 & & (n-1)m+h & & n \cdot m \end{array} \tag{2.3}$$

Por ser o $(qm+h, m) = (h, m)$, os inteiros da h-ésima coluna são primos com m se, e somente se, h é primo com m. E como na primeira linha o número de inteiros que são primos com m é igual a $\phi(m)$, segue-se que existem somente $\phi(m)$ colunas formadas com inteiros que são todos primos com m. Por outro lado, em cada uma destas $\phi(m)$ colunas existem, precisamente, $\phi(n)$ inteiros que são primos com n, porque na progressão aritmética:
$h, m+h, 2m+h, \cdots, (n-1)\cdot m+h$, onde o $(h, m) = 1$,
o número de termos que são primos com n é igual a $\phi(n)$. Assim sendo, o número total de inteiros que são primos com m e com n, isto é, que são primos com m.n, é igual a $\phi(m) \cdot \phi(n)$, e isto significa que $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Lema 2.4. *Se p é um número primo e r, um número natural, então temos que*
$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Demonstração:
De 1 até p^r, temos p^r números naturais. Temos que excluir desses os números que não são primos com p^r, ou seja, todos os múltiplos de p, que são precisamente $p, 2p, \cdots, p^{r-1}p$, cujo número é p^{r-1}. Portanto, $\phi(p^r) = p^r - p^{r-1}$.

Agora sim, podemos generalizar o cálculo de $\phi(m)$ por meio de uma expressão utilizando o teorema abaixo.

Teorema 2.10. *Seja $m > 1$ e $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ a sua decomposição em fatores primos. Então,*

$$\phi(m) = p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1} \cdot (p_1 - 1) \cdots (p_n - 1).$$

Demonstração
O resultado segue, imediatamente, da proposição e do lema anteriores.
De fato, temos
$\phi(m) = \phi(p_1^{\alpha_1}) \cdots \phi(p_n^{\alpha_n}) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_n^{\alpha_n - 1}(p_n - 1)$, *ou seja,*
$\phi(m) = p_1^{\alpha_1 - 1} \cdots p_n^{\alpha_n - 1}.(p_1 - 1) \cdots (p_n - 1)$.

Por meio desses resultados Euler chegou a uma generalização do Pequeno Teorema de Fermat, já demonstrado neste material. Vejamos a seguir.

Teorema 2.11 (Teorema de Euler)**.** *Sejam $m, a \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. Então,*

$a^{\phi(m)} \equiv 1 (mod\ m)$.

Demonstração
$\phi(m)$ é o número de elementos primos com m. E, sendo $\{r_1, r_2, \cdots, r_{\phi(m)}\}$ o conjunto de elementos que sobram após a eliminação daqueles primos com m, constitui um sistema reduzido de resíduos módulo m, e se $(a, m) = 1$, então $\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$ também constitui um sistema reduzido de resíduos módulo m, pois ar_i é primo com m. Logo, segue daí que cada ar_i é congruente a exato um r_j, $1 \leqslant j \leqslant \phi(m)$. Portanto, o produto ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(n)} (mod\ m)$ *que resulta em*
$a^{\phi(m)}(r_1 r_2 \cdots r_{\phi(n)}) \equiv r_1 r_2 \cdots r_{\phi(n)} (mod\ m)$,
como $(m, r_1 r_2 \cdots r_{\phi(n)}) = 1$, *cancelamos o produto* $r_1 r_2 \cdots r_{\phi(n)}$ *em ambos os lados e concluímos o resultado,*

$a^{\phi(m)} \equiv 1 (mod\ m)$.

Como um caso particular do teorema de Euler, para $m = p$ e $p \nmid a$, enunciaremos o PTF com a notação de congruência.

Teorema 2.12 (Pequeno Teorema de Fermat - PTF). *Se p é um número primo e $a \in \mathbf{Z}$, então $a^p \equiv a (mod\ p)$, e se $p \nmid a$, então $a^{p-1} \equiv 1 (mod\ p)$.*

Exemplo 2.16. *Determine o resto da divisão do número* $2222^{5555} + 5555^{2222}$ *por* 7.

Observamos que 7 *é um número primo e* $7 \nmid 5555$. *Logo, pelo PTF, temos que:*
$5555^6 \equiv 1(mod\ 7)$. *Utilizando as propriedades de congruências, encontramos*
$(5555^6)^{370} = 5555^{2220} \equiv 1(mod\ 7)$ *e, por outro lado,* $5555^2 \equiv 4^2 \equiv 2(mod\ 7)$. *Dessas duas congruências resulta que* $5555^{2222} \equiv 2(mod\ 7)\ \ (I)$.
De modo análogo, temos $2222^6 \equiv 1(mod\ 7)$, *pois* $7 \nmid 2222$.
Daí, segue que $(2222^6)^{925} = 2222^{5550} \equiv 1(mod\ 7)$. *De* $2222^5 \equiv 3^5 = 3^3 \cdot 3^2 \equiv 5(mod\ 7)$, *concluímos que* $2222^{5555} \equiv 5(mod\ 7)\ \ (II)$.
Somando as congruências (I) *e* (II), *membros correspondentes, encontraremos* $2222^{5555} + 5555^{2222} \equiv 5 + 2 \equiv 0(mod\ 7)$.
Portanto, o resto da divisão de $2222^{5555} + 5555^{2222}$ *por* 7 *é* 0.

2.5.1 Congruências lineares

Definição 2.6. *Uma congruência linear é uma equação do tipo*

$$ax \equiv b\ (mod\ m) \tag{2.4}$$

onde $a, b, m \in \mathbb{Z}$, $m > 1$.

Uma solução da congruência linear *é um número inteiro* x_0 *tal que* $ax_0 \equiv b(mod\ m)$.
Como $ax_0 \equiv b(mod\ m)$ *se, e somente se,* $m|ax_0 - b$, *isso implica que* $ax_0 - b = m \cdot y_0$, *para* y_0 *inteiro, e encontrar a solução de* (2.4) *é o mesmo que resolver a* ***equação diofantina*** $ax - my = b$. *Por sua vez,* $ax - my = b$ *só admite solução se* $(a, m)|b$. *Essa é a condição de existência da solução de uma congruência linear.*
Como já demonstramos, anteriormente, que a solução particular x_0, y_0 *de uma equação diofantina do tipo* $ax - my = b$, *tal que* $(a, m) = d$, *gera uma infinidade de soluções gerais do tipo* $x_1 = x_0 + (m/d).t$ *e* $y_1 = y_0 - (a/d) \cdot t$, *para t inteiro. Consequentemente, podemos generalizar esse fato para o caso das congruências lineares, considerando* x_0 *uma solução particular e* $x_1 = x_0 + (m/d) \cdot t$ *como solução geral de* (2.4).
NOTA*: No caso da congruência linear, se* $(a, m) = d$ *e* x_0 *é uma solução particular, o número de solu-*

ções incongruentes módulo m é dado pelo valor de d. As demais soluções são ditas congruentes módulo m, ou seja, não representam soluções diferentes.
Esse argumento é expresso pelo teorema a seguir.

Teorema 2.13. *Sejam a, b, m inteiros, com $m > 1$, $(m, a) = d$. Se $d|b$, então a congruência linear $ax \equiv b(mod\ m)$ tem precisamente d* ***soluções incongruentes módulo m****.*

Demonstração*:*
Essa congruência pode ser representada na forma de equação diofantina $ax - my = b$, com soluções $x = x_0 + (m/d) \cdot t$ e $y = y_0 + (a/d) \cdot t$, onde t é um inteiro qualquer. Entre o número infinito de inteiros dados pela primeira equação, considere apenas as que resultam de atribuir a t os valores: $0, 1, 2, \cdots, d-1$. Ou seja, os d inteiros:
$x_0,\ \ x_0 + m/d,\ \ x_0 + 2(m/d)\ , \cdots,\ x_0 + (d-1)(m/d)$.
Devemos mostrar que esses d inteiros são mutuamente incongruentes módulo m e que todos os outros inteiros dados por essa fórmula $x = x_0 + (m/d) \cdot t$ são congruentes módulo m a algum desses inteiros. Com efeito, se fosse
$x_0 + (m/d) \cdot t_1 \equiv x_0 + (m/d) \cdot t_2(mod\ m)$, *onde* $0 \leq t_1 < t_2 \leq d-1$, *então teríamos*
$(m/d) \cdot t_1 \equiv (m/d) \cdot t_2(mod\ m)$. *E como* $(m/d, m) = m/d$, *podemos cancelar o fator comum* (m/d), *o que nos dá a congruência:* $t_1 \equiv t_2(mod\ d)$, *e isto significa que* $d|(t_2 - t_1)$, *que é impossível, sendo* $0 < t_2 - t_1 < d$.
Por outro lado, qualquer outro inteiro $x_0 + (m/d)t$ é congruente módulo m a algum dos d inteiros acima enumerados. De fato, pelo algoritmo da divisão, tem-se $t = dq + r$, onde $0 \leq r \leq d-1$ e, portanto,
$x_0 + (m/d) \cdot t = x_0 + (m/d) \cdot (dq + r) = x_0 + mq + (m/d) \cdot r$,
ou seja, $(x_0 + (m/d) \cdot t) - (x_0 + (m/d) \cdot r) = mq$, *o que implica em* $x_0 + (m/d) \cdot t \equiv x_0 + (m/d) \cdot r(mod\ m)$,
onde $x_0 + (m/d) \cdot r$ é igual a um dos d inteiros selecionados.

É imediato que para $(m, a) = 1$ a solução da congruência módulo m é única.

Exemplo 2.17. *Resolver a congruência linear* $8x \equiv 12(mod\ 20)$.

Como o $(8, 20) = d = 4$ *e* $4|12$, *a congruência admite exatamente 4 soluções incongruentes módulo 20.*
Por inspeção, acha-se $x_0 = 4$ *uma solução particular, e* $(m/d) = 20/4 = 5$.
Logo, as soluções são $x = 4,\ 4+5,\ 4+2\cdot 5,\ 4+3\cdot 5$, *ou seja,* $x = 4\ ,9,\ 14,\ 19$.

É interessante observarmos que uma congruência representa uma equação diofantina, ou que uma equação diofantina pode ser escrita como uma congruência. Assim, podemos optar pelo método que acharmos mais conveniente para encontrar os inteiros soluções particulares dessas equações.

2.5.2 Teorema Chinês dos Restos

Esse teorema fornece um processo para resolução de sistemas de congruências, quando estes admitem solução. Recebe esse nome por terem sido os chineses os primeiros a conhecer tais resultados.

Teorema 2.14. *Se* $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para cada* $i \neq j$ *e* c_i *inteiro , então o sistema*

$$\begin{cases} a_1 x \equiv c_1 (mod\ m_1) \\ a_2 x \equiv c_2 (mod\ m_2) \\ \qquad \vdots \\ a_r x \equiv c_r (mod\ m_r) \end{cases} \tag{2.5}$$

possui solução e esta é única módulo m, onde $m = m_1 \cdot m_2 \cdots m_r$.

***Demonstração**:*
De fato, $(a_i, m_i) = 1$ *garante que* $a_i x \equiv c_i (mod\ m_i)$ *possui uma única solução* b_i, *e cada equação do sistema pode ser reduzida a forma mais simplificada* $x \equiv b_i (mod\ m_i)$. *Definindo* $y_i = m/m_i$ *onde,* $m = m_1 \cdots m_2 \cdot m_r$, *temos* $(y_i, m_i) = 1$, *uma vez que* $(m_i, m_j) = 1$ *para* $i \neq j$. *De* $(y_i, m_i) = 1$, *temos que cada congruência* $y_i x \equiv 1 (mod\ m_i)$ *possui uma única solução que denotamos por* $\overline{y}_i$. *Logo,* $y_i \overline{y}_i \equiv 1 (mod\ m_i)$, $i = 1, 2, \cdots, r$. *Afirmamos que o número x dado por*
$x = b_1 y_1 \overline{y}_1 + b_2 y_2 \overline{y}_2 + \cdots + b_r y_r \overline{y}_r$
é uma solução simultânea para o sistema de congruências. De fato,
$a_i x = a_i b_1 y_1 \overline{y}_1 + a_i b_2 y_2 \overline{y}_2 + \cdots + a_i b_i y_i \overline{y}_i + \cdots a_i b_r y_r \overline{y}_r \equiv a_i b_i y_i \overline{y}_i \equiv a_i b_i \equiv c_i (mod\ m_i)$ *uma vez que* y_j *é divisível por* m_i *para* $i \neq j$, $y_i \overline{y}_i \equiv 1 (mod\ m_i)$ *e* b_i *é solução de* $a_i x \equiv c_i (mod\ m_i)$.

A unicidade: Se $\overline{x}$ é uma outra solução para o sistema, então $a_i\overline{x} \equiv c_i \equiv a_i x(mod\ m_i)$, e sendo $(a_i, m_1) = 1$ obtemos $\overline{x} \equiv x(mod\ m_i)$. Logo, $m_i|(\overline{x} - x)$, $i = 1, 2, \cdots, r$. Mas como $(m_i, m_j) = 1$ para $i \neq j$ temos que
$[m_1 \cdot m_2 \cdots m_r] = m_1 \cdot m_2 \cdots m_r$ e, portanto $m_1 \cdot m_2 \cdots m_r|(\overline{x} - x)$, ou seja, $\overline{x} \equiv x(mod\ m)$ concluindo essa demonstração.

Exemplo 2.18. *Um Coronel do Corpo de Bombeiros, depois de assumir o comando da corporação, quis saber qual era o efetivo do Comando Geral. Para esse objetivo mandou o Ajudante Geral dispor o efetivo sucessivamente em colunas. Quando formadas colunas de 07 indivíduos, sobravam 6 indivíduos; colunas de 11 indivíduos, sobravam 5 e, por fim, quando as colunas eram compostas 13 indivíduos, sobravam 3. Sabendo que o efetivo do Comando Geral, tem menos de 1000 militares, determine quantos oficiais constituem esse efetivo.*
A solução desse problema consiste em encontrar o valor de x que satisfaça, simultaneamente, às três equações que formam o sistema de congruências lineares, a seguir:

$x \equiv 6(mod\ 7)$
$x \equiv 5(mod\ 11)$
$x \equiv 3(mod\ 13)$

Como $(7, 11) = (7, 13) = (11, 13) = 1$, o sistema possui uma única solução módulo 1001 ($m = 7 \cdot 11 \cdot 13 = 1001$), que é dada por $x = b_1 y_1 \overline{y}_1 + b_2 y_2 \overline{y}_2 + + b_3 y_3 \overline{y}_3$.
Temos $b_1 = 6$, $b_2 = 5$ e $b_3 = 3$; $y_1 = 11 \cdot 13 = 143$, $y_2 = 7 \cdot 13 = 91$ e $y_3 = 11 \cdot 7 = 77$;
Para $y_i\overline{y}_i \equiv 1(mod\ m_i)$, obtemos: $143\overline{y}_1 \equiv 1(mod\ 7)$, $91\overline{y}_2 \equiv 1(mod\ 11)$ e $77\overline{y}_3 \equiv 1(mod\ 13)$, cujos resultados são $\overline{y}_1 = 5$, $\overline{y}_2 = 4$ e $\overline{y}_3 = 12$.
Segue que, $x = 6 \cdot 143 \cdot 5 + 5 \cdot 91 \cdot 4 + 3 \cdot 77 \cdot 12 = 4290 + 1820 + 2772 \equiv 874(mod\ 1001)$.
Logo, $x = 874$ é a solução módulo 1001 do sistema de congruências lineares.
Portanto, o Comando Geral possui um efetivo de 874 militares.

No próximo capítulo apresentaremos algumas atividades experimentais na escola com a finalidade de avaliar a proposta na prática e verificar o desempenho dos alunos com essa alternativa complementar de estudos, de modo a confirmar nossos argumentos expostos neste documento.

Capítulo 3

Atividades Experimentais: oficinas de aprendizagens

ESTE capítulo está reservado aos relatos das atividades de sondagem e experimentos que realizamos, por amostragem, com alunos das três séries do Ensino Médio do colégio Estadual Albérico Gomes Santana, situado no município de Cabaceiras do Paraguaçu-Bahia. Os objetivos primordiais dessas atividades concentraram-se na sondagem do nível de conhecimentos sobre os assuntos abordados no tema, a sua utilização na compreensão e resolução de situações diversas de problemas que envolvem tópicos importantes da teoria dos números, bem como analisar as possíveis contribuições no desenvolvimento de habilidades e competências promovidas através da ampliação dos estudos sobre números primos, divisibilidade e propriedades importantes, introduzindo conceitos complementares através da aritmética modular na educação básica.

Prevendo a obtenção de resultados mais significativos em nossa sondagem/pesquisa, convidamos alunos que demonstram gosto e interesse pela Matemática, traduzidos pelo envolvimento com as provas de olimpíadas e desempenho escolar, a participarem de forma voluntária nesse projeto. Conseguimos formar um grupo com 15 alunos, e estivemos juntos em seis encontros, cada um com duração mínima de duas horas e trinta minutos, duas vezes semanal entre os meses de outubro e novembro do ano 2015. Organizamos essa etapa em três momentos distintos: no primeiro momento (primeiro encontro) uma sondagem sobre os conhecimentos prévios dos alunos; o segundo momento, um pouco mais longo (quatro encontros), para exposição teórica dos conteúdos propostos; e no terceiro momento (último encontro) uma verificação dos resultados e efeitos produzidos pelos encontros anteriores. A seguir, apresentaremos detalhes da dinâmica de trabalho aplicada nesses encontros.

O 1º momento:

No primeiro momento de nossa atividade, aplicamos um teste de sondagem aos alunos para verificar o nível de conhecimento prévio, assim como, analisar as estratégias conhecidas e usadas por eles para resolução de problemas de aritmética com divisibilidade. O teste consistia num questionário composto de 11 questões envolvendo aritmética dos restos e divisão com valores inviáveis por meio de cálculos exaustivos (potências de expoentes com valores elevados), problemas com possibilidades de equações e infinitas soluções (equações diofantinas lineares e sistemas de congruências lineares) e aplicação de teoremas, proposições importantes para generalização de resultados.

As cinco primeiras questões envolveram divisibilidade de potências com expoentes de valores altos, ou a soma e produto delas, por números inteiros. Algumas delas extraídas da Olímpiada Brasileira de Matemática das Escolas Públicas (OBMEP), portanto, já cobradas em avaliações desses alunos.

Questões de números 1 a 5:

1) Determine o resto da divisão do número 2^{257} *por* 7.

2) (Banco questões OBMEP2010). Será o número $3^{444} + 4^{333}$ *divisível por* 5*?*

3) (Banco questões OBMEP2010). Qual é o menor número natural n para o qual $10^n - 1$ *é um múltiplo de* 37*?*

4) Mostrar que o inteiro $n = 13^{16} - 2^{43} \cdot 517$ *é divisível por* 3.

5) Determinar qual é o algarismo das unidades na representação decimal do número $N = (2006^{2007} + 2005 \cdot 2007^{2007})^{2007}$.

Na Figura 3.1, apresentamos o desempenho dos alunos nessas cinco questões. Percebemos que a maioria dos alunos pesquisados não conseguiram resolver as questões propostas, principalmente aquelas compostas por expressões com potenciação. Através da observação dos cálculos efetuados, concluímos que o método utilizado por aqueles que atingiram o acerto foi o das tentativas e erros, às vezes, exaustivos e, em outros casos utilizando cálculo de múltiplos e divisores sem associação com propriedades da aritmética modular.

A sexta questão envolvia a divisão de um polinômio de grau bastante elevado por outro de grau inferior 1111 vezes:

6) (IME – Instituto Militar de Engenharia)- Provar que $P(x) = x^{9999} + x^{8888} + x^{7777} + \cdots + x^{1111} + 1$ *é divisível por* $D(x) = x^9 + x^8 + \cdots + x + 1$.

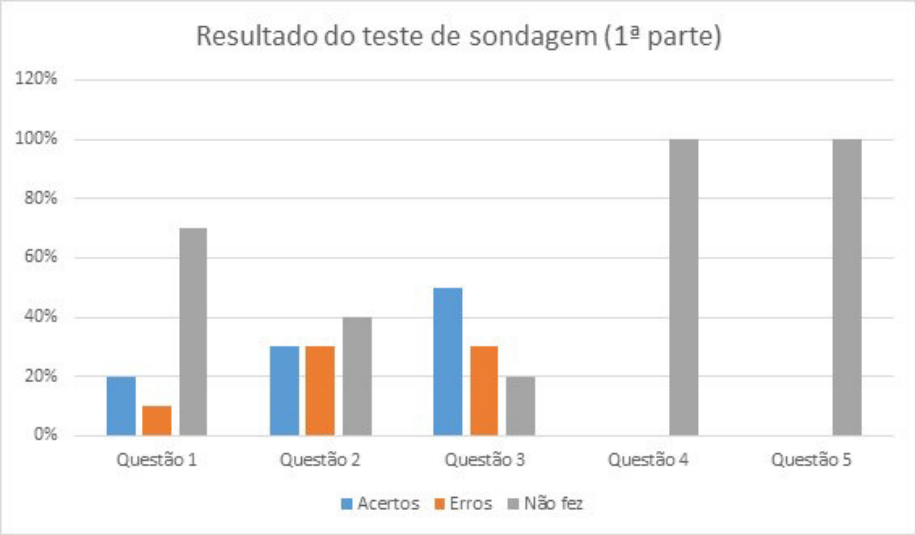

Figura 3.1: Desempenho do alunos - sondagem

Inviável por meio da estratégia de tentativas ou cálculos exaustivos, essa não foi respondida por nenhum dos alunos. Percebemos os anseios deles por uma resposta acessível e simplificada para tal questão, despertando, assim a curiosidade e o interesse pela ampliação dos seus conhecimentos básicos.

A sétima questão, retirada da edição de 2015 da OBMEP, referia-se ao jogo envolvendo um problema sobre operações com restos de divisões. Essa questão exigia do aluno a análise e estabelecimentos de estratégias para expor sua solução. Apenas um aluno respondeu de modo coerente a solução possível:
7) (Banco questões OBMEP2015). Jogando com o resto na divisão por 3 :
Arnaldo e Bernaldo decidem jogar um jogo que possui um número limitado de jogadas. Arnaldo escreve o número 1 *no quadro em sua primeira jogada. Em seguida, Bernaldo escreve* 2 *ou* 4 *no quadro. Depois disso, Arnaldo escreve* 3 *ou* 9 *no quadro. Os dois continuam jogando alternadamente mantendo a regra de que na jogada n o jogador escreve n ou* n^2 *no quadro. Arnaldo vence o jogo se, após a última jogada, a soma dos números no quadro for divisível por* 3*. Se a soma não for divisível por* 3*, então Bernaldo vence. Suponha que o jogo acabe na jogada de número* 15*. Mostre que Bernaldo pode garantir a vitória.*

Questões de 8 a 11:
8) Subindo uma escada de dois em dois degraus, sobra um degrau. Subindo a mesma escada de três

em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o seu número é múltiplo de 7 e está compreendido entre 40 e 100.
9) (Banco questões OBMEP2015). Contando Chocolates: João possui mais que 30 e menos que 100 chocolates. Se ele organizar os chocolates em linhas de 7, sobrará um. Caso ele os organize em linhas de 10, sobrarão 2. Quantos chocolates ele possui?
10) (Banco questões Obmep2015). Pulos do grilo sem cair do penhasco: Um grilo pode dar pulos de duas distâncias: 9 e 8 metros. Ele disputa uma corrida da de 100 metros que vai até a beira de um penhasco. Quantos pulos o grilo deve dar para chegar ao fim da corrida, mas sem passar do ponto final e cair do penhasco?
11) Um camponês tem um certo número de ovos numa cesta. Quando os divide por 3, sobra-lhe 1; quando os divide por 4, sobram 2 ovos; e quando os divide por 5, sobram 3. Quantos ovos tem o camponês nessa cesta, sabendo que tinha uma quantidade maior que 150 e menor de 200?

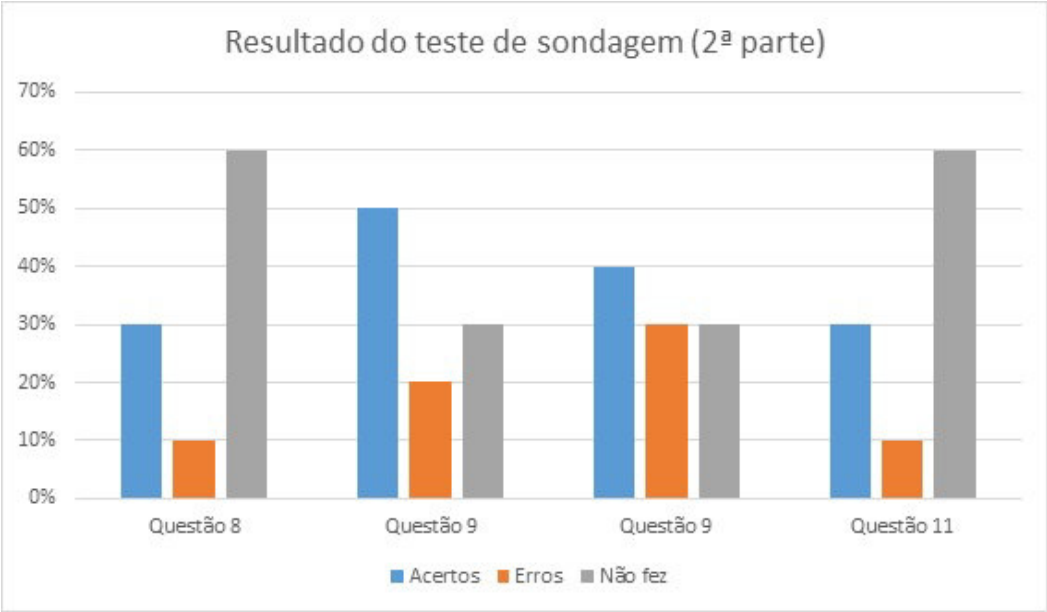

Figura 3.2: Desempenho dos alunos - sondagem (continuação)

A segunda parte do teste contempla questões sobre equações diofantinas e sistemas de congruência lineares. O gráfico da Figura 3.2 mostra que a maioria das questões tiveram menos de 50 % de acertos, e em metade delas o percentual de alunos que não conseguiram fazer ou erraram chegou a casa dos 80%. Para os acertos, a resolução de equações diofantinas foi feita por

meio de tentativas escrevendo os múltiplos possíveis que contemplasse o enunciado. Quanto aos sistemas de congruências lineares, suas equações eram substituídas pelo cálculo de múltiplos dos divisores dados adicionados aos respectivos restos, representando as soluções pela intersecção desses valores, em determinado intervalo dado pela questão. Constituía um processo inverso ao enunciado, que se torna exaustivo quando se dispõe de valores muitos altos, e não estabelecia um caso geral que permitisse escrever todas as infinitas soluções congruentes.

O 2º momento: os encontros de números 2, 3, 4 e 5:

O segundo momento de atividade foi dedicado a uma apresentação elementar dos conteúdos relacionados a teoria dos números que fundamentam esse trabalho. Fizemos uma breve explanação dos principais resultados, explorando proposições e teoremas importantes, e relacionando todas as situações ao cálculo da aritmética modular como uma forma alternativa, que permite expressar casos complexos de divisibilidade de modo mais acessível à compreensão do aluno, por meio da redução a restos congruentes simplificando valores, antes extremamente inviáveis ao cálculo de tentativas, e, com utilização de propriedades que permitem efetuar operações de modo muito mais simples e rápido.

Inicialmente, apresentamos conceitos fundamentais de divisibilidade abordando proposições e teoremas, até então, desconhecidos pelos alunos, possibilitando a ampliação dos conhecimentos sobre a divisão euclidiana, mdc e algorítimo de Euclides. Realizamos um estudo aprofundado sobre a teoria dos números primos, destacando tópicos relevantes como o teorema fundamental da aritmética e o problema da fatoração de números muito grandes, outros aspectos intrigantes da distribuição e o reconhecimento de um número primo, e as tentativas pela busca de um padrão realizadas por grandes matemáticos, em especial os números de Fermat e os de Mersenne, que possibilitaram conjecturas que perduram ainda nos dias atuais.

A seguir, exploramos a definição e resolução de equações diofantinas lineares e congruências lineares como formas de expressão e determinação de restos de divisões e, teoria auxiliar na compreensão e resolução de equações de duas variáveis inteiras. Por fim, separamos momento especial para apresentar uma aplicação importante das congruências lineares: o teorema chinês dos restos. Mostramos que poderíamos determinar soluções de problemas instigantes, que despertam a curiosidade enigmática das possibilidades para um dado número inteiro positivo.

O 3º momento: a verificação dos resultados práticos

Neste encontro, último dos seis promovidos, aplicamos novamente um teste básico, agora para verificação do desempenho dos alunos após uma exposição concisa de conceitos complemen-

tares à teoria dos números no ensino básico.
Os resultados observados no teste de verificação demonstraram avanços significativos em relação ao desempenho no nosso primeiro encontro (Figuras 3.3 e 3.4).

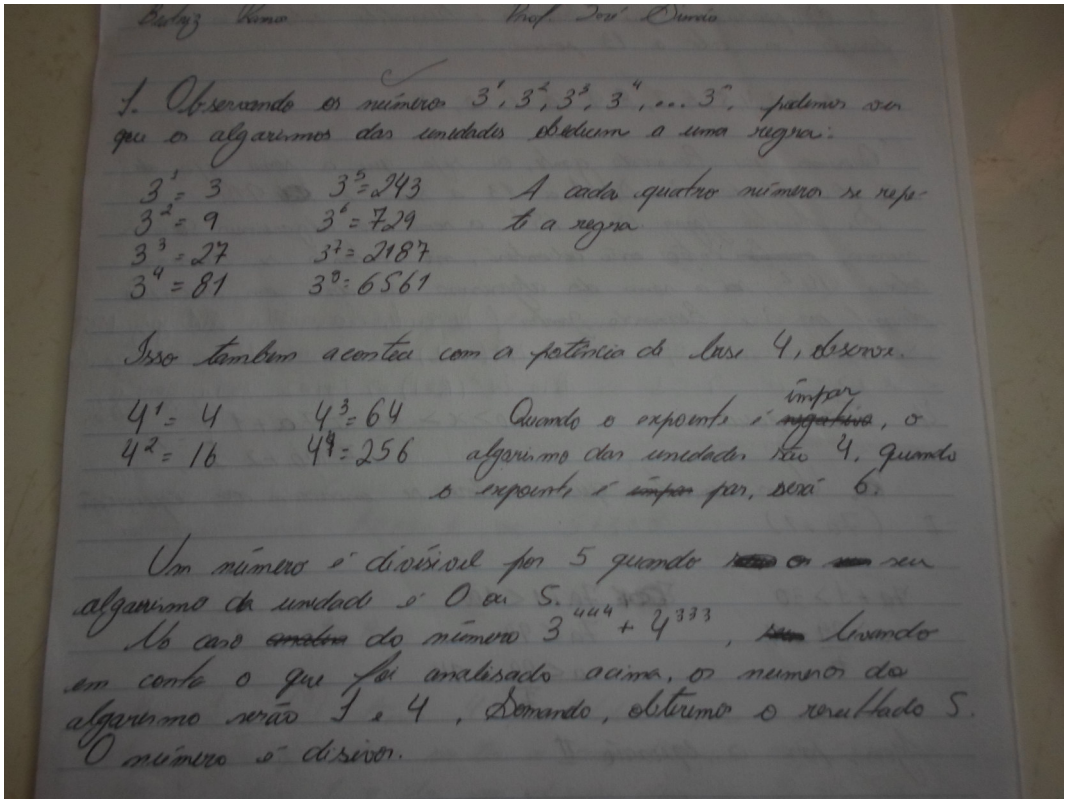

Figura 3.3: Questão sondagem

A utilização da definição de congruência modular e suas propriedades para a determinação de restos em divisões de potências de valores extremamente altos, o uso do pequeno teorema de Fermat como ferramenta para expressão dos restos, e a utilização do Algorítmo de Euclides estendido para resolução de equações diofantinas, são indícios dessa evolução no conhecimento sobre tópicos da teoria dos números não abordados nas séries que compõem a educação básica.
Analisando respostas das questões, as numeradas de 1 a 4, relacionadas ao cálculo de mdc, números primos e divisibilidade por inteiros, foram as que tiveram maior número de acertos:

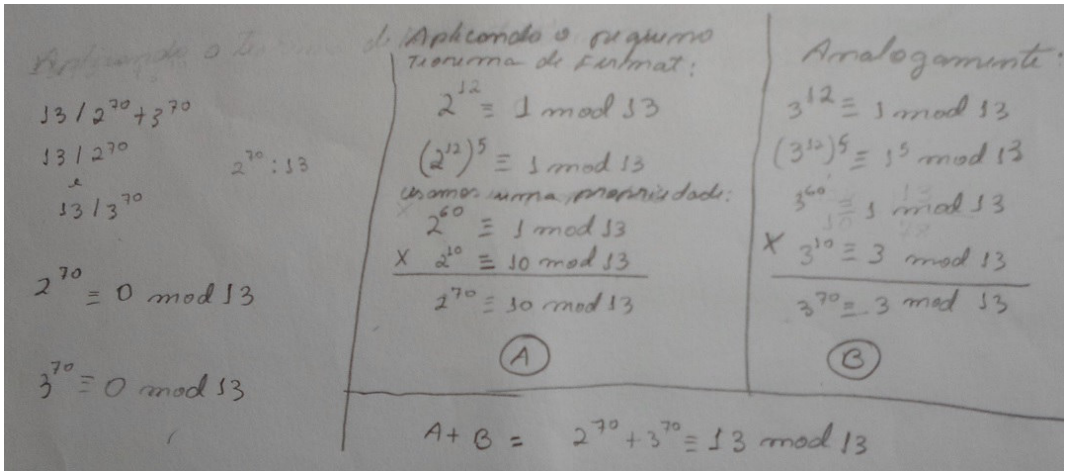

Figura 3.4: Questão verificação

1) O mdc de dois números positivos a e b é 8*. Na determinação desse mdc utilizando o algoritmo de Euclides, os quocientes obtidos, sucessivamente, foram* $2, 1, 1$ *e* 4*. Calcular o valor de a e de b.*
2) Achar todos os primos que são iguais a um quadrado perfeito menos 1*.*
3) Ache o resto da divisão de 2^{50} *por* 7*.*
4) Mostre que 13 *divide* $2^{70} + 3^{70}$ *ou que* $2^{70} + 3^{70} \equiv 0(mod 13)$*.*

As questões 1 e 3 tiveram 70% de alunos bem sucedidos, seguida pela 4 que teve 50% acetos e algumas soluções parciais, sendo que boa parte deles utilizaram o pequeno teorema de Fermat para a resolução dessas questões.

Na segunda parte, as questões de número 5 a 10, envolvendo a resolução de equações diofantinas e teorema chinês dos restos:

5) Achar todos os inteiros X tais que $1 \leq X \leq 100$ *e* $X \equiv 7(mod 17)$*.*
6) De quantas maneiras diferentes pode-se comprar selos de 3 *reais e de* 5 *reais de modo que se gaste* 50 *reais?*
7) Um cachecol custa, na Rússia, 19 *rublos, mas o caso é que o comprador só tem notas de* 3*, e o caixa, só de* 5*. Nessas condições, será possível pagar a importância da compra, e de quantos modos possíveis?*
8) (Adaptação do problema de Sun-Tsu) - Uma senhora estava caminhando para um mercado quando um cavalo se bateu com a sua cesta de ovos. O cavaleiro queria pagar os danos e perguntou para a senhora

quantos ovos haviam na cesta. Ela não se lembrava exatamente da quantidade, mas sabia que se tirasse os ovos da cesta de 3 em 3, sobravam 2 ovos. Se tirasse de 5 em 5, sobravam 3 ovos e de 7 em 7 sobravam 2. Qual seria a menor quantidade de ovos que ela poderia ter?

Alguns alunos ainda utilizaram métodos convencionais de tentativas e erros para resolução de congruáriascongruência e equações diofantinas. Embora a média de acertos para as diofantinas seja de 50%, só 60% desses usaram método adequado para expressar as soluções de modo geral. O teorema do resto chinês para resolução de sistemas de congruências não foi utilizado pelos alunos, que se queixaram de pouco espaço de tempo para a sua assimilação, e a tentativa de solução ainda foi pela busca de múltiplos que satisfizesse a condição do problema.
O gráfico da Figura 3.5 mostra como foi o desempenho dos alunos por assunto abordado.

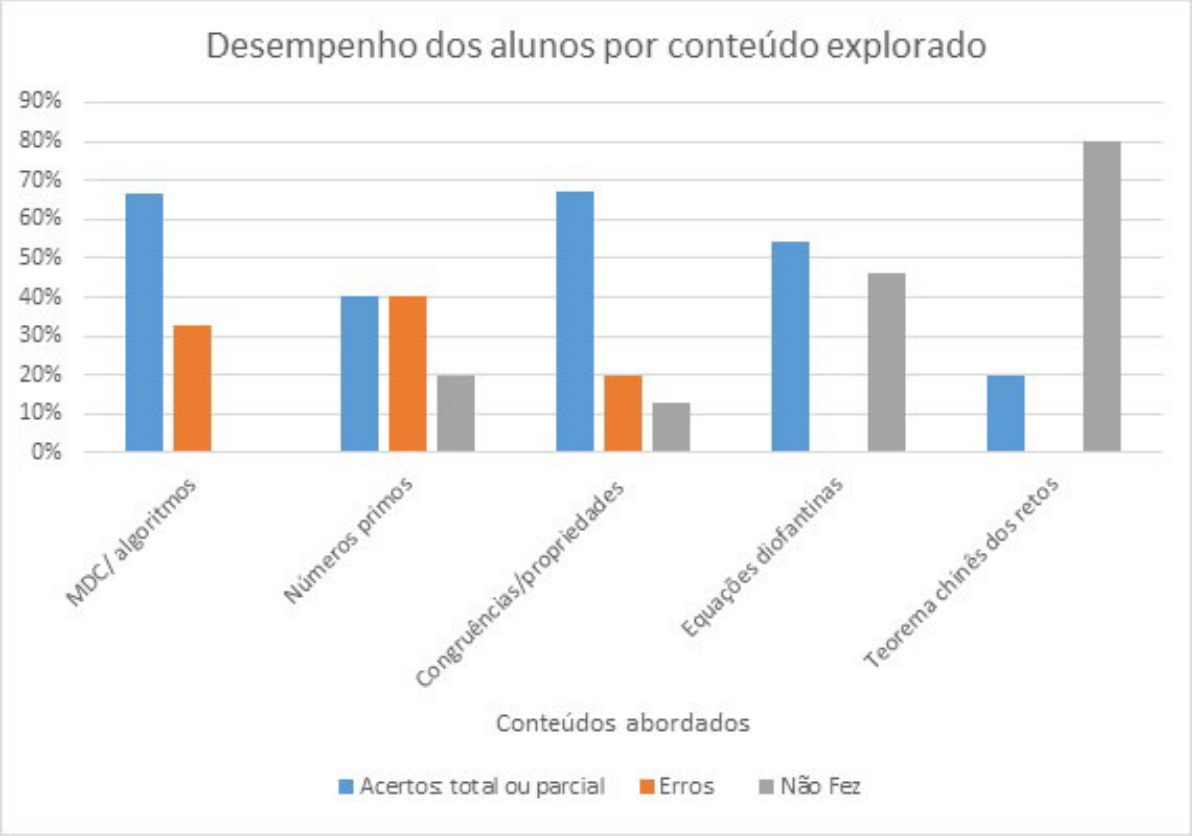

Figura 3.5: Desempenho dos alunos - verificação

As figuras 4.1 e 4.2, em Apêndices, são registros das atividades desenvolvidas pelos alunos, na escola, durante a realização das oficinas.

Capítulo 4

Considerações Finais

O intuito deste trabalho de conclusão de curso é contribuir para a melhoria da Educação Básica, propondo desafios de uma abordagem mais profunda sobre a teoria dos números, como tópicos sobre números primos e divisibilidade nos inteiros estudados superficialmente nas escolas e que não têm sido suficientes para sanar as dificuldades dos alunos reveladas nos baixos índices de proficiências medidos pelas avaliações do ensino no país; e, em especial, promover o estudo de congruências lineares como conceitos complementares essenciais na resolução de problemas complexos, seja por meio de oficinas, reforços em turnos opostos, ou grupos de estudos com alunos participantes de olimpíadas.

Não entraremos no mérito da discussão sobre inserção de conteúdos no currículo escolar da disciplina matemática, uma vez que, divisibilidade e números primos já faz parte do currículo estudado nas escolas, portanto propomos uma abordagem mais aprofundada dos conceitos e propriedades importantes desses assuntos durante a explanação em sala de aula, bem como ampliar essa exploração promovendo estudo das equações diofantinas, congruências e suas propriedades, em momentos opostos ou complementares ao horário aula. Para isso, defendemos uma discussão sobre o aproveitamento dos horários de atividades complementares, na escola, do professor da disciplina para promoção desses estudos extras.

Ao longo do texto apresentamos aspectos relevantes da história da teoria dos números, destacando grandes nomes da Matemática. Também expusemos toda a fundamentação teórica dos conteúdos mencionados nesse trabalho, destacamos posicionamento e observações de como pensam vários autores. E no percurso pedagógico escolar percebemos as dificuldades enfrentadas pelos alunos para o estabelecimento de estratégias e operações com problemas elementares sobre aritmética.

Em nossa atividade experimental de pesquisa e aplicação, embora tenhamos envolvidos apenas uma parte amostral dos alunos, selecionamos voluntários que demonstram o gosto pela matemática e formam o grupo daqueles que detêm os melhores desempenhos escolares na disciplina. E, comprovamos que parte significativa dos alunos não tem ideia de como proceder diante dessas questões que, entretanto, são exploradas em olimpíadas e outras avaliações externas como a OBMEP, requerendo maior atenção por parte do ensino básico diante das dificuldades enfrentadas pelos alunos, que, na maioria das vezes, têm nos questionado sobre a exploração de temas não contemplados em sala de aula, reforçando nosso argumento.

Acreditamos que nossa pesquisa servirá para mostrar como o estudo das congruências lineares e equações diofantinas contribui para melhorar a aprendizagem dos alunos em situações que antes pareciam fora ao alcance por meio de esforços repetitivos e exaustivos. E, portanto, defendemos uma melhor exploração desses conteúdos elementares que possibilitam o desenvolvimento de conhecimentos, competências e constituem elementos importantes para a motivação do aluno ao torná-lo ativo no estudo da matemática por meio da reutilização de tópicos já estudados como afirma POMMER (2013).

Por fim, esperamos que esse trabalho seja um motivador de professores e alunos da educação básica, e superior, para uma exploração mais profunda desse tema, bem como a proliferação das ideias aqui contidas para a melhoria do nosso ensino aprendizagem.

APÊNDICES

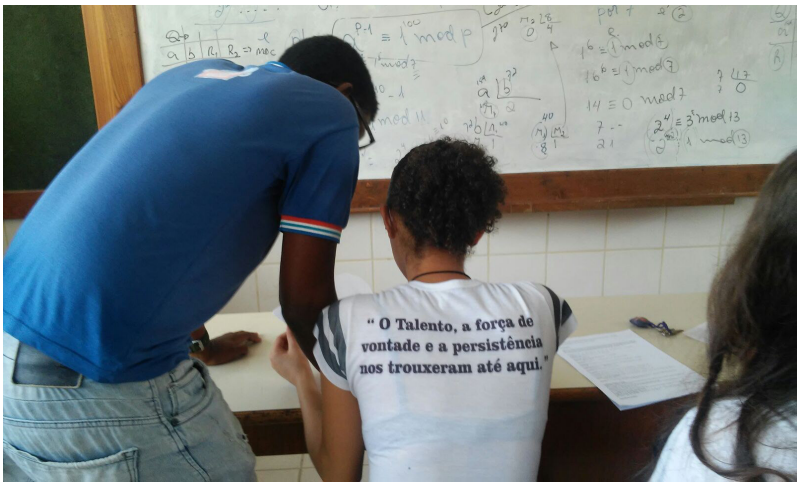

Figura 4.1: Desenvolvimento das atividades

Figura 4.2: Desenvolvimento das atividades

Referências Bibliográficas

[1] BRASIL. Ministério da Educação. **Parâmetros Curriculares Nacionais**: Ensino Fundamental. Brasília, DF: Ministério da Educação, 1997.

[2] BRASIL. Ministério da Educação. **Parâmetros Curriculares Nacionais**: Ensino Médio. Brasília, DF: Ministério da Educação, 2000.

[3] BOYER, Carl B. **História da Matemática**. Tradução: Elza F. Gomide. São Paulo: Edgard Blücher, 1974.

[4] ALENCAR FILHO, Edgar de. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

[5] DOMINGUES, Higino H.**Fundamentos de Aritmética**. São Paulo: Atual, 1991.

[6] HEFEZ, Abramo. **Elementos de Aritmética**. 2ªed. Rio de Janeiro: SBM, 2011.

[7] LINS, Rômulo Campos; GIMENEZ, Joaquim. **Perspectiva em Aritmética e Álgebra para o Século XXI**.(coleção perspectiva em educação matemática). 7ª ed. Campinas - SP: Papirus, 1997.

[8] RIBENBOIM, Paulo. **Números Primos: Velhos mistérisos e novos recordes**. (Coleção matemática universitária) 1ª ed. Rio de Janeiro: IMPA, 2014.

[9] OLIVEIRA, Silvio Barbosa de.**As equações diofantinas lineares e o livro didático de matemática para o ensino médio**. Dissertação(Mestrado em Educação).São Paulo: PUC, 2006. Disponível em: <http://livros01.livrosgratis.com.br/cp009412.pdf>. Acesso em agosto de 2015.

[10] POMMER, Wagner M. **As Equações Diofantinas Lineares no Ensino Médio como tema motivador para o desenvolvimento de competências**. In:X

Encontro Nacional de Matemática. Salvador, julho, 2010. Disponível em: <http://www.gente.eti.br/lematec/CDS/ENEM10/artigos/CC/T11_CC218.pdf>. Acesso em agosto 2015.

[11] POMMER, Wagner M. **Equações Diofantinas Lineares no Ensino Básico: Uma abordagem didático-epistemológica.**. 1ª ed. São Paulo: Edição do Autor, USP 2013. Disponível em: <http://stoa.usp.br/wmpommer/files/3915/20695/Livro+EDL+Uma+abordagem+didatico+epistemogica.pdf>. Acesso em novembro 2015.

[12] RESENDE, M.R. **Re-significando a disciplina Teoria dos Números na formação do professor de Matemática na Licenciatura**. Tese (Doutorado em Educação Matemática), PUC-SP, 2007.

[13] SANTOS, J.P.O. **Introdução à Teoria dos Números**. 2.ed. Rio de Janeiro: IMPA, 2000.

[14] SAUTOY, Marcus du. **A música dos números primos**: a história de um problema não resolvido na matemática. Tradução: Diego Alfaro. Rio de Janeiro: Jorge Zahar Ed., 2007.