UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Números primos, nossos amigos únicos

Carlos Eduardo de Carvalho Macedo

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP SÃO CARLOS

Carlos Eduardo de Carvalho Macedo

Números primos, nossos amigos únicos

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Geraldine Góes Bosco

USP – São Carlos
Abril de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

M141n

Macedo, Carlos Eduardo de Carvalho
Números primos, nossos amigos únicos. / Carlos Eduardo de Carvalho Macedo; orientador Geraldine Goes Bosco. -- São Carlos, 2019.
82 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

1. Teorema Fundamental da Aritmética. 2. Congruências. 3. Pequeno Teorema de Fermat. 4. Números Primos. 5. História dos Números Primos. I. Bosco, Geraldine Goes, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Carlos Eduardo de Carvalho Macedo

Prime numbers, our unique friends

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Geraldine Góes Bosco

USP – São Carlos
April 2019

Dedico este trabalho a todos que se encantam com a área do conhecimento, a todos cujas mentes são inquietas na busca de novos horizontes e estão sempre dispostos a aprender mais.

AGRADECIMENTOS

Agradeço primeiramente à Deus que permitiu que tudo isso fosse possível. Agradeço em seguida a minha avó Alexandrina (in memoriam), a minha mãe Vera Lúcia, a minha esposa Tatiane e a minha filha Raíssa, as quatro grandes mulheres da minha vida por estarem ao meu lado o tempo todo me incentivando e apoiando para que pudesse concluir mais essa etapa, mulheres essas que dedico todo meu amor. Agradeço também a toda a equipe de professores e coordenadores do projeto PROFMAT do polo da USP de Ribeirão Preto/SP pelo empenho de cada um deles e em especial a minha orientadora Geraldine por acreditar no meu trabalho e por todo o seu esforço.

Agradeço também ao suporte financeiro pois, "o presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (Capes) - Código do Financiamento 001".

"A Matemática é o alfabeto com o qual
Deus escreveu o universo."
(Galileu Galilei)

RESUMO

MACEDO.C.E.C. **Números primos, nossos amigos únicos**. 2019. 82 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Neste trabalho é apresentado um breve levantamento da história dos números primos e de que maneira o assunto acerca desses números aparecem no novo cenário trazido pela BNCC. Provamos o Teorema Fundamental da Aritmética e apresentamos duas ferramentas importantes de cálculo, que são as Congruências e o Pequeno Teorema de Fermat. Apresentamos ainda uma proposta didática e um material diferenciado para ser utilizado em sala de aula.

Palavras-chave: História dos números primos, números primos, Teorema Fundamental da Aritmética, Congruências e Pequeno Teorema de Fermat.

ABSTRACT

MACEDO.C.E.C. **Prime numbers, our unique friends**. 2019. 82 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

In the present work is presented a brief data collection about the history of prime numbers and how this subject is shown in the new scenario brought by BNCC (Common Curricular National Base) . It was proved the Fundamental Arithmetic Theorem and it was presented two important ways to calculate that are the Congruence and the Fermet Theorem. It is given a teaching method and a differentiated material to be used in class.

Keywords: History of Prime Numbers, Prime Numbers, Fundamental Theorem of Arithmetic, Congruences and Fermat's Little Theorem.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Esta dissertação teve como motivação vários resultados interessantes da Teoria dos Números, vistos pelo autor nas disciplinas de Aritmética e Matemática Discreta do Profmat. Somou-se a isso também, a experiência da orientadora do trabalho com ensino de Aritmética, no PIC-OBMEP. A ideia inicial era pesquisar situações-problema que poderiam ser aplicadas em sala de aula, mas o trabalho foi na direção de um meio termo entre divulgação científica e o rigor das provas. Os números primos tornaram-se logo os protagonistas do trabalho, e a pergunta de anos anteriores de um medalhista da OBMEP reapareceu: por que mesmo a fatoração de um número natural em números primos é única? O chamado Teorema Fundamental da Aritmética é usado o tempo todo desde o sexto ano do ensino fundamental, mas a essência das ideias que levaram à sua prova, pouco é discutida. Vários textos acabaram por apoiar e motivar a escolha do tema, dentre eles podemos citar Dudley em (DUDLEY, 1969) pela maneira interessante de abordar o assunto, pela riqueza de detalhes nas suas provas e demonstrações e nos exemplos apresentados; e Sautoy em (SAUTOY, 2007) ao apresentar de maneira agradável a história de um dos mais enigmáticos problemas da matemática - "será que existe uma harmonia[1], um padrão[2] entre os números primos?". Questão que ocupou durante séculos (e ainda ocupa) boa parte do tempo das mentes mais ousadas da Matemática.

Como o Teorema Fundamental da Aritmética nos remete à composição dos números inteiros por meio da multiplicação de blocos primos, isso nos lança à ideia da divisão, em particular à noção de divisibilidade, já que a divisão está relacionada à multiplicação. Levando em conta essa linha de pensamento, resolvemos apresentar também um estudo breve sobre Congruência (Aritmética dos Restos) e o Pequeno Teorema de Fermat, que são duas ferramentas importantes para trabalharmos com cálculos envolvendo números

[1] Harmonia: Equilíbrio ou combinação entre os elementos.
[2] Padrão: norma determinada consensualmente por todos os elementos, que é usada como base para estabelecer uma previsão.

muito grandes.

Esse trabalho tem como objetivo apresentar parte da Matemática que passa, muitas vezes, desapercebida, hora por descuido ou até mesmo por desconhecimento. Não é raro nos depararmos com indagações: "Números Primos! Eles ainda são usados?". Poucos sabem da sua importância e vivem sem saber das suas diversas utilidades, limitando-se a acreditar que eles servem apenas para cálculos elementares como o do Mínimo Múltiplo Comum (mmc) ou do Máximo Divisor Comum (mdc). Isso ocorre com inúmeros temas dentro da Matemática, o que nos motivou a focar nesse assunto, apresentando-o com certo rigor, porém com vários exemplos e aplicações, tentando deixar os conceitos mais esclarecedores e motivadores aos leitores.

Iniciamos na seção 1.1 com uma breve apresentação histórica sobre os Números Primos. Destacaremos alguns dos grandes matemáticos que tiveram alguma contribuição em seu estudo. Na seção 1.2 apresentaremos como o assunto é trabalhado dentro do contexto da Educação Básica atual, e o que a Base Nacional Comum Curricular (BNCC) determina para um novo cenário da Educação Básica brasileira.

Na seção 1.3 destacaremos os tópicos das unidades temáticas da BNCC e da matriz de referência do ENEM que se relacionam com o trabalho aqui desenvolvido. Já na seção 1.4, apresentaremos a descrição dos próximos capítulos do trabalho.

1.1 Um pouco de história dos Números Primos

O conceito de número surgiu em resposta às necessidades do dia-a-dia, que eram de ordem prática. Começando, provavelmente, pela correspondência um a um, permitindo, com facilidade, a comparação de quantidades de elementos entre grupos. Porém, essa capacidade da inteligência humana permite ainda escrever números sem ter que relacioná-los, necessariamente à quantidades. Não sabemos, com exatidão, quando isto ocorreu.(IFRAH, 2009)

A mão do homem é o mais antigo acessório de contagem da humanidade e foi através dos seus dez dedos que o homem desenvolveu sua capacidade de contar. Objetos como "pedras, conchas, pauzinhos, terços de contas, bastões entalhados, nós de cordas, etc..."(IFRAH, 2009, p.25) foram, durante muito tempo, utilizados pelo homem como ferramentas de contagem. Com o passar dos tempos esses objetos passaram a tomar a forma de símbolos numéricos, pois o homem sentiu a necessidade de representar grandes quantidades com um mínimo de símbolos possível.

Várias civilizações como, por exemplo, a babilônica, a egípcia e a romana, criaram seus próprios sistemas de numeração. Adotaram símbolos, elaboraram regras e desenvolveram formas consistentes de representação de seus números. Porém, "...a criação dos

algarismos indo-arábicos e a criação do zero foram tão revolucionários quanto o domínio do fogo e o desenvolvimento da prática da agricultura."(IFRAH, 2009, p.27)

Como consequência desses acontecimentos tão significativos o homem desenvolveu, ao longo da história, uma habilidade incrível para lidar com os números. E nesse cenário, surge um elemento notório, o Número Primo, que será o personagem principal do nosso trabalho.

Os gregos desenvolveram resultados importantes sobre números primos. Há indícios de que os primeiros estudos tenham vindo da Escola Pitagórica (cerca 530 a.C.) que já compreendia a ideia de primalidade. Contudo é impossível ter certeza sobre esse fato, pois faltam documentos da época, pois não há nem mesmo peças ou utensílios matemáticos desses tempos. Mas foi com Euclides de Alexandria (cerca de 300 a.C.) que alguns desses resultados tomaram a forma hoje conhecida.(BOYER, 2003)

"Os Elementos"de Euclides contém teoremas importantes sobre números primos, incluindo a demonstração de sua infinitude e a demonstração de que todo número que não é primo, pode ser decomposto em um produto de números primos e de maneira única, chamado de Teorema Fundamental da Aritmética. Esses teoremas serão demonstrados ao longo do desenvolvimento dos próximos capítulos.

Eratóstenes de Cirene (cerca de 200 a.C.), foi outro grego que desenvolveu trabalhos com Números Primos e o primeiro a criar um algoritmo para determiná-los, conhecido como crivo de Eratóstenes. Podemos destacar outros nomes como o célebre francês, Pierre de Fermat (1601 - 1665) que não era um matemático de profissão, mas sim um jurista por formação acadêmica, tanto é que o título que a história lhe concedeu foi de "O Príncipe dos Amadores". Fermat "...dedicou seu excepcional talento ao estudo amadorístico da Matemática e nela deixou sua marca de gênio."(GARBI, 2008, p.194)

Fermat estudou diversas áreas da matemática, mas foi graças aos seus estudos em Teoria dos Números que ele ficou famoso. Fermat afirmava que todo número na forma $2^{2^n}+1$ seria um número primo, que ficou conhecido como "Número de Fermat". Mas o arquiteto da Teoria Moderna dos Números estava errado, e os números $F_n = 2^{2^n}+1$ não são todos primos. De fato, em 1732, Euler mostrou que 641 divide F_5, pois $F_5 = 2^{2^5}+1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$, portanto composto. Fermat deixa também, como parte de seu legado, um importante teorema que envolve números primos e divisibilidade chamado de Pequeno Teorema de Fermat, o qual será apresentado no Capítulo 3 deste trabalho.

O interesse desperto em Fermat pela Matemática, possivelmente, deu-se com a leitura de uma tradução latina, feita por Calude Gaspar Bachet de Méziriac, em 1621, da Aritmética de Diophante, um texto sobrevivente da famosa Biblioteca de Alexandria, queimada pelos árabes no ano de 646, e que reunia cerca de dois mil anos de conhecimentos matemáticos.

Fermat jamais publicou um livro em vida, estudando apenas para sua satisfação. Comunicava suas pesquisas por meio da correspondência que mantinha com grandes matemáticos da época. Marin Mersenne, era um de seus correspondentes, mas outros como, René Descartes, John Wallis, Blaise Pascal e Christian Huygens, também faziam parte de seu círculo postal.(GARBI, 2008)

O padre Marin Mersenne (1588 - 1648) teve um papel importante na história da Matemática francesa do século XVII e também foi uma das poucas amizades de Fermat. Sua grande contribuição foi na Teoria dos Números, em especial, na busca por uma fórmula que descrevesse todos os números primos. Os números de Mersenne são números inteiros da forma $M_p = 2^p - 1$, com p primo. Diversos matemáticos acreditavam que esses números eram primos, porém $M_{11} = 2^{11} - 1 = 2\,047 = 23 \cdot 89$ é composto. Apesar disso Mersenne é ainda lembrado por sua tentativa de prever os números primos.

Após Fermat e Mersenne, Leonhard Euler (1707 - 1783), trouxe novos avanços à Teoria dos Números. Verificou, por exemplo, que F_5 (ou o quinto número de Fermat) não era primo e estendeu o Pequeno Teorema de Fermat. Euler ao estudar o Pequeno Teorema de Fermat, "percebeu sua grande importância e foi bem sucedido em provar um teorema que continha o Teorema de Fermat como caso particular"(RIBENBOIM, 2015, p.75) chamado Teorema de Euler ou ainda Teorema de Euler-Fermat. Euler tinha fascínio por calcular números primos, chegando a produzir tabelas com todos os primos até pouco mais de 100 000. Uma descoberta curiosa de Euler foi a fórmula $x^2 + x + 41$. Ao calcular todas as respostas obtidas substituindo os números naturais de 0 a 39 nessa fórmula, geramos uma lista de quarenta números primos. Euler sabia que a fórmula iria falhar, pois para $x = 41$, o resultado seria divisível por 41. Contudo falha antes pois, para $x = 40$ o resultado também não é primo.(SAUTOY, 2007)

Carl Friederich Gauss (1777 - 1855) foi um dos maiores matemáticos de todos os tempos. Gauss quando criança distraía-se com cálculos matemáticos. Seus mestres, quando perceberam seu talento para a Matemática apresentaram-no ao Duque de Brunswick, que financiou seus estudos.(BOYER, 2003)

Ao chegar em Göttingen em 1795, Gauss estava encantado pela Teoria dos Números, inspirado por Euler. "Gauss sempre dizia: A Matemática é a Rainha das Ciências e a Teoria dos Números é a Rainha da Matemática."(GARBI, 2008, p.272)

> "O grande avanço de Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1 000 e assim por diante. Se tomássemos o número N, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e N? Por exemplo, existem 25 primos até o número 100. Portanto temos uma chance de um em

> quatro de encontrar um primo se escolhermos um número aleatório entre 1 e 100. Como se altera essa proporção se buscarmos os primos de 1 a 1 000 ou de 1 a 1 000 000? Armado com tabelas de números primos, Gauss iniciou sua busca. Ao observar a proporção de primos no universo de números, notou o surgimento de um padrão à medida que a contagem se elevava. Apesar da aleatoriedade desses números, parecia ser possível entrever uma regularidade estonteante."(SAUTOY, 2007, p.57)

Gauss havia achado uma relação entre os primos e a função logarítmica, chamada de $\pi(a)$. Gauss conjecturou que, "...à medida que o número a cresce, $\pi(a)$, ou seja, a quantidade de primos menores que a, tende à relação $a/ln(a)$"(GARBI, 2008, p.277). Esse teorema só foi demonstrado em 1896, por dois matemáticos franceses, usando técnicas avançadas de Teoria Analítica.(GARBI, 2008)

Durante muitos anos grandes matemáticos estiveram obstinados em determinar o próximo número primo, procurando fórmulas para encontrá-lo. Gauss, por sua vez, procurou responder a algo mais amplo: quantos primos há entre um e um milhão. "Era como se as gerações anteriores houvessem escutado a música dos primos nota por nota, sendo incapazes de perceber a composição completa."(SAUTOY, 2007, p.59)

Poderíamos citar outros tantos nomes de grandes matemáticos que desenvolveram importantes trabalhos sobre os Números Primos, porém não queremos nos estender muito mais.

1.2 Um breve cenário do processo de ensino-aprendizagem e a Base Nacional Comum Curricular

Atualmente temos a nítida sensação de que o processo de ensino-aprendizagem, em especial, no campo da Matemática, não tem correspondido às expectativas.

Mesmo sabendo que a Matemática tem um papel importante no nosso cotidiano, os alunos pouco se interessam, e dessa maneira percorrem toda a sua trajetória escolar (ensino básico) sem aproveitar, nem mesmo o mínimo dos assuntos trabalhados. Podemos confirmar isso com os baixos desempenhos registrados pelo IDEB (Índice de Desenvolvimento da Educação Básica). Vivemos ainda a triste realidade de saber que alguns alunos se afastam da escola, interrompendo o processo de ensino-aprendizagem.

O texto de apresentação do documento Diretrizes Curriculares Nacionais da Educação descreve:

> "A Educação Básica de qualidade é um direito assegurado pela Constituição Federal e pelo Estatuto da Criança e do Adolescente. Um dos fundamentos do projeto de Nação que estamos construindo a formação escolar é o alicerce indispensável e condição primeira para o exercício pleno da cidadania e o acesso aos direitos sociais, econômicos, civis e políticos. A educação deve proporcionar o desenvolvimento humano na sua plenitude, em condições de liberdade e dignidade, respeitando e valorizando as diferenças."(DIRETRIZES CURRICULARES, 2013, p.4)

O desenvolvimento de uma educação de qualidade requer compromisso dos órgãos públicos, das instituições de ensino, da família e da sociedade como um todo, pois o desenvolvimento do indivíduo está diretamente relacionado ao desenvolvimento da sociedade, já que o indivíduo está inserido num ambiente de interação e convívio social. Exige também regras que estabeleçam os direitos e os deveres de cada um, ou seja, o desenvolvimento da Educação e por consequência da sociedade, está relacionado ao desafio de lidar com pessoas.(BNCC, 2017)

A escola é um importante espaço de convívio, propiciando, acima de tudo, um ambiente favorável à criação de uma sociedade justa e igualitária, desenvolvendo ainda os saberes, a criatividade e a preparação para a continuidade dos estudos."Assim, para além da garantia de acesso e pemanência na escola, é necessário que sistemas, redes e escolas garantam um patamar de aprendizado a todos os estudantes."(BNCC, 2017, p.8)

Consideraremos que:

> "Na BNCC, competência é definida como mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas, cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas da vida cotidiana, do pleno exercício da cidadania e do mundo do trabalho."(BNCC, 2017, p.8)

Caracterizando essas competências a BNCC admite que a "educação deve afirmar valores e estimular ações que contribuam para a transformação da sociedade, tornando-a, também, mais justa..."(DIREITOS HUMANOS, 2013, p.47)

Dentre os objetivos gerais da Base Nacional Comum Curricular o trabalho aqui desenvolvido apresentará relação com os seguintes itens:

- "Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo a colaborar para a construção de uma sociedade justa, democrática e inclusiva."(BNCC, 2017, p.9)

- "Agir pessoalmente e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação, tomando decisões com base em princípios éticos, democráticos, inclusivos, sustentáveis e solidários."(BNCC, 2017, p.10)

Procura também assumir o compromisso de que:

> "...a Educação Básica deve visar à formação e o desenvolvimento humano global, o que implica compreender a complexidade e a não linearidade desse desenvolvimento, rompendo com visões reducionistas que privilegiam ou a dimensão intelectual (cognitiva) ou a dimensão afetiva. Significa, ainda, assumir uma visão plural, singular e integral da criança, do adolescente, do jovem e do adulto - considerando-os como sujeitos de aprendizagem - e promover uma educação voltada ao seu acolhimento, reconhecimento e desenvolvimento pleno, nas suas singularidades e diversidades."(BNCC, 2017, p.14)

> "Assim a BNCC propõe a superação da fragmentação radicalmente disciplinar do conhecimento, o estímulo à sua aplicação na vida real, a importância do contexto para dar sentido ao que se aprende e o protagonismo do estudante em sua aprendizagem e na construção de seu projeto de vida."(BNCC, 2017, p.15)

1.3 Unidades temáticas da BNCC e da Matriz de Referência ENEM

Os números primos aparecem, como objeto de conhecimento na unidade temática Números no 6º Ano do Ensino Fundamental, com o objetivo de desenvolver as habilidades "**EF06MA05** - Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000 e **EF06MA06** - Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor."(BNCC, 2017, p.299)

E pela Matriz de Referência do ENEM, temos como eixo cognitivo (comum a todas as áreas do conhecimento):

(I) **"Dominar linguagens(DL):** dominar a norma culta da Língua Portuguesa e fazer uso das linguagens matemática, artística e científica e das línguas espanhola e inglesa."

(II) **"Enfrentar situações-problema (SP):** selecionar, organizar, relacionar, interpretar dados e informações representados de diferentes formas, para tomar decisões e enfrentar situações-problema."

(IV) **"Construir argumentação (CA)** relacionar informações, representadas em diferentes formas, e conhecimentos disponíveis em situações concretas, para construir argumentação consistente."

E como competência específica de Matemática e suas tecnologias, nosso trabalho relaciona-se com a:

"Competência de área 1 - Construir significados para números naturais, inteiros, racionais e reais"

Desenvolvendo as seguintes habilidades:

(H1) "Reconhecer, no contexto social, diferentes significados e representações dos números e operações - naturais, inteiros, racionais ou reais."

(H3) "Resolver situações-problema envolvendo conhecimentos numéricos."

(H5) "Avaliar propostas de intervenção na realidade utilizando conhecimentos numéricos."

1.4 Nosso Trabalho

Como já dissemos no início do capítulo, a busca pela beleza e pelo encanto de se trabalhar com a Aritmética motivou o estudo mais aprofundado de seu principal personagem que são os números. Saber trabalhar com a composição básica desses elementos, saber que cada número (não primo) é fruto de uma combinação de fatores primos, e mais, saber que essa composição é única é muito importante para entendermos algumas características dos números e até mesmo de algumas operações que os envolvem.

Apresentar algoritmos para buscarmos números primos que talvez os alunos não acreditassem que poderiam existir, até mesmo propor indagações como, "será que em algum momento isso para?". Apresentar alguns desafios de fatorar números razoavelmente grandes. Enfim, propor algumas atividades como: construir crivos, solucionar alguns problemas serão alguns dos desafios que iremos enfrentar ao longo da construção desse trabalho para tentar torná-lo interessante e agradável. E que fique registrado um "desabafo", o maior desafio a ser enfrentado não será o de criar problemas, atividades belas e interessantes para nós educadores, mas sim atividades que envolvam, cativem e despertem a atenção e a curiosidade da comunidade escolar, em especial de nossos alunos.

No capítulo 2, por meio de exemplos apresentaremos alguns lemas e teoremas que serão necessários para demonstrarmos o Teorema Fundamental da Aritmética. Já

no capítulo 3 apresentaremos o conceito de Congruência usando exemplos numéricos e em seguida de uma maneira mais formal. Apresentaremos ainda o Pequeno Teorema de Fermat, que trabalha com o conceito de Congruência associado aos números primos. No capítulo 4 apresentaremos uma sequência didática baseada em um material concreto, elaborado durante o desenvolvimento deste trabalho. O material é um dos produtos deste trabalho de pesquisa, assim como a sequência didática proposta.

No capítulo 5 apresentamos algumas considerações finais e as atividades utilizadas na sequência didática estão disponíveis no Apêndice A.

CAPÍTULO

2

A UNICIDADE DA FATORAÇÃO

Neste capítulo será apresentado um breve estudo do conjunto dos números inteiros ($\mathbb{Z}$), em especial do conjunto dos números naturais ($\mathbb{N}$). O leitor verá que apesar de estarmos em contato com os números Naturais de forma aparentemente "natural", há muitos fatos intrigantes a serem descobertos.

Através de alguns problemas, será possível rever conceitos como múltiplos, divisores, números primos, máximo divisor comum e também a decomposição de um número em fatores primos. Ao longo dessa unidade apresentaremos alguns lemas, corolários e teoremas que serão ferramentas necessárias para provarmos que a decomposição em fatores primos é única. Alguns desses conceitos muito provavelmente o leitor já conhece, porém vamos estudá-los com um pouco mais de formalidade, mas de uma forma interessante, agradável e prazerosa de ser lida.

2.1 A divisibilidade

O conceito de número está associado, basicamente, a noções de contagem/ordem (Números Naturais); a contagem/orientação (Números Inteiros); a medidas (Números Racionais e Reais) - e com uma noção mais generalizada de orientação para o plano (Números Complexos).(RIPOLL; RANGEL; GIRALDO, 2016)

A designação do conceito de número compreende rever muitas das noções elementares a ele relacionadas. O assunto da Teoria dos Números são os números, e boa parte da Teoria dos Números é dedicada aos números inteiros. Normalmente os números naturais são usados apenas para transmitir informações quantitativas (3 pares de tênis por R$ 189,00) sem o interesse em suas propriedades. Quando contamos uma quantidade de tênis, um valor em espécie, por exemplo, é indiferente saber quantos divisores tem o 3, se 189 é um número primo ou não.(DUDLEY, 1969)

Para iniciar nossos estudos tomaremos como conhecidas as propriedades da adição, subtração, multiplicação, divisão (e/ou divisibilidade) e ordem nos inteiros. Uma propriedade que podemos destacar é que, dados dois números inteiros a e b, com $a > 0$ e qualquer b, podemos dividir b por a e deixar o menor resto possível. Essa operação é chamada de Divisão Euclidiana, que consiste em estabelecer a quantidade de múltiplos de a que podemos determinar em b, ou seja, de acordo com (HEFEZ, 2015, p.54), "existem dois números naturais q e r, unicamente determinados, tais que $b = aq + r$ com $0 \leqslant r < a$". Quando o resto dessa divisão for 0 (zero), dizemos que b é divisível por a.

Sobre o conceito de divisibilidade, podemos formalizá-lo da seguinte maneira: dados dois inteiros a e b, dizemos que a divide b e escrevemos $a \mid b$ se existir um $c \in Z$ tal que $b = a \cdot c$, ou seja, a é divisor ou fator de b ou, ainda, diremos que b é um múltiplo de a, ou b é divisível por a. Caso contrário, escrevemos $a \nmid b$ (a não divide b).

Por exemplo, $12 \mid 96$ pois $96 = 12 \cdot 8$, mas $12 \nmid 100$, pois $\nexists\, c \in Z$ tal que $100 = 12 \cdot c$.

Usaremos também duas propriedades importantes dos inteiros que são "Princípio do Menor Inteiro" - um conjunto não-vazio de inteiros que é limitado inferiormente, contém um menor elemento; e seu correspondente o "Princípio do Maior Inteiro" - um conjunto não-vazio de inteiros que é limitado superiormente, contém um maior elemento.

Para motivar os próximos resultados apresentamos aqui uma questão que foi proposta por (DUDLEY, 1969) - *Em certo país, as cédulas são de* $\$1,00$, $\$10,00$ *e* $\$25,00$. *Seria possível ter 100 cédulas totalizando* $\$500,00$*?*

Considerando a cédulas de $\$1,00$, b cédulas de $\$10,00$ e c cédulas de $\$25,00$, temos:

$$\begin{cases} a + 10b + 25c = 500 \quad (I) \\ a + b + c = 100 \quad (II) \end{cases}$$

Fazendo $(I) - (II)$ ficamos com:

$$9b + 24c = 400$$

Para responder à questão proposta vamos usar dois resultados. Um deles diz que: se tivermos três números inteiros, sendo que o menor entre eles divide os outros dois maiores, então o número menor dividirá a soma e a diferença dos outros dois. Por exemplo, tomemos os números 15, 45 e 120. É fácil verificar que $15 \mid 45$ e que $15 \mid 120$. E como $45 + 120 = 165 = 11 \cdot 15$, temos que $15 \mid (45 + 120)$, assim como $15 \mid (120 - 45) = 75$.

Esse resultado será enunciado no Lema 1, e exibida sua respectiva demonstração.

O outro resultado é uma ampliação do primeiro. Se considerarmos agora uma quantidade qualquer de números inteiros, sendo que, o menor entre eles divide o restante dos números considerados, então, esse número divide qualquer combinação linear entre

eles. Por exemplo, vamos considerar os números 7, 21, 35, 42, e 84. É fácil verificar que $7 \mid 21$, $7 \mid 35$, $7 \mid 42$, e que $7 \mid 84$. Então, se tomarmos os números 11, 13, 15 e 18, o resultado nos diz que:

$$\begin{aligned} 7 &\mid (11 \cdot 21 + 13 \cdot 35 + 15 \cdot 42 + 18 \cdot 84) \\ \Rightarrow 7 &\mid (231 + 455 + 630 + 1512) \\ \Rightarrow 7 &\mid 2828, \text{ pois } 2828 = 404 \cdot 7. \end{aligned}$$

Esse resultado será formalizado pelo Lema 2, e sua prova será exibida na sequência.

Voltemos à questão das cédulas. Com esses dois resultados, podemos concluir que se $3 \mid 9a$ e $3 \mid 24b$ então, pelo lema 2, $3 \mid 9a + 24b$, ou seja $9a + 24b$ deve ser múltiplo de 3, e não poderia ser igual a 400. Logo a resposta é não.

Lema 1. Sejam a, b e $d \in Z$, se $d \mid a$ e $d \mid b$, então $d \mid (a \pm b)$.

Prova:

Se $d \mid a$ e $d \mid b$, sabemos então que existem m e $n \in Z$, tal que:

$$\begin{cases} a = d \cdot m \\ b = d \cdot n \end{cases}$$

Logo:

$a \pm b = d \cdot m \pm d \cdot n$

$a \pm b = d \cdot (m \pm n)$

Assim, temos que, $a \pm b = d \cdot (m \pm n)$, ou seja $a \pm b$ é múltiplo inteiro de d, logo $d \mid a \pm b$.■

Lema 2. Sejam $a_1, a_2, ..., a_n, c_1, c_2, ..., c_n$ e $d \in Z$. Se $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$ então $d \mid (a_1c_1 + a_2c_2 + ... + a_nc_n)$.

Prova:

Se $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$, sabemos então que existem m_1, m_2, ..., $m_n \in Z$, tal que:

$$\begin{cases} a_1 = d \cdot m_1 \\ a_2 = d \cdot m_2 \\ \vdots \\ a_n = d \cdot m_n \end{cases}$$

Logo:

$a_1c_1 + a_2c_2 + ... + a_nc_n = dm_1c_1 + dm_2c_2 + ... + dm_nc_n$

$a_1c_1 + a_2c_2 + ... + a_nc_n = d(m_1c_1 + m_2c_2 + ... + m_nc_n)$

Portanto $d \mid (a_1c_1 + a_2c_2 + ...a_nc_n)$.■

Continuamos com mais algumas definições necessárias para o desenvolvimento de nosso estudo.

2.2 O máximo divisor comum

Sejam a, b e $d \in Z$, dizemos que d é o **Máximo Divisor Comum** de a e b (escreve-se $d = mdc(a,b)$) se, e somente se:

(i) $d > 0$;

(ii) $d \mid a$ e $d \mid b$;

(iii) se $c \mid a$ e $c \mid b$, então $c \leq d$.

A condição (i) diz que d é um divisor comum de a e b; e (ii) diz que ele (d) é o maior de todos os divisores comuns.

Vejamos alguns exemplos, $mdc(60,84) = 12$ e $mdc(91,135) = 1$.

Notemos que $mdc(0,0)$ não é definido, mas se a e b forem ambos inteiros não nulos, então o conjunto de todos os seus divisores comuns é um conjunto de inteiros que é limitado superiormente pelo maior divisor comum entre eles. De fato, se $mdc(a,b)$ for definido, então é positivo, ou seja, $mdc(a,b) \geq 1$, pois $1 \mid a$ e $1 \mid b$ para quaisquer inteiros a e b.

Como exemplo, apresentamos uma maneira para calcular o valor de $mdc(343,280)$:

1. Primeiro dividimos o maior valor entre eles pelo menor, que podemos expressar da seguinte maneira:

	1				
343	280				
	63				

   Na tabela acima, nessa primeira etapa, na segunda linha temos 343 como o dividendo e 280 como o divisor. Neste caso, o quociente dessa divisão colocamos na primeira linha logo acima do divisor, ou seja, nesse caso o quociente é igual a 1. E o resto da divisão colocamos abaixo do divisor, que nesse caso é igual a 63.

2. Dividiremos agora o 280 pelo resto da divisão anterior, o 63, resultando:

	1	4			
343	280	63			
	63	28			

   Já nessa segunda etapa, temos, na segunda linha, o 280 como novo dividendo e o 63 como novo divisor. Na primeira linha, logo acima do 63, temos o 4 que é o quociente, e na terceira linha logo abaixo do 63 o 28, que é o resto dessa divisão.

3. Continuando com esse procedimento, dividiremos agora o 63 pelo resto 28, então temos:

	1	4	2		
343	280	63	28		
	63	28	7		

Já nessa terceira etapa temos, na segunda linha os números 63 e 28 como dividendo e divisor, respectivamente. Na primeira linha logo acima do 28 o quociente 2, e na terceira linha logo abaixo do 28 o resto 7.

4. Prosseguindo, dividiremos agora o 28 pelo 7, obtendo:

	1	4	2	4	
343	280	63	28	7	
	63	28	7	0	

Novamente na segunda linha colocamos o dividendo 28 e o divisor 7. Na primeira linha, acima do 7 colocamos o 4 que é o quociente, abaixo do 7 o 0 que é o resto da divisão. Nesse momento, ou seja, no momento em que o resto da divisão é 0 (zero), finalizamos nosso cálculo e concluímos que o $mdc(343;280) = 7$.

É interessante notar que se fizermos o cálculo de trás pra frente, temos que:

$$\begin{aligned}
7 &= 63-(2\cdot 28)\\
7 &= 63-[2\cdot(280-4\cdot 63)]\\
7 &= 63-2\cdot 280+8\cdot 63\\
7 &= 9\cdot 63-2\cdot 280\\
7 &= [9\cdot(343-1\cdot 280)]-2\cdot 280\\
7 &= 9\cdot 343-9\cdot 280-2\cdot 280\\
7 &= 9\cdot 343-11\cdot 280.
\end{aligned}$$

Encontramos x e y tal que $343x+280y=7$, ou seja, $x=9$ e $y=-11$. Com essas ideias em mente podemos enunciar o seguinte teorema.

Teorema 1. Se a e $b \in Z$ e $mdc(a;b) = d$, então há inteiros x e y tais que $ax+by=d$.

Prova:

Considere $C = \{a\cdot x+b\cdot y;\ x,y \in Z\}$ e $n = a\cdot x_0+b\cdot y_0$ onde n é o menor elemento natural de C. Supondo, por absurdo, que $n \nmid a$, então:

$$a = n\cdot q+r \quad \text{com} \quad 0<r<n:$$

$$r = a - n \cdot q$$

Substituindo $n = a \cdot x_0 + b \cdot y_0$ na equação acima ficamos com:

$$\begin{aligned} r &= a - (a \cdot x_0 + b \cdot y_0) \cdot q \\ r &= a - a \cdot q \cdot x_0 - b \cdot q \cdot y_0 \\ r &= a \cdot (1 - q \cdot x_0) + b \cdot (-q \cdot y_0) \end{aligned}$$

Logo r é uma combinação linear de a e b, então $r \in C$. Mas isso é um absurdo, pois $0 < r < n$, e n é o menor elemento de C, portanto podemos concluir que $n \mid a$. Analogamente, $n \mid b$, assim n é divisor comum de a e b. Por hipótese temos que $d = mdc(a;b)$, logo:

$$\begin{aligned} d \mid a \quad &\Rightarrow \quad a = d \cdot q_1 \\ d \mid b \quad &\Rightarrow \quad b = d \cdot q_2 \end{aligned}$$

Mas $n = a \cdot x_0 + b \cdot y_0$, então:

$$\begin{aligned} n &= (d \cdot q_1) \cdot x_0 + (d \cdot q_2) \cdot y_0 \\ n &= d \cdot q_1 \cdot x_0 + d \cdot q_2 \cdot y_0 \\ n &= d \cdot (q_1 \cdot x_0 + q_2 \cdot y_0) \end{aligned}$$

Logo $d \mid n$, e portanto $d \leq n$. Mas d é o maior divisor comum de a e b, logo temos que $d = ax_0 + by_0$ e $d = n$.■

Corolário 1. Se $d \mid ab$ e $mdc(d;a) = 1$, então $d \mid b$.

Prova:

Como $mdc(d;a) = 1$, então, pelo Teorema 1, sabemos que existem números inteiros x e y tais que:

$$dx + ay = 1 \tag{2.1}$$

Multiplicando ambos os lados da equação 2.1 por b, temos $(dx)b + (ay)b = b$, cujo primeiro termo, $(dx)b = d(xb)$ é divisível por d, e cujo segundo termo, $(ay)b = (ab)y$ é divisível por d, por hipótese. Assim d divide b, como queríamos demonstrar.■

Notemos que se $mdc(a,d) \neq 1$ no Corolário 1, então a conclusão é falsa. Por exemplo, $6 \mid 9 \cdot 4$, mas $6 \nmid 9$ e $6 \nmid 4$, porém o $mdc(6,9) \neq 1$ e $mdc(6,4) \neq 1$.

Esse corolário diz algo que usamos sem pensar: se um número d divide o produto de outros dois números, a e b e d e a não têm divisores comuns além do 1, então necessariamente d tem que dividir b.

2.3 A unicidade da fatoração

Vamos começar essa seção com o seguinte problema:

> "Uma professora distribuiu 286 bombons igualmente entre seus alunos do 6º ano. No dia seguinte, ela distribuiu outros 286 bombons, também igualmente, entre seus alunos do 7º ano. Os alunos do 7º ano reclamaram que cada um deles recebeu 2 bombons a menos que os alunos do 6º ano. Quantos alunos a professora tem no 7º ano?"

Para abordarmos esse problema vamos explorar de quantas maneiras podemos dividir 286 balas.

$$286 = 2 \cdot 143 = 2 \cdot 11 \cdot 13 \tag{2.2}$$

Notamos que não conseguimos mais "quebrar" em pares de inteiros os números 2, 11 e 13. Mas, como a multiplicação goza das propriedades comutativa e associativa, podemos então, a partir dos números 2, 11 e 13 construir outras multiplicações que geram o 286, como segue abaixo:

$$286 = 2 \cdot 143 = 2 \cdot 11 \cdot 13 = \begin{cases} 1 \cdot 286 \\ 2 \cdot (11 \cdot 13) = 2 \cdot 143 \\ 11 \cdot (2 \cdot 13) = 11 \cdot 26 \\ 13 \cdot (2 \cdot 11) = 13 \cdot 22 \end{cases} \tag{2.3}$$

Obtemos assim uma lista de todos as "partes"que podem gerar o 286 através de uma multiplicação. Essas partes são chamadas de fatores ou de divisores naturais de 286. Denotando por $D(286)$ o conjunto dos divisores naturais de 286, temos que:

$$D(286) = \{1, 2, 11, 13, 22, 26, 143, 286\} \tag{2.4}$$

Como os únicos divisores de 286 que diferem de duas unidades são o 11 e o 13, e como $286 = 11 \cdot 26$, temos que cada aluno da turma de 26 alunos do 7º Ano recebeu 11 bombons. Por outro lado, para completar, como $286 = 13 \cdot 22$, foram dados 13 bombons para os 22 alunos do 6º ano. Vale a pena refletirmos se a professora poderia, em outra sala, distribuir outros 286 bombons e cada aluno receber 12 bombons. Como vimos em 2.2, 2.3 e 2.4 não existe nenhum número n, com $n \in N$, tal que $12 \cdot n = 286$, ou seja, não é possível dividir em 12 partes inteiras o número 286.

Vamos retornar à forma decomposta dos números para notarmos algo interessante:

$$\frac{286}{11} = \frac{2\cdot 11\cdot 13}{11} = 2\cdot 13 = 26 \tag{2.5}$$

$$\frac{286}{12} = \frac{2\cdot 11\cdot 13}{2\cdot 2\cdot 3} = \frac{11\cdot 13}{2\cdot 3} \tag{2.6}$$

Em 2.6 fica claro que não é possível efetuar mais nenhuma simplificação e muito menos efetuar uma divisão inteira com os números envolvidos. Logo 12 não divide 286, ou ainda, 286 não é divisível por 12. Vamos destacar os números 2, 11 e 13 e comentar sobre algumas de suas características peculiares.

Estes números, conforme notamos, não podem ser "quebrados"em blocos menores naturais, pois são números que têm apenas dois divisores naturais, o 1 e ele mesmo.

Números inteiros, maiores que 1, que têm apenas dois divisores naturais, o 1 e ele mesmo, são chamados de números primos. Um inteiro maior que 1 que não é primo é chamado de número composto. Logo, os números 2, 3, 5, 7, 11, 13, ... são números primos e os números 4, 6, 8, 9, 10, 12, 15, ... são números compostos. Os números 0 e 1 não entram nessas classificações.

Em geral, na educação básica, os números primos são utilizados apenas como os elementos de uma fatoração, que por sua vez é aplicada apenas como uma ferramenta auxiliar para determinar o cálculo do Máximo Divisor Comum (mdc) ou do Mínimo Múltiplo Comum (mmc), empregados na resolução de algumas situações-problema e no caso do mmc, para somar ou subtrair frações com denominadores diferentes. De modo geral não leva-se em conta se existe apenas uma maneira de fatorar um número ou não.

Podemos dizer que a circunstância da fatoração ser única, parece óbvia e evidente, dependendo de nossa habilidade e familiaridade com as propriedades dos números inteiros. Porém Dudley em (DUDLEY, 1969) apresentou um estudo interessante ao considerar um subconjunto de $\mathbb{N}$ onde a fatoração não é única. Dentre os elementos desse subconjunto, aqueles que eram divisíveis apenas por 1 e por ele mesmo foram chamados de "Promes". Apresentaremos a seguir um outro subconjunto de $\mathbb{N}$ onde a fatoração também não é única para ilustrarmos esse estudo.

Considere um subconjunto T dos Naturais, contendo todos os números da forma $3n+1$, com $n = 0,1,2,3,....$ Chamaremos de Mínion o elemento de T que não tiver divisores diferentes de 1 e dele mesmo em T, ou seja:

$$T = \{t \in \mathbb{N} : t = 3n+1\}$$

Logo, os números $1,4,7,10,13,...,19,...,43,...,52,...,109,...,460,...,1210,...$ são elementos do conjunto T. O 4, o 10 e o 19 são exemplos de Mínions, enquanto $52 = 4\cdot 13$ não

é. Os números 460 e 1 210 são exemplos cuja fatoração em Mínions não é única, como segue:

$$\begin{aligned} 10 \cdot 46 &= 460 = 4 \cdot 115 \\ 22 \cdot 55 &= 1210 = 10 \cdot 121 \end{aligned}$$

Vemos que o 460 poderia ser decomposto no produto de 10 por 46 ($46 = 3 \cdot 15 + 1$), e também no produto 4 por 115 ($115 = 3 \cdot 38 + 1$). O mesmo ocorre com o número 1210 em relação aos números 22 ($22 = 3 \cdot 7 + 1$) e 55 ($55 = 3 \cdot 18 + 1$), ou em relação aos números 10 e 121 ($121 = 3 \cdot 40 + 1$).

O que vamos provar aqui é que no conjunto dos Números Naturais isso não é possível, pois o subconjunto do conjunto dos Números Naturais que contém números cujos divisores são o 1 e ele mesmo, decompõem os Números Naturais de maneira única.

A partir de alguns Lemas e Teoremas, apresentaremos algumas consequências e aplicações da Unicidade da Fatoração e, em particular, a importância dessas partículas indivisíveis chamada de Números Primos.

Como já citamos anteriormente, os números inteiros, maiores que 1 que são divisíveis apenas por 1 e por ele mesmo, chamados de Números Primos são interessantes e enigmáticos:

> "Esses números são os próprios átomos da aritmética. São os números indivisíveis que não podem ser representados pela multiplicação de dois números menores... Todo número não primo pode ser formado pela multiplicação desses blocos de construção Primos. Cada uma das moléculas do mundo físico é composta por átomos da tabela periódica de elementos químicos. Uma lista dos primos é a tabela periódica do Matemático."(SAUTOY, 2007, p.13)

Nosso objetivo nesta seção é provar que todo número inteiro maior que 1, que não é primo, pode ser escrito como produto de Números Primos, e o mais importante, de maneira única.

Vamos a princípio provar que todo número inteiro n, maior que 1, é divisível por, pelo menos, um primo. Utilizaremos, sempre que possível, ao longo de nossas demonstrações, exemplos numéricos para que fique mais clara sua visualização.

Lema 3. Todo inteiro n, $n > 1$, é divisível por um Número Primo.

Prova:

Tomemos n um número inteiro maior que 1. Então temos que:

- (I) n é primo, ou;

- (II) n é composto.

Vamos analisar cada um dos casos separadamente:

- (I) n é primo: se n for primo, por definição, ele é divisível por 1 e por *ele mesmo*, logo é divisível por um primo.

Por exemplo: 17 é um número primo e $17|17$, pois $17 = 1 \cdot 17$

- (II) n é composto: se n não for primo então temos um conjunto de elementos que dividem n, com pelo menos mais um elemento além do 1 e dele mesmo. Seja:

$$D(n) = \{1; d_1; d_2; ...; d_i; n\}$$

Escrevendo $D(n) = \{1\} \bigcup \{d_1; d_2; ...; d_i\} \bigcup \{n\}$, vamos destacar o subconjunto de $D(n)$ formado pelos divisores de n maiores que 1 e menores que ele mesmo, ou seja:

$$\{d_i \in D(n) : 1 < d_i < n\}$$

O "Princípio do Menor Elemento"(DUDLEY, 1969) nos garante que algum dos d_i's é o menor elemento, que chamaremos simplesmente de d. Se d tivesse um divisor maior que 1 e menor que ele mesmo, esse divisor também seria divisor de n e seria menor que d, mas isso é impossível, pois d é o menor dos elementos desses divisores, logo d é primo e n tem um divisor primo.■

Para exemplificar a parte **(II)** da prova do Lema 3 vamos considerar o número 36. O conjunto dos divisores de 36 é:

$$D(36) = \{1; 2; 3; 4; 6; 9; 12; 18; 36\} = \{1\} \bigcup \{2; 3; 4; 6; 9; 12; 18\} \bigcup \{36\}$$

Destacando apenas o subconjunto dos divisores de 36, maiores que 1 e menores que ele mesmo ficamos com $\{2; 3; 4; 6; 9; 12; 18\}$. Esse conjunto apresenta um menor elemento, nesse caso o 2, que é primo.

Vamos supor por absurdo que 4 seja o menor dos elementos acima. O número 4 apresenta como divisor, maior que 1 e menor que ele mesmo o número 2. Mas 2 também é divisor de 36 e, portanto, 4 não é o menor elemento.

Com o auxílio do Lema 3, podemos provar que cada inteiro positivo pode ser escrito como um produto de primos.

Lema 4. Todo inteiro n, $n > 1$, pode ser escrito como um produto de primos.

Prova:

Pelo Lema 3, sabemos que existe pelo menos um número primo p_1, tal que $p_1|n$. Logo n pode ser escrito da forma:

$$n = n_1 \cdot p_1, \text{ com } 1 \leq n_1 < n$$

Se $n_1 = 1$ então $n = 1 \cdot p_1 = p_1$, e não há nada a ser feito.

Se $n_1 > 1$ então, pelo Lema 3, temos novamente, que existe um número primo p_2 que divide n_1. Logo n_1 pode ser escrito da forma:

$$n_1 = n_2 \cdot p_2, \text{ com } 1 \leq n_2 < n_1$$

Se $n_2 = 1$, então $n_1 = 1 \cdot p_2 = p_2$, e portanto $n = p_2 \cdot p_1$, que representa n através de um produto de primos.

Se $n_2 > 1$ então, pelo Lema 3, temos novamente que existe um número primo p_3 que divide n_2. Logo n_2 pode ser escrito da forma:

$$n_2 = n_3 \cdot p_3 \text{ com } 1 \leq n_3 < n_2$$

Se $n_3 = 1$, ficamos com:

$$n_2 = 1 \cdot p_3 = p_3 \text{ e}$$

$n = n_1 \cdot p_1 = n_2 \cdot p_2 \cdot p_1 = p_3 \cdot p_2 \cdot p_1$ que é uma expressão que representa n através de um produto de primos.

Se $n_3 > 1$, continuamos até chegar a um $n_i = 1$, pois $n > n_1 > n_2 > n_3 > ... > n_i$ e cada um dos n_i's é positivo.

Tal sequência não pode ser infinita, pois está contida no conjunto dos divisores naturais de n. Portanto para algum n_{i-1}, teremos que:

$n_{i-1} = n_i \cdot p_i = 1 \cdot p_i = p_i$ e n fica escrito da forma:

$n = n_1 \cdot p_1 = n_2 \cdot p_2 \cdot p_1 = ... = n_{i-1} \cdot p_{i-1} \cdot ... \cdot p_2 \cdot p_1 = p_i \cdot p_{i-1} \cdot ... \cdot p_2 \cdot p_1$ que é uma expressão que representa n através de um produto de números primos.■

Para exemplificarmos o Lema 4 tomemos o número 900. Como 900 é par logo é um múltiplo de 2, portanto: $900 = 450 \cdot 2$, com $n_1 = 450$ e $p_1 = 2$.

Como $n_1 > 1 \Rightarrow 450 = n_2 \cdot p_2$, com $n_2 = 225$ e $p_2 = 2$, ou seja $450 = 225 \cdot 2$. Continuamos seguidamente "quebrando"os números compostos em produtos de fatores primos:

- $\Rightarrow n_2 > 1$, então $225 = n_3 \cdot p_3$, com $n_3 = 75$ e $p_3 = 3$, ou seja $225 = 75 \cdot 3$.
- $\Rightarrow n_3 > 1$, então $75 = n_4 \cdot p_4$, com $n_4 = 25$ e $p_4 = 3$, ou seja, $75 = 25 \cdot 3$.
- $\Rightarrow n_4 > 1$, então $25 = n_5 \cdot p_5$, com $n_5 = 5$ e $p_5 = 5$, ou seja, $25 = 5 \cdot 5$.
- $\Rightarrow n_5 > 1$, então $5 = n_6 \cdot p_6$, com $n_6 = 1$ e $p_6 = 5$. Como $n_6 = 1$ temos que $p_6 = n_5$ é um número primo.

Então, sintetizando temos:

900	2
450	2
225	3
75	3
25	5
5	5
1	

Agrupando as bases iguais temos que $900 = 5^2 \cdot 3^2 \cdot 2^2$ que é uma expressão que representa 900 através de um produto de números primos.

Antes de mostrar que cada inteiro positivo tem apenas uma única decomposição em fatores primos, provaremos um teorema simples, porém fundamental, sobre esses números: trata-se da existência de infinitos números primos. Uma demonstração deste teorema foi proposta por Euclides (300 a.C.) em sua obra Os Elementos, uma das obras mais influentes da história.(GARBI, 2008)

Teorema 2. (Euclides 300 a.C.): Existem infinitos números primos.

A ideia proposta por Euclides é simples. Ela começa pelo fato descrito no Lema 4, de que todo inteiro n, $n \geq 2$, pode ser escrito como produto de primos. Tomemos os primos 2, 3, 5 e 7 já citados anteriormente. Euclides multiplicou-os, obtendo $2 \cdot 3 \cdot 5 \cdot 7 = 210$, e então - seu toque de gênio - adicionou 1 ao produto, obtendo 211.

Como vimos no Lema 3, todo inteiro n, $n > 1$, é divisível por um primo. O que dizer do número 211? Ele claramente não é divisível por 2, 3, 5 ou 7, logo deve haver outros primos que não foram incluídos na lista, que geram o número 211. Neste caso, 211 é primo, mas realmente Euclides não defendia o fato de que um número obtido dessa forma seria sempre primo, mas sim que, existem outros primos que constituem esse número e que não estão na lista.

A tabela a seguir (DUDLEY, 1969) mostra como ao adicionar 1 ao produto $p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r$; exibiremos um novo número primo diferente de p_1, p_2, p_3, ..., p_r.

r	p_r	$p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r + 1$	*Divisores Primos*
1	2	3	3
2	3	7	7
3	5	31	31
4	7	211	211
5	11	2 311	2 311
6	13	30 031	59; 509
7	17	510 511	19; 97; 277
8	19	9 699 691	347; 27 953

Tabela 1 – (DUDLEY, 1969)

Agora vamos ver uma prova formal do Teorema 2.

Prova:

Considere a hipótese de que a quantidade de números primos seja finita e que p_1, p_2, p_3, ..., p_r são todos os números primos existentes. Considere n um número inteiro que seja o produto desses números, ou seja, $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r$.

Tomemos agora o sucessor de n, ou seja, $n+1 = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r + 1$. O número $n+1$ não pode ser primo, pois todos os números primos existentes estão na composição de n, portanto $n+1$ é composto. Pelo Lema 3, $n+1$ é divisível por um número primo denotado por p_i. Logo, temos que $n+1 = k_1 \cdot p_i$ com $k_1 \in \mathbb{Z}$, mas n, por definição, é o produto de todos os números primos existentes, então n também é divisível por p_i, logo $n = k_2 \cdot p_i$ com $k_2 \in \mathbb{Z}$. Portanto ficamos com:

$$\begin{cases} n+1 = k_1 \cdot p_i \quad (I) \\ n = k_2 \cdot p_i \quad (II) \end{cases}$$

Substituindo (II) em (I) vem:

$$k_2 \cdot p_i + 1 = k_1 \cdot p_i \Rightarrow k_1 \cdot p_i - k_2 \cdot p_i = 1 \Rightarrow (k_1 - k_2) \cdot p_i = 1$$

Concluímos então que 1 também é múltiplo de p_i, consequentemente 1 é divisível por p_i. Mas isso é absurdo, pois, por definição, temos que, p_i sendo primo, é maior que 1. Logo p_i não pode dividir 1.

Portanto, a hipótese de que temos uma quantidade finita de números primos é um absurdo e concluímos que existem infinitos números primos.■

Os lemas seguintes, provados nos "Elementos de Euclides", darão os resultados que tornarão possível demonstrar a unicidade da fatoração.

Lema 5. Seja p um número primo, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Prova:

Uma vez que p seja primo, seus únicos divisores são 1 e p. Então $mdc(p,a) = p$ ou $mdc(p,a) = 1$. No primeiro caso, $p \mid a$ e a prova está concluída. No segundo caso, temos que, p e a são primos entre si, logo o Corolário 1 nos diz que $p \mid b$ e concluímos o que queríamos demonstrar.■

Lema 6. Seja p um número primo, se $p \mid a_1a_2...a_k$, então $p \mid a_i$ para algum i, $i = 1,2,...,k$.

Prova:

O Lema 6 é verdadeiro por inspeção para $k = 1$, e pelo Lema 5 é verdadeiro se $k = 2$. Procederemos por indução. Suponha que o Lema 6 seja verdadeiro para $k = r$. Suponhamos então, que $p \mid a_1a_2...a_{r+1} \rightarrow p \mid (a_1a_2...a_r)a_{r+1}$, e o Lema 5 nos permite concluir que $p \mid a_1a_2...a_r$ ou $p \mid a_{r+1}$. No primeiro caso, a hipótese de indução nos garante que $p \mid a_i$ para algum $i = 1,2,...,r$ e o lema está provado.■

Lema 7. Se q_1, q_2, ..., q_n e p forem primos e se $p \mid q_1q_2...q_n$, então $p = q_k$, para algum $1 \leqslant k \leqslant n$.

Prova:

A partir do Lema 6, sabemos que $p \mid q_k$ para algum $1 \leqslant k \leqslant n$. Uma vez que p e q_k são primos, $p = q_k$, pois q_k, sendo primo, tem como únicos divisores o 1 e o próprio q_k. e p sendo primo, não é igual a 1.■

Teorema 3. (Teorema da Fatoração Única) - Qualquer inteiro positivo pode ser escrito como produto de primos de uma só maneira.

Prova:

Lembrando que consideramos como idênticas todas as fatorações que diferem apenas pela ordem dos fatores. Já sabemos a partir do Lema 4 que qualquer inteiro n, $n > 1$ pode ser escrito como um produto de primos. Assim, para completar a prova do teorema, precisamos mostrar que n não pode ter duas dessas representações. Então temos que mostrar que os mesmos primos aparecem em cada produto, e o mesmo número de vezes, embora sua ordem possa ser diferente. Ou ainda, devemos mostrar que os números primos p_1, p_2, ..., p_m são apenas um rearranjo dos números primos q_1, q_2, ..., q_r e $m = r$, isto é:

$$\begin{aligned} n = p_1 \cdot p_2 \cdot ... \cdot p_m \quad &\text{e} \quad n = q_1 \cdot q_2 \cdot ... \cdot q_r \\ \Rightarrow p_1 \cdot p_2 \cdot ... \cdot p_m \quad &= \quad q_1 \cdot q_2 \cdot ... \cdot q_r \end{aligned}$$

Se $p_1 | n$ então existe $i \in \{1,2,...,r\}$ tal que $q_i = p_1$, e portanto:

$$\frac{n}{q_i} = \frac{n}{p_1} = q_1 \cdot q_2 \cdot ... \cdot q_{i-1} \cdot q_{i+1} \cdot ... \cdot q_r \quad .$$

Se $p_2|n$ então $q_j|n$ para algum $j \in \{1,2,..i-1,i+1,...,r\}$ tal que $p_2 = q_j$. Logo:

$$\frac{n}{q_i \cdot q_j} = \frac{n}{p_1 \cdot p_2} = q_1 \cdot q_2 \cdot ... \cdot q_{j-1} \cdot q_{j+1} \cdot ... \cdot q_{i-1} \cdot q_{i+1} \cdot ... \cdot q_r$$

Se $m < r$ teremos

$$\frac{n}{p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot ... \cdot p_m} = 1,$$

e

$$\frac{n}{p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot ... \cdot p_m} = q_{k_{m+1}} \cdot q_{k_{m+2}} \cdot ... \cdot q_{k_r}$$

Levando a um absurdo:

$$1 = q_{k_{m+1}} \cdot q_{k_{m+2}} \cdot ... \cdot q_{k_r}.$$

O mesmo acontece se $m > r$, e portanto $m = r$. Como vimos, a cada etapa, existe um número primo p_i, $i \in \{1,2,..,m\}$ que corresponde a um primo q_j, $j \in \{1,2,...,r\}$, e não necessariamente com $i = j$, ou seja, os números p_1, p_2, ..., p_m são um rearranjo de q_1, q_2, ..., q_r, e as duas fatorações podem se diferenciar apenas na ordem de seus fatores.■

CAPÍTULO

3

CONGRUÊNCIAS E O PEQUENO TEOREMA DE FERMAT

Nesta unidade apresentaremos “uma das noções mais fecundas da aritmética”(HEFEZ, 2014, p.192) chamada de congruência ou também conhecida como aritmética dos restos. Mostraremos a relação entre números primos e a congruência através do Pequeno Teorema de Fermat. Procuraremos expor conceitos e resultados de uma maneira menos intrincada, deixando algumas provas e demonstrações para o leitor mais interessado.

3.1 Congruências

Iniciamos nosso trabalho apresentando as congruências por meio de um relógio tradicional que marca até 12 horas. Passadas 4 horas a partir das 10 horas, olhamos o relógio e vemos que são 2 horas, fato que estamos acostumados. Quando o ponteiro das horas retorna ao 12 inicia-se a contagem novamente, ou seja, temos que $10+4=14$ é o mesmo que $12+2$, ou melhor, 2 horas. Esse processo é o mesmo que achar o resto da divisão da soma dos tempos por 12.

Nesse exemplo consideramos como “módulo 12”, pois 12 é nossa referência, ou melhor, nosso ponto de partida da recontagem das horas. Isso ocorre, pois de 12 em 12 horas percorremos um período completo nesse relógio tradicional, logo, 13 horas, por exemplo, é o mesmo que 1 hora, já 18 horas é o mesmo que 6 horas. A partir de agora denominaremos esse relógio como calculadora-relógio, pois será a nossa ferramenta de cálculo, e diremos, por exemplo, que 13 é congruente a 1 módulo 12 e 18 é congruente a 6 módulo 12 e para representarmos essas congruências utilizaremos a seguinte notação:

$$13 \equiv 1 \text{ (módulo 12)}$$

$$18 \equiv 6 \text{ (módulo 12)}$$

Vejamos agora o que ocorre quando saímos do relógio tradicional de 12 horas e usamos outro relógio que marca até 15 horas. Vejamos a seguinte situação, $13+8$ módulo 15, como $13+8=21$, e o 21 quando dividido por 15 deixa resto 6, dizemos que $13+8$ é congruente a 6 módulo 15, ou ainda:

$$13+8 \equiv 6 \text{ (módulo 15)}$$

Como faríamos para multiplicar numa calculadora-relógio? Sabemos que a multiplicação é uma sequência de somas de mesmas parcelas, por exemplo, 4×10 significa somar quatro números 10. Para exemplificar essa situação, retornaremos a uma calculadora-relógio que marca até 12 pois é mais prático para ser utilizado em sala de aula já que esse tipo de relógio é "familiar"entre os alunos. Vejamos a seguinte situação:

$$\begin{aligned} 10 &\equiv 10 \text{ (módulo 12), pois } 10 = 0{\cdot}12{+}10 \\ 20 &\equiv 8 \text{ (módulo 12), pois } 20 = 1{\cdot}12{+}8 \\ 30 &\equiv 6 \text{ (módulo 12), pois } 30 = 2{\cdot}12{+}6 \\ 40 &\equiv 4 \text{ (módulo 12), pois } 40 = 3{\cdot}12{+}4 \end{aligned}$$

Notamos que, nesse caso (módulo 12), para cada múltiplo de 10 o "ponteiro"do relógio recua 2 horas, ou seja em quatro "grupos"de 10 o relógio irá recuar $4 \times 2 = 8$ horas, logo $12-8=4$. É o mesmo que $40 \equiv 4$ (módulo 12).

Consideramos agora a situação no caso da multiplicação ser 6×10. Já sabemos que $4 \times 10 \equiv 4$ (módulo 12), então:

$$\begin{aligned} 40 &\equiv 4 \text{ (módulo 12), pois } 40 = 3{\cdot}12{+}4 \\ 50 &\equiv 2 \text{ (módulo 12), pois } 50 = 4{\cdot}12{+}2 \\ 60 &\equiv 0 \text{ (módulo 12), pois } 60 = 5{\cdot}12{+}0 \end{aligned}$$

Logo, no caso, 6×10, o ponteiro recuou $6 \times 2 = 12$ horas até parar novamente em 12. E como o zero é um número importante, denominamos essa posição como sendo o 0 (zero) numa calculadora-relógio de 12 horas, pois todo número que é múltiplo de 12, deixa resto 0 (zero) numa divisão por 12. Isso ocorre pois a aritmética dos restos ou congruência está associada a fenômenos periódicos, ou seja, ocorre ou se repete em intervalos regulares.(COUTINHO, 2015)

Vejamos agora a seguinte situação, $15 \equiv 3$ módulo 12, pois $15 = 1 \cdot 12 + 3$ e $14 \equiv 2$ módulo 12, pois $14 = 1 \cdot 12 + 2$ e quando efetuamos a multiplicação 15×14 temos o produto igual a 210 e $210 \equiv 6$ módulo 12, pois $210 = 17 \cdot 12 + 6$. Chamamos a atenção nesse momento para notarmos que o 3 e 2 são, respectivamente, as congruências de 15 e 14 módulo 12. Esse fato será descrito pela Proposição 3.

$$\begin{aligned} 15 &\equiv 3 \text{ (módulo 12)} \\ 14 &\equiv 2 \text{ (módulo 12)} \\ 15 \cdot 14 &\equiv 3 \cdot 2 \equiv 6 \text{ (módulo 12)} \end{aligned}$$

E como funcionaria a operação de potência numa calculadora-relógio? Tomemos 10^4, que representa multiplicar o 10 por ele mesmo quatro vezes. Logo:

$$\begin{aligned} 10 &\equiv 10 \text{ (módulo 12)} \\ 10^2 = 100 &\equiv 4 \text{ (módulo 12), pois } 100 = 8{\cdot}12{+}4 \\ 10^3 = 1000 &\equiv 4 \text{ (módulo 12), pois } 1000 = 83{\cdot}12{+}4 \\ 10^4 = 10000 &\equiv 4 \text{ (módulo 12), pois } 10000 = 833{\cdot}12{+}4 \end{aligned}$$

É interessante observar que:

$$\begin{aligned} 10^2 &\equiv 4 \text{ (módulo 12)} \\ 10^2 \cdot 10 &\equiv 4 \cdot 10 \equiv 4 \text{ (módulo 12)} \\ 10^3 &\equiv 40 \equiv 4 \text{ (módulo 12)} \\ 10^3 &\equiv 4 \text{ (módulo 12)} \\ 10^3 \cdot 10 &\equiv 4 \cdot 10 \equiv 4 \text{ (módulo 12)} \\ 10^4 &\equiv 40 \equiv 4 \text{ (módulo 12)} \\ 10^4 &\equiv 4 \text{ (módulo 12)} \end{aligned}$$

A grande magia da calculadora-relógio está justamente no fato de que muitas vezes não precisamos saber o valor de um produto ou até mesmo de uma potência para determinarmos o resto da divisão de um número inteiro a por um número natural m.(SAUTOY, 2013)

Vamos analisar uma sugestão de cálculo proposta por Sautoy em (SAUTOY, 2013). Procuremos, a posição que marcará o ponteiro para 7^{99} numa calculadora-relógio de 12 horas (o que corresponde a determinar o resto da divisão de 7^{99} por 12).

$$\begin{aligned} 7^1 &\equiv 7 \text{ (módulo 12)} \\ 7^2 = 49 &\equiv 1 \text{ (módulo 12), pois } 49 = 4\times12+1 \\ 7^3 = 343 &\equiv 7 \text{ (módulo 12), pois } 343 = 28\times12+7 \\ 7^4 = 2401 &\equiv 1 \text{ (módulo 12), pois } 2401 = 200\times12+1 \\ 7^5 = 16807 &\equiv 7 \text{ (módulo 12), pois } 16807 = 1400\times12+7 \end{aligned}$$

Analisando este exemplo, verificamos que há um padrão. Quando o expoente é par o resto é 1 e quando o expoente é ímpar o resto é 7, o que nos leva a acreditar que 7^{99} deixa resto 7 numa calculadora-relógio de 12 horas. Porém seremos um pouco mais criteriosos, utilizando algumas propriedades da potência.

Para desenvolver esses cálculos utilizaremos várias vezes a igualdade $7^3 \equiv 7$ (módulo 12). Vejamos:

$$\begin{aligned} 7^{99} = (7^3)^{33} &\equiv 7^{33} \text{ (módulo12)} \\ 7^{99} &\equiv 7^{33} \equiv (7^3)^{11} \equiv 7^{11} \text{ (módulo12)} \\ 7^{99} &\equiv 7^{11} \equiv (7^3)^3 \cdot 7^2 \text{ (módulo12)} \\ 7^{99} &\equiv 7^{11} \equiv 7^3 \cdot 7^2 \text{ (módulo12)} \\ 7^{99} &\equiv 7 \cdot 7^2 \text{ (módulo12)} \\ 7^{99} &\equiv 7^3 \text{ (módulo12)} \\ 7^{99} &\equiv 7 \text{ (módulo12)} \end{aligned}$$

Portanto, 7^{99} deixa resto 7 na divisão por 12. Essa propriedade será enunciada no Corolário 2, na página 52.

Apresentaremos a seguir a Aritmética dos Restos de uma maneira formal.

Comecemos definindo o "mod m", que já foi bastante usado no texto, e para o qual esperamos que os exemplos escolhidos tenham dado certa intuição a respeito.

> "Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se $a \equiv b$ (mod m)."(HEFEZ, 2014, p.192)

Por exemplo $102 \equiv 47$ (mod 5), pois os restos da divisão de 102 e 47 por 5 são iguais a 2.

Decorre imediatamente da definição que a congruência módulo m, é uma relação de equivalência. Vamos enunciar isso explicitamente abaixo. (HEFEZ, 2014)

Proposição 1. Seja $m \in \mathbb{N}$. Para todos a, b, $c \in \mathbb{Z}$, tem-se que:

(i) $a \equiv a \pmod{m}$;

(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Para verificarmos se dois números inteiros a e b são congruentes módulo m não necessitamos efetuar a divisão de cada um deles por m e depois comparar os restos, basta aplicar o seguinte resultado:

Proposição 2. Suponha que a, b, $m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid (b-a)$.

Prova:

($\Rightarrow$): $a \equiv b \pmod{m} \Rightarrow m \mid (b-a)$

Considere $a = m \cdot q_1 + r_1$, com $0 \leqslant r_1 < m$, e $b = m \cdot q_2 + r_2$, com $0 \leqslant r_2 < m$, as divisões euclidianas de a e b por m, respectivamente. Logo:

$$b - a = mq_2 + r_2 - (mq_1 + r_1)$$

$$b - a = mq_2 + r_2 - mq_1 - r_1$$

$$b - a = m(q_2 - q_1) + (r_2 - r_1)$$

Mas $a \equiv b \pmod{m}$ se os restos de suas divisões euclidianas são iguais, portanto $r_2 = r_1$ então $r_2 - r_1 = 0$, o que é equivalente dizer que $m \mid (b-a)$.

($\Leftarrow$): $m \mid (b-a) \rightarrow a \equiv b \pmod{m}$

$$a - b = mq_1 + r_1 - (mq_2 + r_2)$$

$$a - b = mq_1 + r_1 - mq_2 - r_2$$

$$a - b = m(q_1 - q_2) + (r_1 - r_2)$$

E sabemos que $a-b$ é divisível por m, por hipótese. Logo $m \mid (a-b)$ e $m \mid [m(q_1 - q_2)]$, então $m \mid (r_1 - r_2)$. Lembrando que $0 \leq r_1 < m$ e $0 \leq r_2 < m$, então:

$$-m < r_1 - r_2 < m$$

Mas o único número que pertence ao intervalo $-m < r_1 - r_2 < m$ que é divisível por m é o 0 (zero). Portanto só existe uma possibilidade para essa diferença:

$$r_1 - r_2 = 0$$

$$r_1 = r_2$$

Ou seja, se $a-b$ é divisível por m, então a nossa conclusão é que a e b deixam o mesmo resto na divisão por m. Logo $a \equiv b \pmod{m}$. Como queríamos demonstrar.

Proposição 3. Sejam a, b, c, d, $m \in \mathbb{Z}$, com $m > 1$.

(i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+c \equiv b+d \pmod{m}$;

(ii) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

Corolário 2. Para todos $n \in \mathbb{N}$, a, $b \in \mathbb{Z}$, se $a \equiv b \pmod{m}$, então tem-se que $a^n \equiv b^n \pmod{m}$.

E deixaremos essas demonstrações como uma sugestão de estudo e/ou pesquisa e sugerimos como referência (HEFEZ, 2014).

3.2 Pequeno Teorema de Fermat

"Fermat fez uma descoberta fundamental acerca de uma calculadora-relógio com número primo de horas, digamos p. Ele descobriu que se escolhermos um número natural nessa calculadora e o elevarmos à potência p, sempre obtém o número inicial. Esse é o chamado Pequeno Teorema de Fermat para distingui-lo do famoso Último Teorema de Fermat."(SAUTOY, 2013, p.225)

A tabela a seguir foi baseada em (SAUTOY, 2013, p.226) onde tomamos o 2 como o número escolhido da calculadora-relógio e determinamos todas as suas potências de 1 à 11. Nas linhas seguintes apresentamos os resultados obtidos correspondentes ao tipo de calculadora adotado, ou seja, na linha 2 os resultados são correspondentes a uma calculadora convencional, já na terceira linha os resultados são correspondentes a uma calculadora-relógio de 3 horas. Na quarta linha os resultados são correspondentes a uma calculadora-relógio de 4 horas e assim sucessivamente até a linha 11 onde os resultados são correpondentes a uma calculadora-relógio de 11 horas.

	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
Calc. convencional	2	4	8	16	32	64	128	256	512	1024	2048
Calc. relógio de 3 horas	2	1	2	1	2	1	2	1	2	1	2
Calc. relógio de 4 horas	2	0	0	0	0	0	0	0	0	0	0
Calc. relógio de 5 horas	2	4	3	1	2	4	3	1	2	4	3
Calc. relógio de 6 horas	2	4	2	4	2	4	2	4	2	4	2
Calc. relógio de 7 horas	2	4	1	2	4	1	2	4	1	2	4
Calc. relógio de 8 horas	2	4	0	0	0	0	0	0	0	0	0
Calc. relógio de 9 horas	2	4	8	7	5	1	2	4	8	7	5
Calc. relógio de 10 horas	2	4	8	6	2	4	8	6	2	4	8
Calc. relógio de 11 horas	2	4	8	5	10	9	7	3	6	1	2

Tabela 2 – Congruências e o Pequeno Teorema de Fermat

É interessante observar que para as calculadoras relógio com um número primo de horas, verificamos que após $p-1$ passos obtemos como resultado o 1, pois no *p-ésimo* passo retornamos ao ponto inicial. Já nas linhas que não apresentam um número primo de horas isso não ocorre.

Teorema 4. (Pequeno Teorema de Fermat) Seja p um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \pmod{p}$.

Prova:

(I): a é múltiplo de p;

$$a \equiv 0 \text{ (mod p)} \Rightarrow a^p \equiv 0^p \text{ (mod p)} \Rightarrow a^p \equiv 0 \text{ (mod p)}$$

(II): a não é múltiplo de p;

Tomemos $a \in \mathbb{Z}$ e p primo com $mdc(a,p) = 1$, ou seja, o máximo divisor comum entre a e p é igual a 1, logo a e p são primos entre si. Utilizaremos ainda uma propriedade das congruências que para a e p primos entre si, existe um a' tal que $a' \cdot a \equiv 1 \pmod{p}$. Esse elemento a' é chamado de *inverso multiplicativo módulo p*. [1]

Usando essas ideias temos que:

$$\begin{aligned} a^p &\equiv a \text{ (mod p)} \\ \Rightarrow a' \cdot a^p &\equiv a' \cdot a \text{ (mod p)} \\ \Rightarrow a' \cdot a \cdot a^{p-1} &\equiv a' \cdot a \text{ (mod p)} \\ \Rightarrow 1 \cdot a^{p-1} &\equiv 1 \text{ (mod p)} \\ \Rightarrow a^{p-1} &\equiv 1 \text{ (mod p)} \end{aligned}$$

[1] Para maiores detalhes sobre o inverso multiplicativo módulo p indicamos (HEFEZ, 2014) como uma referência.

Logo, provar que $a^p \equiv a \pmod{p}$ é equivalente a provar que $a^{p-1} \equiv 1 \pmod{p}$. De fato:

$$\begin{aligned} a^{p-1} &\equiv 1 \text{ (mod p)} \\ \Rightarrow a \cdot a^{p-1} &\equiv a \cdot 1 \text{ (mod p)} \\ \Rightarrow a^p &\equiv a \text{ (mod p)} \end{aligned}$$

Considere agora a sequência $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$. Essa é a sequência de $p-1$ múltiplos de a. O que precisamos a princípio é provar que nessa sequência nós não temos nenhum múltiplo de p.

Suponha, por absurdo, que exista algum $k \in \{1, 2, \ldots, p-1\}$ tal que $k \cdot a$ seja múltiplo de p, ou seja, $p \mid k \cdot a$. Mas p não divide k, pois $1 \leqslant k < p$, então $p \mid a$, mas isso não é possível, pois $mdc(a, p) = 1$. Portanto nessa nossa sequência $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$ não existe nenhum múltiplo de p.

Vamos mostrar ainda que nessa lista não existem dois elementos que sejam congruentes módulo p.

Tomemos para isso k_1 e $k_2 \in \{1, 2, \ldots, (p-1)\}$ com $k_1 \neq k_2$ de tal maneira que $k_1 \cdot a \equiv k_2 \cdot a \pmod{p}$.

$$\begin{aligned} a \cdot k_1 &\equiv a \cdot k_2 \text{ (mod p)} \\ a' \cdot a \cdot k_1 &\equiv a' \cdot a \cdot k_2 \text{ (mod p)} \\ 1 \cdot k_1 &\equiv 1 \cdot k_2 \text{ (mod p)} \\ k_1 &\equiv k_2 \text{ (mod p)} \end{aligned}$$

Como k_1 e k_2 são menores que p, pois $1 \leqslant k_1 < p-1$ e $1 \leqslant k_2 < p-1$, então para que k_1 seja congruente a k_2, só é possível quando $k_1 = k_2$. Mas isso contraria nossa hipótese inicial que diz que $k_1 \neq k_2$. Logo na nossa lista não existem dois números distintos que sejam congruentes módulo p.

Portanto cada um dos elementos da sequência $\{1, 2, \ldots, p-1\}$ está associado a um único elemento da sequência $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$, não necessariamente nessa ordem, então:

$$\begin{aligned} 1 \cdot a,\ 2 \cdot a,\ \ldots,\ (p-1) \cdot a &\equiv 1,\ 2,\ \ldots,\ p-1 \text{ (mod p)} \\ a^{p-1} \cdot (1 \cdot 2 \cdot \ldots (p-1)) &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \text{ (mod p)} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \text{ (mod p)} \end{aligned}$$

Mas como $mdc(p,(p-1)!)=1$, isso nos permite concluir que:

$$\begin{aligned} a^{p-1}\cdot\ (p-1)! &\equiv (p-1)!\ (\text{mod p}) \\ a^{p-1} &\equiv 1\ (\text{mod p}) \end{aligned}$$

Exatamente como queríamos demonstrar.■

Vamos verificar a utilização do Pequeno Teorema de Fermat para calcular o resto da divisão envolvendo potências "grandes". Calculemos por exemplo o resto da divisão 2^{257} por 7. Temos que encontrar N tal que $N \equiv 2^{257}\ (\text{mod } 7)$.

Lembrando que N é o resto da divisão de 2^{257} por 7. Como $257 = 6\cdot 42+5$, logo:

$$\begin{aligned} N &\equiv 2^{257}(mod 7) \\ N &\equiv 2^{6\cdot 42+5}(mod 7) \\ N &\equiv (2^6)^{42}\cdot 2^5(mod 7) \end{aligned}$$

Observe que fizemos a divisão de 257 por 6 justamente para podermos utilizar o Pequeno Teorema de Fermat(PTF), pois se $p=7$ então $p-1=6$ e acabamos de provar que $a^{p-1}\equiv 1\ (\text{mod } p)$. Então:

$$\begin{aligned} N &\equiv (2^6)^{42}\cdot 2^5\ (\text{mod } 7) \\ N &\equiv (1)^{42}\cdot 2^5\ (\text{mod } 7) \\ N &\equiv 1\cdot 2^5\ (\text{mod } 7) \\ N &\equiv 2^5\ (\text{mod } 7) \\ N &\equiv 32\ (\text{mod } 7) \\ N &\equiv 4\ (\text{mod } 7) \end{aligned}$$

Portanto 2^{257} dividido por 7 deixa resto 4.

Vejamos como calcular o resto da divisão de 3^{23456} por 13.

$$
\begin{aligned}
N &\equiv 3^{23\ 456} \pmod{13} \\
N &\equiv 3^{1\ 954\times 12+8} \pmod{13} \\
N &\equiv (3^{12})^{1\ 954}\cdot 3^{8} \pmod{13} \\
N &\equiv (1)^{1\ 954}\cdot 3^{8} \pmod{13} \\
N &\equiv 1\cdot 3^{3}\cdot 3^{3}\cdot 3^{2} \pmod{13} \\
N &\equiv 1\cdot 1\cdot 1\cdot 3^{2} \pmod{13} \\
N &\equiv 3^{2} \pmod{13} \\
N &\equiv 9 \pmod{13}
\end{aligned}
$$

Portanto $3^{23\ 456}$ dividido por 13 deixa resto 9.

Além de ser uma ferramenta poderosa de cálculo, como vimos nos exemplos anteriores, o Pequeno Teorema de Fermat também é utilizado na busca de novos números primos, pois determinar números primos "grandes"não é uma tarefa fácil, nem prática, através das divisões sucessivas já que conforme vamos andando no conjuntos dos números naturais, eles se tornam cada vez mais raros.Em 05 de janeiro de 2018 foi anunciada a descoberta do maior número primo conhecido até a data(ANSEDE, 2018). Tal feito foi atribuído ao engenheiro norte americano de 51 anos, Jonathan Pace. Esse número pertence a família dos números primos de Mersenne e é obtido através da expressão $2^{77\ 232\ 917}-1$ e apresenta 23 249 425 dígitos.(ANSEDE, 2018)

O estudo sobre números primos é muito amplo, curioso, brilhante e ao mesmo tempo enigmático. Deixaremos para os leitores, como uma mensagem de entusiasmo, que o estudo deste assunto é enriquecedor e agradável. Temos muito ainda a estudar e a descobrir sobre esses números.

CAPÍTULO

4

ATIVIDADES EM SALA DE AULA

Devido ao vasto domínio que envolve o estudo dos números primos, pela diversidade de suas propriedades, pelas suas características peculiares e enigmáticas e pela importância de suas aplicações, tal conteúdo constitui um rico campo a ser explorado.

Neste capítulo apresentaremos algumas atividades desenvolvidas com alunos do 9º Ano do Ensino Fundamental da EMEF – Prof. Paulo Freire em Ribeirão Preto/SP e que podem servir como sugestões de atividades para professores que se interessam em desenvolver aulas diferentes das tradicionais. Apresentaremos um conjunto de atividades desenvolvidas a partir das ideias apresentadas por Sautoy em (SAUTOY, 2007) que diz sobre os números primos "(...) esses números são os próprios átomos da aritmética(...)" e seguindo os princípios apresentados pela BNCC, que diz que:

> "Apesar de a Matemática ser, por excelência, uma ciência hipotético dedutiva, porque suas demonstrações se apoiam sobre um sistema de axiomas e postulados, é de fundamental importância também considerar o papel heurístico das experimentações na aprendizagem da Matemática."(BNCC, 2017)

Complementado por:

> "Os processos matemáticos de resolução de problemas, de investigação, de desenvolvimento de projetos e da modelagem podem ser citados como formas privilegiadas da atividade matemática, motivo pelo qual são, ao mesmo tempo, objeto e estratégia para aprendizagem ao longo de todo o Ensino Fundamental. Esses processos de aprendizagem são potencialmente ricos para o desenvolvimento de competências fundamentais para o letramento matemático (raciocínio, representação, comunicação e argumentação) e para o desenvolvimento do pensamento computacional."(BNCC, 2017)

4.1 Atividades e materiais propostos

As atividades e materiais que propusemos aqui têm como objetivo introduzir de maneira lúdica e pouco tradicional o conceito dos números primos, suas propriedades e aplicações na própria matemática, como é o caso da fatoração única de um número natural.

Usando a ideia já citada acima de que os números primos são os "átomos da aritmética", foram utilizados objetos, ou seja, esferas de isopor para representá-los. Com as esferas de isopor e palitos de madeira foram construídas estruturas similares às moléculas para representarem os números compostos. Para indicar os números primos distintos, as esferas foram pintadas por cores diferentes e os palitos de madeira (churrasco) foram utilizados para uní-las (essa união através dos palitos representa a operação de multiplicação, ou seja, quando unimos um átomo que representa o número primo 2 com um átomo que representa o número primo 3, estamos criando uma "molécula"que representa o número composto 6). Através da construção dessas estruturas "moleculares" representamos os números naturais que não são primos, ou seja, os números naturais compostos. Como exemplo apresentamos a seguir o número 815 788 304 100 que fatorado fica $2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 17^2 \cdot 23^2$ (um número que é quadrado perfeito), veja a Figura 1:

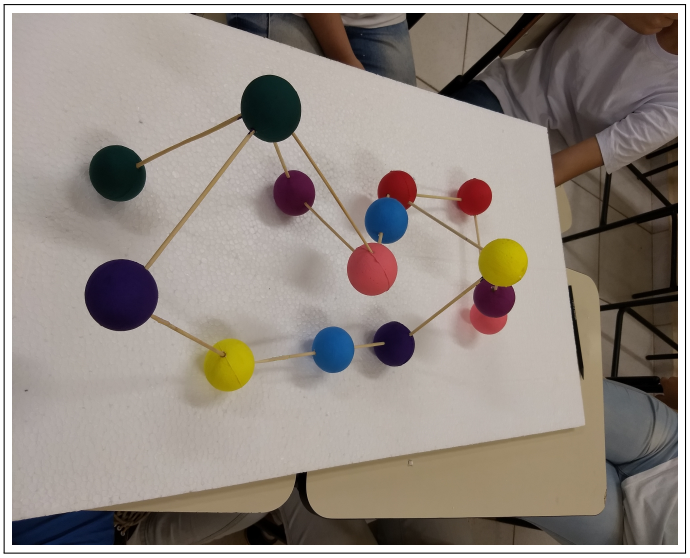


Figura 1 – Número através de sua representação "molecular"

4.2 Material utilizado

- Bolinhas de isopor 50 mm;
- Tinta artesanato PVA de cores diferentes(*);
- Palitos de madeira (churrasco);

- Papel sulfite;
- Envelopes grandes (*);
- Caixa de papelão para arquivo (*);
- Saquinhos pláticos;
- Lápis e /ou caneta;
- Lápis de cor;
- Calculadora.

Obs.: Os materiais (*) são opcionais, ou seja, a qualidade do trabalho não será comprometida pela falta deles.

4.3 Confecção do material

As esferas deverão ser pintadas em grupos de cores diferentes, pois cada cor representará um número primo. A quantidade de esferas e a quantidade de cores variam dependendo da quantidade de alunos e da quantidade de números primos com que o professor deseja trabalhar. O professor por praticidade e também por economia ao invés de pintar, poderá escrever os números primos nas esferas, porém o trabalho com cores fica mais atrativo. Essas esferas deverão ser agrupadas e armazenadas dentro dos saquinhos plástico para que fiquem organizadas.

Na Figura 2 a seguir apresentamos duas imagens para ilustrar o material e a legenda adotada:

Figura 2 – Legenda e Números Primos

Logo após o professor deverá selecionar algumas atividades a fim de serem trabalhadas com os alunos. Essas atividades deverão ser impressas, organizadas e separadas

dentro dos envelopes, pois posteriormente serão distribuídas gradativamente para os alunos. As atividades que foram utilizadas aqui nesse trabalho estão disponíveis no Apêndice A.

Todo esse material (esferas, envelope com as atividades e os palitos serão colocados dentro das caixas e cada uma dessas caixas será entregue para cada um dos grupos, ou seja, cada grupo terá seu kit (caixa) de material, como ilstrado pela Figura 3.

Figura 3 – Kit de material

4.4 Roteiro de aula

Nesta seção apresentaremos uma sequência para que o professor possa se orientar na realização das aulas práticas.

Inicialmente os alunos deverão ser divididos em grupos de quatro ou cinco integrantes e cada um desses grupos receberá um kit de material. A seguir apresentamos a sequência de atividades abordadas por esse trabalho.

4.4.1 Crivo de Eratóstenes

Como já comentamos no início deste trabalho, Eratóstenes de Cirene (cerca de 200 a.C.), foi um dos gregos que desenvolveu trabalhos com Números Primos e o primeiro a criar um algoritmo para determiná-los, conhecido como crivo de Eratóstenes. O procedimento é simples, a princípio criamos uma tabela de números até onde se pretende chegar. Para essa atividade, criamos uma tabela com os números de 1 à 120. Como o que nos interessa são números primos, ou seja, um número inteiro maior que 1, então excluímos o 1 desta lista. A partir daí passamos a eliminar todos os múltiplos de 2 com exceção dele

mesmo. O próximo número não eliminado é o 3, então passamos a eliminar (ou peneirar/crivar) seus múltiplos com exceção dele mesmo. O próximo número não eliminado da tabela é o 5, então passamos a crivar (peneirar/eliminar) seus múltiplos com exceção dele mesmo. Continuamos assim sucessivamente, e em ordem, até o momento em que tomemos um número que não tenha sido eliminado, e ao crivar seus múltiplos diferentes dele mesmo, não encontremos nenhum. Quando isso ocorrer significa que o trabalho terminou e os elementos que sobraram, são todos os números primos de sua tabela, que no caso aqui, são todos os números primos menores que 120, como ilustrado pela Figura 4. Essa atividade será importante para que possamos realizar algumas atividades a seguir como: a fatoração e o teste de primalidade.

- Enunciado: Determine todos os números primos menores que 120.
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: identificar números primos.
- Material: lápis e/ou caneta e uma tabela de números naturais impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: múltiplos de um número natural e números primos.

4.4.2 Representação dos números na forma retangular

Nesta atividade os alunos deverão representar alguns números de todas as maneiras possíveis como uma disposição retangular, ou seja, construir todos os retângulos possível que apresentam o número citado como o valor de sua área, por exemplo: com o número 5 podemos construir apenas um único retângulo 1×5, já o número 6, pode ser representado por 1×6 ou 2×3, considerando que $a \times b$ e $b \times a$, têm a mesma representação. Através dessas representações os alunos devem classificar os números em primos ou compostos. Logo, pelo exemplo anterior, temos que 5 é primo e o 6 é um número composto. Atividades representadas pelas Figuras 5, 6, 7, 8.

- Enunciado: Determine todas as maneiras de representar cada um dos números a seguir numa disposição retangular. Em seguida, determine se o número é primo ou composto.
- Números: 11, 12, 13, 14, 15, 16, 17, e 18.
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: identificar que cada número primo (p) só pode ser representado através do produto de 1 por ele mesmo ($1 \times p$).

- Material: lápis de cor e atividade impressa contendo alguns números naturais e malhas quadriculadas, material fornecido pelo professor.
- Temáticas a serem abordadas: divisores de um número natural, conceito de área e números primos.

4.4.3 Fatoração

Nesta atividade os alunos têm que fatorar cada um dos números apresentados. A partir da fatoração eles precisam determinar o número de divisores e classificá-los em quadrados perfeitos ou não. Essa análise foi previamente trabalhada com a turma, ou seja, foi mostrado para os alunos que para um número ser um quadrado perfeito, os expoentes dos números primos, na forma fatorada, são todos pares e se isso não ocorrer é porque o número não é um quadrado perfeito. Outro ponto que foi ressaltado é que se um número for um quadrado perfeito, ela apresentará uma quantidade ímpar de divisores, caso contrário, não é um quadrado perfeito. Para essa atividade utilizaremos os números primos encontrados no Crivo de Eratóstenes. Nessa atividade também será explorado como determinar a quantidade de divisores[1] naturais de um número, e verificar se o número é um quadrado perfeito[2] ou não. Essa atividade está ilustrada pelas Figuras 9, 10 e 13.

- Enunciado: Escreva cada um dos números abaixo como um produto de números primos, ou seja, decomponha (fatore) cada um desses números. Determine ainda a quantidade de divisores naturais de cada um deles, e classifique-os em quadrados perfeitos ou não.
- Números: 900, 2 431, 3 150, 20 449, 44 100, 5 112 121.
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: representar números naturais compostos como um produto de números primos.
- Material: lápis e/ou caneta e atividade impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: critérios de divisibiliade, divisão envolvendo números naturais, quantidade de divisores de um número natural e a identificação dos quadrados perfeitos.

[1] Se $N = p_1^a \cdot p_2^b \cdot \ldots \cdot p_r^k$ é um número natural na sua forma fatorada, temos que o número de divisores naturais de N é dado por $(a+1)\cdot(b+1)\cdot\ldots\cdot(k+1)$

[2] Uma das maneiras que temos para verificarmos se um natural é um quadrado perfeito ou não é verificar na sua forma fatorada se todos os expoentes dos números primos são pares ou não. Se todos os expoentes forem pares trata-se de um quadrado perfeito, no entanto, se pelo menos um dos expoentes não for par o número não é um quadrado perfeito.

4.4.4 Teste de Primalidade

Nesta atividade os alunos precisam verificar se um número é primo ou não. O teste de primalidade utilizado aqui foi o das divisões sucessivas. Iniciamos essa etapa do trabalho comentando com os alunos que para sabermos se um número inteiro n é primo, não há necessidade de testarmos todos os números primos menores que n, mas sim precisamos testar todos os números primos p, tal que $p \leq \sqrt{n}$[3]. Para essa atividade foi colocado à disposição dos grupos uma calculadora e novamente foram utilizados os números primos encontrados no Crivo de Eratóstenes. Figuras 11 e 12.

Destacamos aqui o quanto é difícil determinar se um número é primo, pois conforme os números aumentam, fica extremamente difícil fatorá-los. Daí a importância desses números para a utilização na criptografia.

- Enunciado: Verifique se os números abaixo são primos ou compostos.
- Números: 659, 977, 1 453, 3 337, 8 633, 9 631.
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: descobrir números primos.
- Material: lápis e/ou caneta, calculadora, crivo de Eratóstenes e/ou uma lista de números primos e atividade impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: divisibilidade, o uso de calculadora em sala de aula e números primos.

Em todas as atividades o material concreto foi objeto de acompanhamento, mas nas atividades posteriores a manipulação deste material foi muito útil, pois a partir dele, os alunos puderam visualizar a resolução de uma maneira mais clara. Inclusive a resolução de uma das atividades foi feita apenas com o material concreto, dispensando cálculos durante a resolução da atividade, ficando, o cálculo, reservado apenas para concluí-la.

4.4.5 Transformando em quadrados perfeitos

Nesta atividade os alunos deverão transformar os números em quadrados perfeitos, ou seja, os alunos precisam fatorar cada uma dos números e verificar quais são os números primos que não estão em uma quantidade par. Para isso o material concreto foi muito útil. Atividade ilustrada pelas Figuras 14, 15, 16, 17 e 18.

- Enunciado: Qual é o menor inteiro positivo que devemos multiplicar por 300 para obter um inteiro positivo que seja quadrado perfeito? (Justifique sua resposta)

[3] Para maiores esclarecimentos sugerimos (DUDLEY, 1969)

- Enunciado: Qual é o menor inteiro positivo pelo qual devemos multiplicar 2 016 para obter um inteiro quadrado perfeito? (Justifique sua resposta)
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: identificar números quadrados perfeitos e determinar sua raiz quadrada.
- Material: esferas, palitos, lápis e/ou caneta e atividade impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: fatoração, números quadrados perfeitos e sua raiz quadrada.

4.4.6 Será que dá para dividir?

Nesta atividade os alunos puderam verificar através da fatoração se um número é par ou ímpar. E em outra atividade associada, e com a utilização do material concreto, puderam verificar se um número é divisível por outro, e o mais importante, o porquê. Para isso, a utilização do material concreto fez toda a diferança, pois os alunos puderam reparar que para um número ser par é necessário que na sua fatoração aparece pelo menos um número primo 2, e no caso da divisibilidade verificaram que quando um número é divísivel por outro é porque um deles é múltiplo do outro, ou seja, nas suas composições de primos o divisor aparece na fatoração do dividendo, por exemplo, $36/12 = (2\cdot 2\cdot 3\cdot 3)/2\cdot 2\cdot 3$. Note que no numerador da fração temos a fatoração do número 12, logo 36 é um múltiplo de 12, e ao fazermos as simplificações ficamos apenas com o número três do numerador, logo $36/12 = 3$. Se por acaso o dividendo não apresentar números primos suficientes para serem simplificados pelo divisor, o dividendo não é divisível pelo divisor. Figuras 19, 20 e 21.

- Enunciado: Considere os números cujas decomposições em fatores primos são $M = 2^8\cdot 3^7\cdot 5^9$ e $N = 3^2\cdot 5^4\cdot 7^5$, responda: a) O número N é ímpar? b) M/N é um número inteiro?
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: verificar se um número natural é divisível por outro.
- Material: esferas, palitos, lápis e/ou caneta e atividade impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: números pares e números ímpares, divisibilidade e fatoração.

4.4.7 Que número é esse?

Nesta atividade o aluno deverá verificar qual é o menor número inteiro que é divisível por outros números simultaneamente, ou seja, os alunos devem verificar qual é o menor número que apresenta números primos suficientes para serem simplificados por vários números primos simultaneamente. Esta atividade foi resolvida apenas utilizando o material concreto. Os cálculos foram utilizados somente para concluí-la. Figuras 22, 23 e 24.

- Enunciado: Qual é o menor inteiro positivo n tal que $n/3$, $n/4$, $n/5$, $n/6$ e $n/7$ são números inteiros?
- Tempo de aula: aproximadamente 50 minutos.
- Objetivos: determinar o menor múltiplo comum de um número natural de uma maneira não convencional (mmc).
- Material: esferas, palitos, lápis e/ou caneta e atividade impressa, material fornecido pelo professor.
- Temáticas a serem abordadas: múltiplos de um número natural, fatoração e mínimo múltiplo comum.

A aula teve início com uma breve explicação conceitual (momento teórico expositivo) seguida da realização das atividades. As avaliações foram feitas a partir da participação em aula, presença, desenvolvimento da atividade em grupo bem como o avanço das ideias pertinentes à temática e a realização dos exercícios propostos.

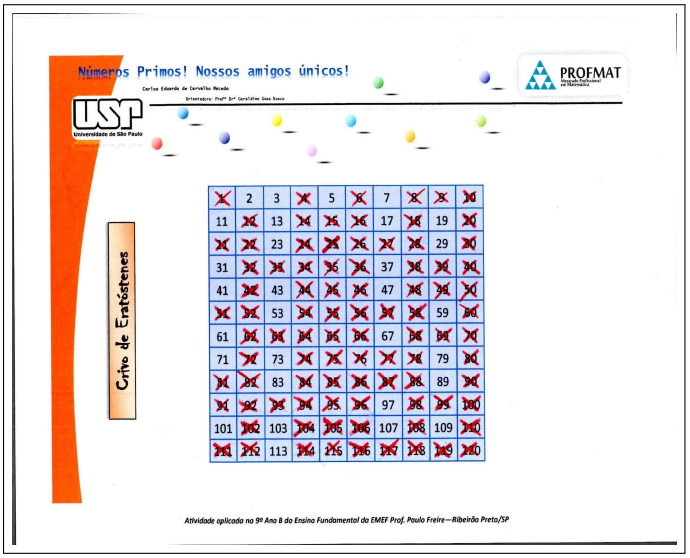


Figura 4 – Crivo de Eratóstenes

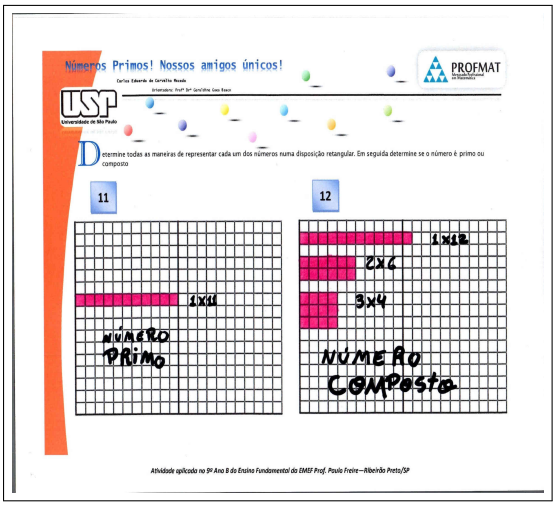


Figura 5 – Números: 11 (primo) e 12 (composto)

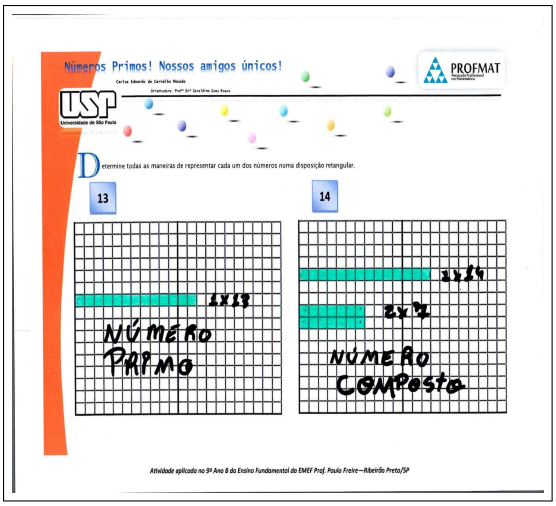


Figura 6 – Números: 13 (primo) e 14 (composto)

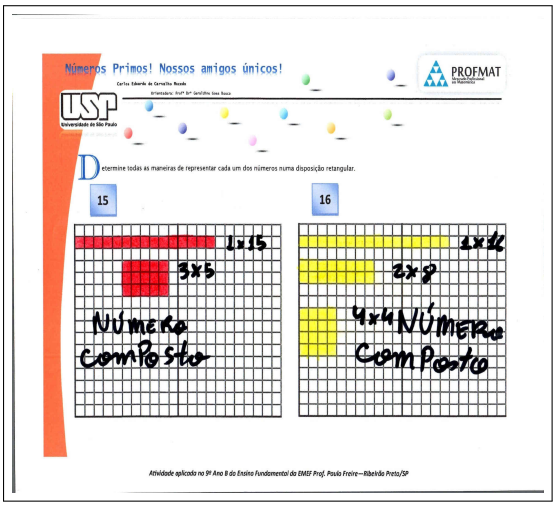


Figura 7 – Números: 15 (composto) e 16 (composto)

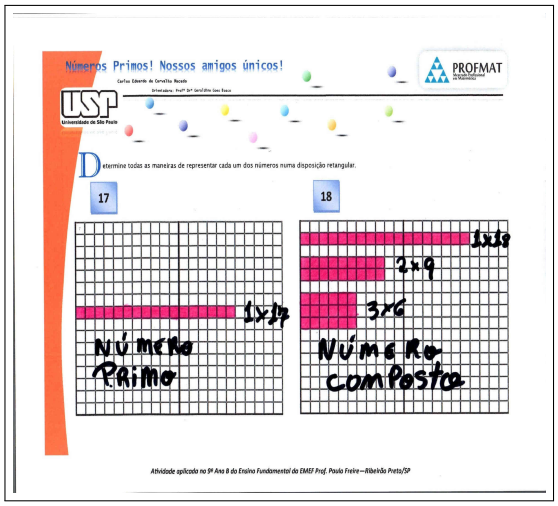


Figura 8 – Números: 17 (primo) e 18 (composto)

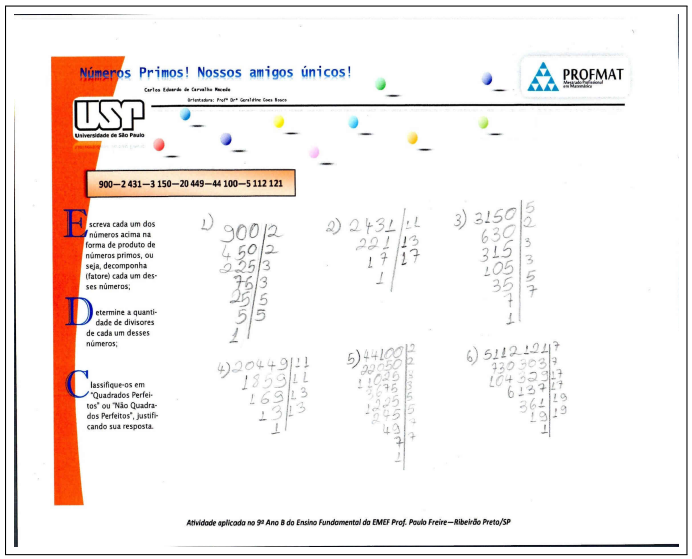


Figura 9 – Fatoração

4.5 Observações interessantes

O tempo de realização de cada atividade poderá variar dependendo das características das turmas e do grau de dificuldade das atividades propostas pelo professor. Sugerimos que a princípio as atividades sejam de nível mais fácil para que os alunos sintam interesse e aprendam a manusear o material, e em outro momento o professor repita algumas das atividades com um grau maior de dificuldade para que os alunos se sintam desafiados.

A realização das atividades através do material aqui proposto tornou a aula mais interessante e envolvente. A busca da solução através da modelagem gerou um grande interesse na turma, possibilitando o desenvolvimento de diversas estratégias e a troca de ideias entre os integrantes do grupo tornando a aula dinâmica e envolvente.

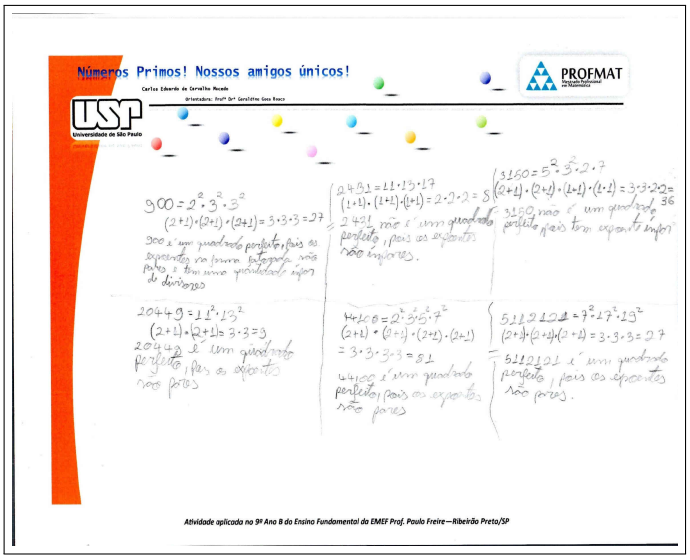


Figura 10 – Quantidade de divisores e classificação em quadrados perfeitos ou não quadrados perfeitos

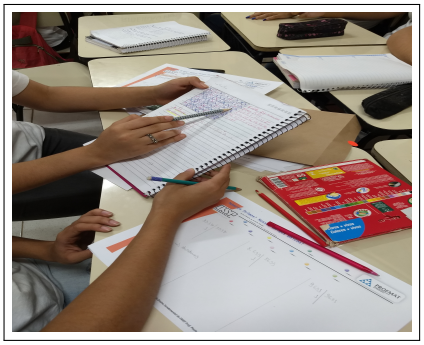


Figura 11 – Teste de primalidade - Selecionando os primos

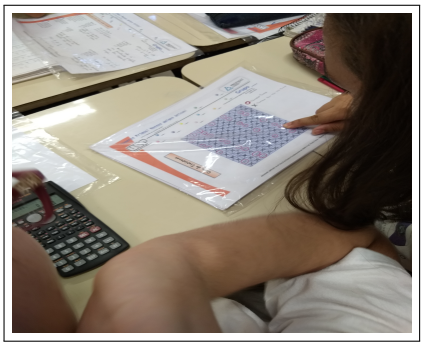


Figura 12 – Teste de primalidade - Auxílio da calculadora

Deixamos aqui também a sugestão para professores que atuam com alunos que apresentam algum tipo de deficiência: essas bolinhas podem ser diferenciadas pelo diâmetro, ou por algum tipo de material de textura, para a utilização por exemplo, com alunos que apresentam deficiência visual, garantindo o trabalho coletivo e permitindo a inclusão dos mesmos.

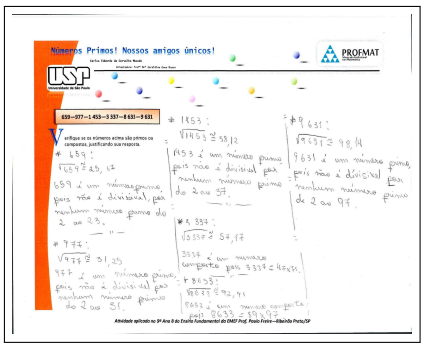


Figura 13 – Teste de primalidade

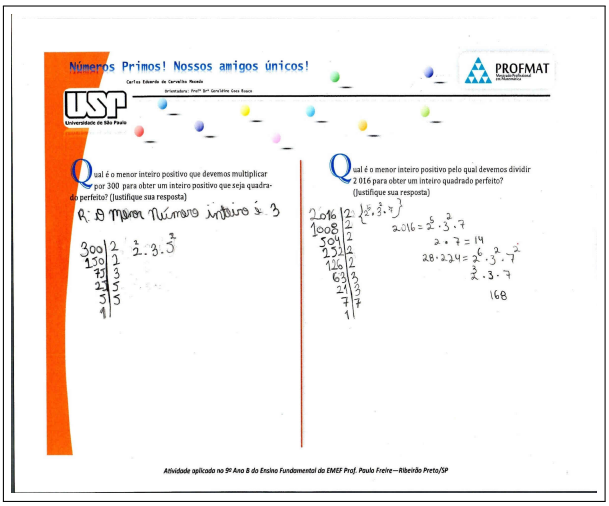


Figura 14 – Transformando em quadrados perfeitos

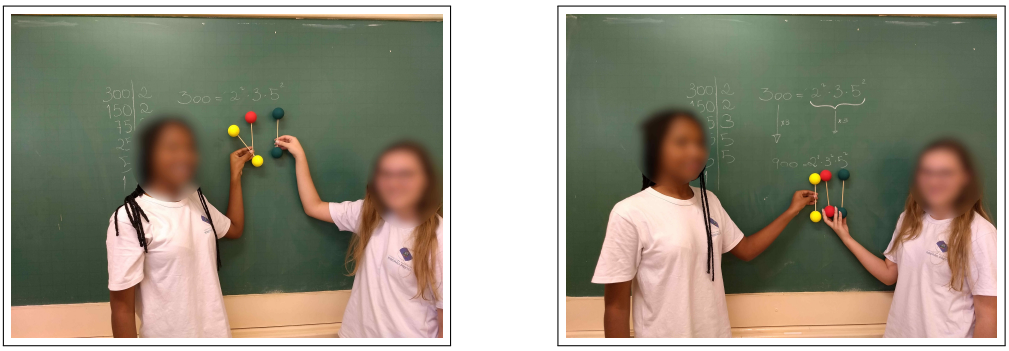


Figura 15 – A esquerda o número 300 e a direita o 900

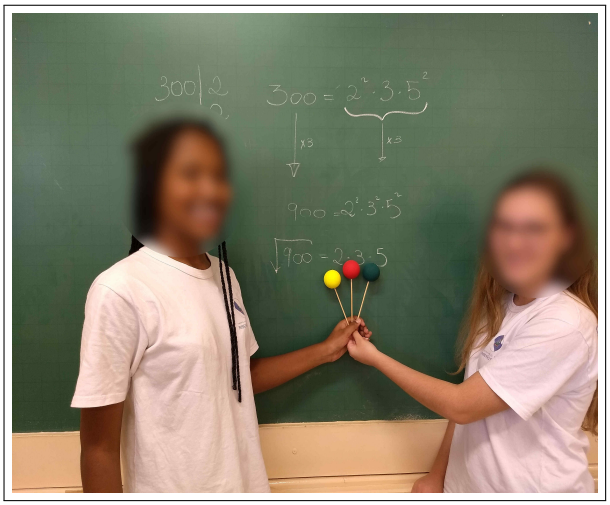


Figura 16 – $\sqrt{900} = 2 \cdot 3 \cdot 5 = 30$

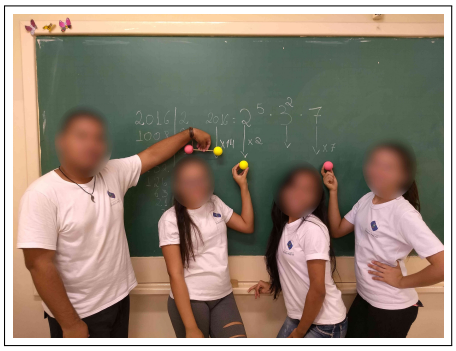


Figura 17 – A esquerda o número 2 016 e a direita o $2\ 016 \cdot 14 = 28\ 224$

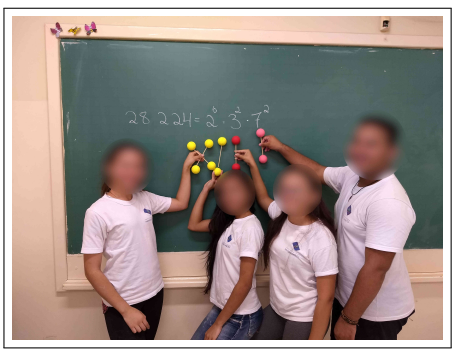


Figura 18 – A esquerda o número 28 224 e a direita o $\sqrt{28\ 224} = 2^3 \cdot 3 \cdot 7 = 168$

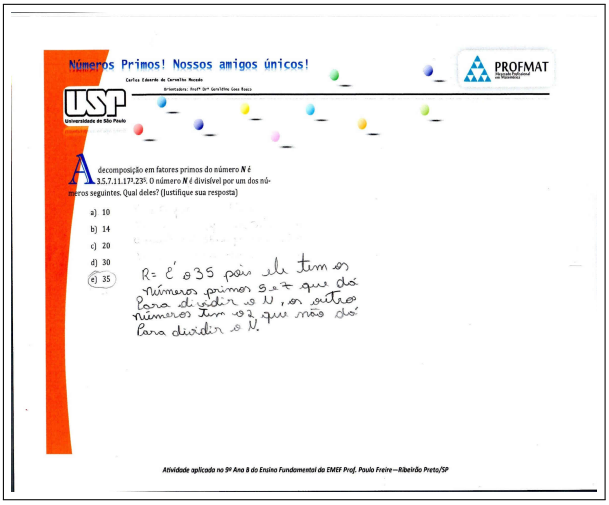


Figura 19 – Por qual dos números N é divisível

Figura 20 – N e os números das alternativas, todos na forma fatorada

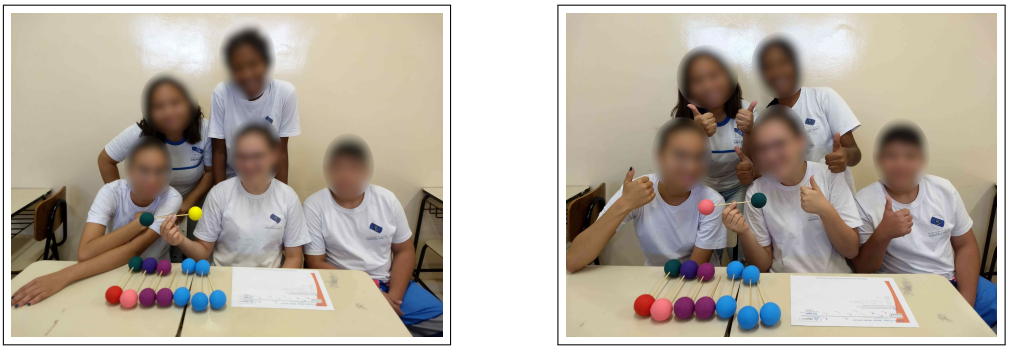


Figura 21 – A esquerda não é divisível e a direita é divisível


Figura 22 – A esquerda divisível por 3 e a direita divisível por 3 e 4


Figura 23 – A esquerda divisível por 3, 4 e 5 e a direita divisível por 3, 4, 5 e 6

Figura 24 – Pronto - n é divisível por 3, 4, 5, 6 e 7

CAPÍTULO

5

CONSIDERAÇÕES FINAIS

Neste trabalho apresentamos um pouco da história dos números primos destacando o nome de alguns dos grandes matemáticos que dedicaram parte de suas vidas para desvendarem o mistério desse grande enigma. Apresentamos um breve panorama do processo de ensino-aprendizagem e as novas diretrizes estipuladas pela BNCC, em especial ao que se refere aos números primos.

Elaboramos dois capítulos teóricos para serem a base dos conceitos e resultados sobre os números primos, os protagonistas desde trabalho. Estudamos vários conceitos e resultados que nos levaram à prova do Teorema Fundamental da Aritmética que diz que todo número inteiro pode ser decomposto em fatores primos e de maneira única. Apresentamos também o conceito de Congruências (ou Aritmética dos Restos) e o Pequeno Teorema de Fermat.

Ao longo do estudo para o desenvolvimento desse trabalho muitos conceitos tornaram-se mais claros e a aritmética começou a adquirir um outro sentido, o interesse pelo novo e a ampliação de novos horizontes tornaram possíveis o desenvolvimento de uma proposta didática e um material diferenciado para ser utilizado em sala de aula na educação básica. Esse material surpreendeu pelo resultado apresentado, pois despertou um grande interesse e participação na turma em que foi trabalhado. Devido a esse resultado positivo apresentamos aqui de maneira detalhada esse material, tal como a confecção do mesmo, um roteiro de aulas práticas e alguns exemplos das atividades desenvolvidas.

Enfim, esperamos que esse trabalho entusiasme mentes curiosas a sempre estarem dispostas à procura do novo, de algo a mais, e que sirva de apoio para os professores que se interessam em desenvolver aulas diferentes das tradicionais, apresentando novas aplicações em sala de aula.

REFERÊNCIAS

ANSEDE, M. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/01/05/ciencia/1515173661_363350.html>. Acesso em: 17/12/2018. Citado na página 56.

BOYER, C. B. **História da Matemática**. [S.l.]: Edgard Blücher, 2003. Citado nas páginas 23 e 24.

COUTINHO, S. C. **Criptografia**. [S.l.]: SBM, 2015. Citado na página 48.

DUDLEY, U. **Elementary Number Theory**. [S.l.]: W.H. Freeman and Company, 1969. Citado nas páginas 17, 21, 31, 32, 38, 40, 42, 43 e 63.

GARBI, G. G. **A Rainha das Ciências - Um grande passeio pelo maravilhoso mundo da Matemática**. [S.l.]: Livraria da Física, 2008. Citado nas páginas 23, 24, 25 e 42.

HEFEZ, A. **Aritmética**. [S.l.]: SBM, 2014. Citado nas páginas 47, 50, 51, 52 e 53.

_____. **Iniciação à Aritmética**. [S.l.]: SBM, 2015. Citado na página 32.

IFRAH, G. **Os Números: a história de uma grande invenção**. [S.l.]: Globo, 2009. Citado nas páginas 22 e 23.

MINISTÉRIO DA EDUCAÇÃO. **Direttrizes Curriculares para Educação Básica**: Diretrizes curriculares. Brasília, 2013. 542 p. Citado na página 26.

MINISTÉRIO DA EDUCAÇÃO E CULTURA. **Base Nacional Comum Curricular**: Bncc. Brasília, 2017. 472 p. Citado nas páginas 26, 27 e 57.

RIBENBOIM, P. **Números Primos, amigos que causam problemas**. [S.l.]: SBM, 2015. Citado na página 24.

RIPOLL, C.; RANGEL, L.; GIRALDO, V. **Números Inteiros**. Rio de Janeiro: SBM, 2016. Citado na página 31.

SAUTOY, M. du. **A Música dos Números Primos - A história de um problema não resolvido na Matemática**. [S.l.]: Jorge Zahar, 2007. Citado nas páginas 21, 24, 25, 39 e 57.

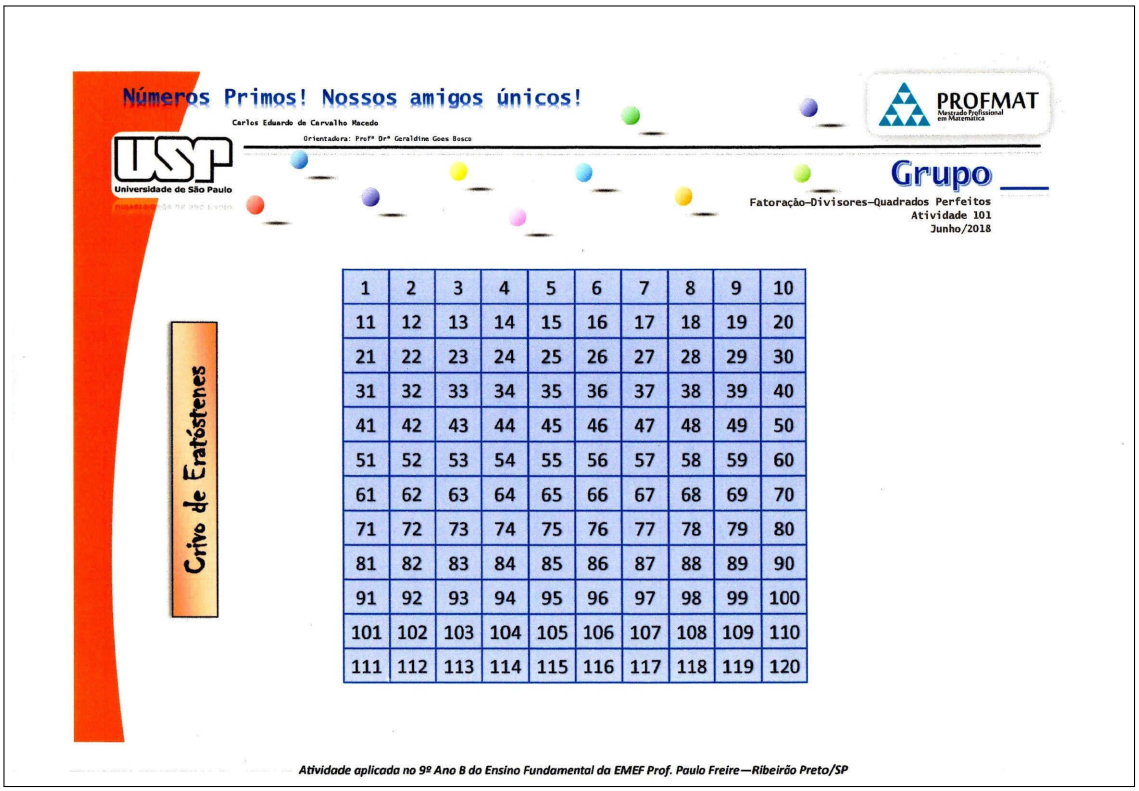
_____. **Os Mistérios dos Números - Uma viagem pelos grandes enigmas da Matemática**. [S.l.]: Jorge Zahar, 2013. Citado nas páginas 49 e 52.

SECRETARIA DE DIREITOS HUMANOS DA PRESIDÊNCIA DA REPLÚBLICA. **Caderno de Eduacação em Direitos Humanos**: Educação em direitos humanos. Brasília, 2013. 73 p. Citado na página 26.

APÊNDICE

A

SUGESTÕES DE ATIVIDADES



Números Primos! Nossos amigos únicos!

Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco

USP Universidade de São Paulo

PROFMAT Mestrado Profissional em Matemática

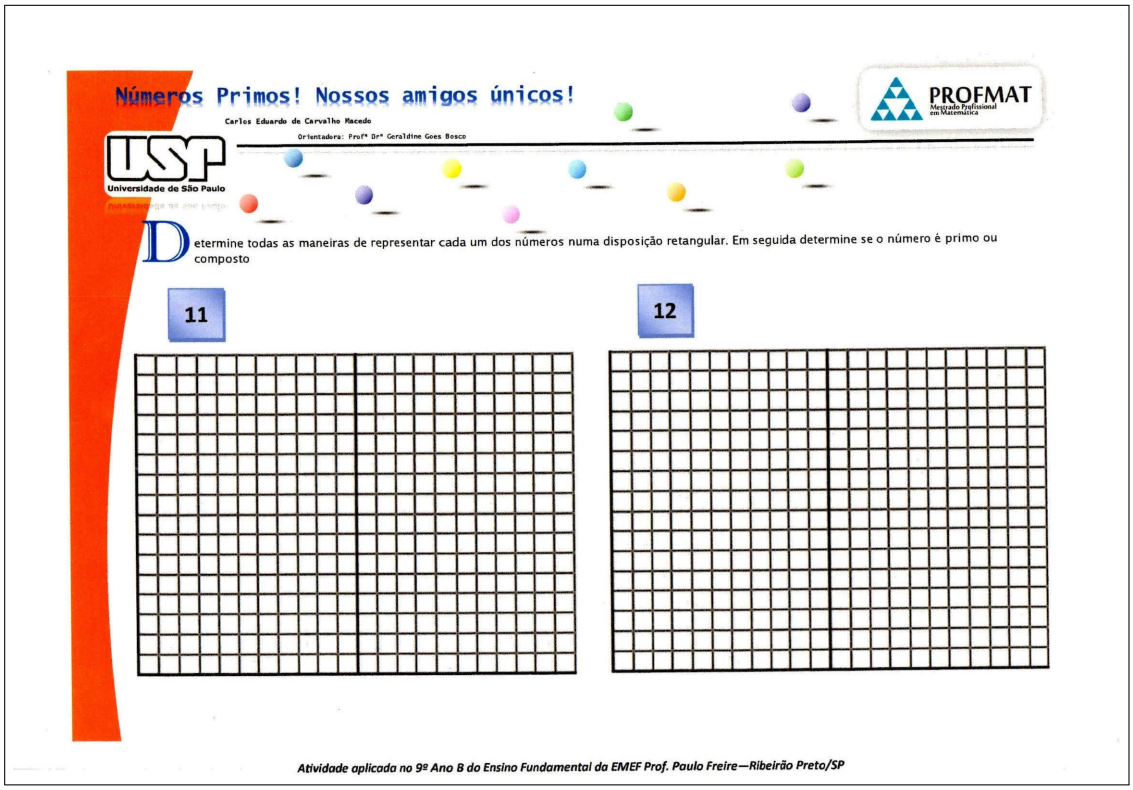
Grupo ___

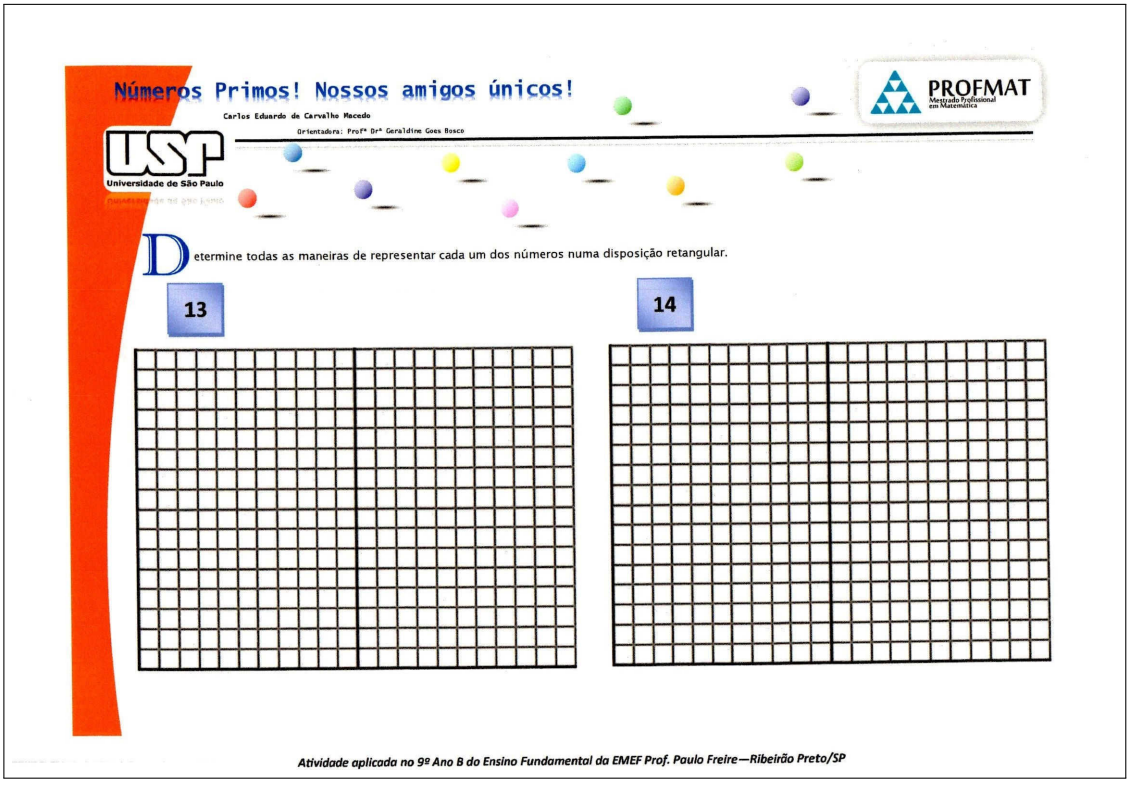
Fatoração-Divisores-Quadrados Perfeitos
Atividade 101
Junho/2018

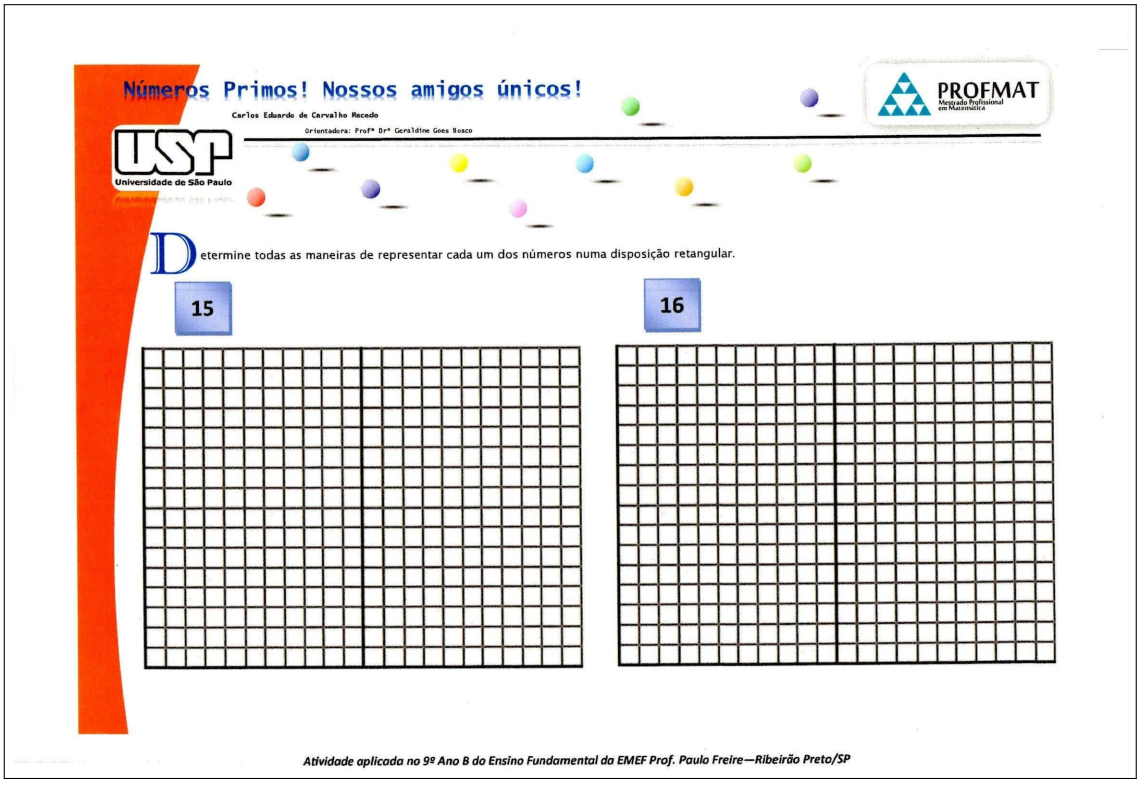
Crivo de Eratóstenes

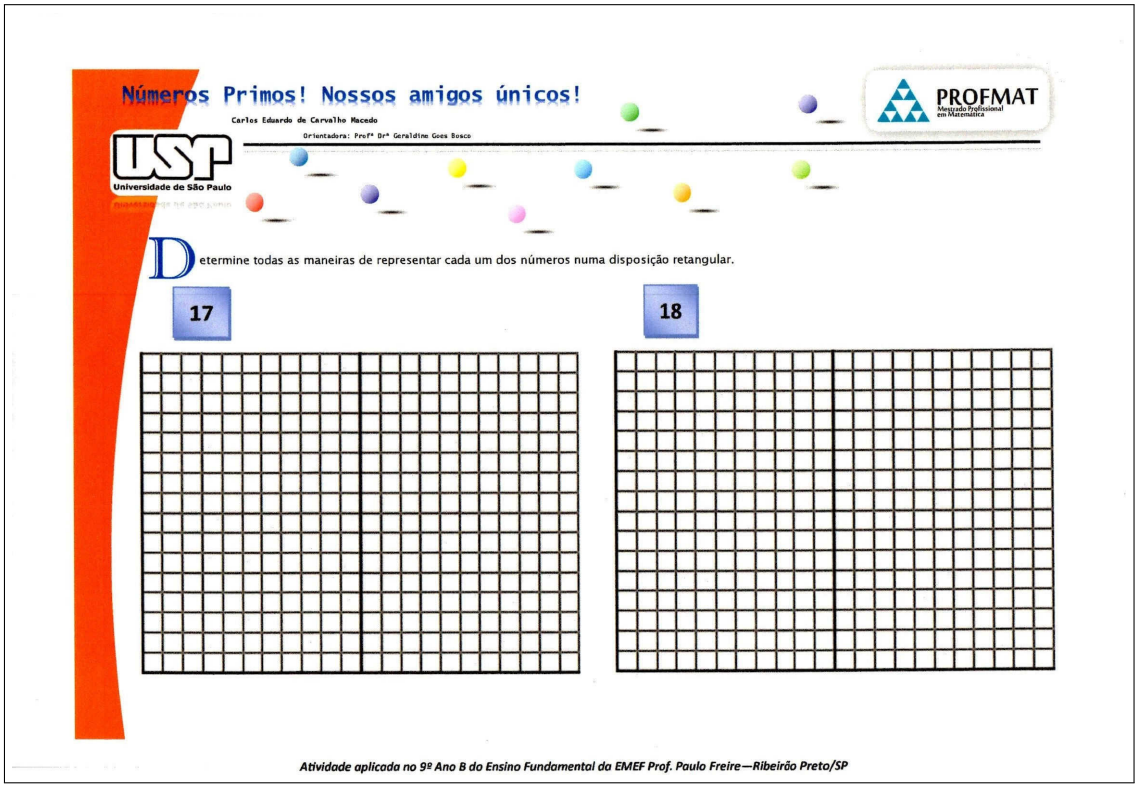
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

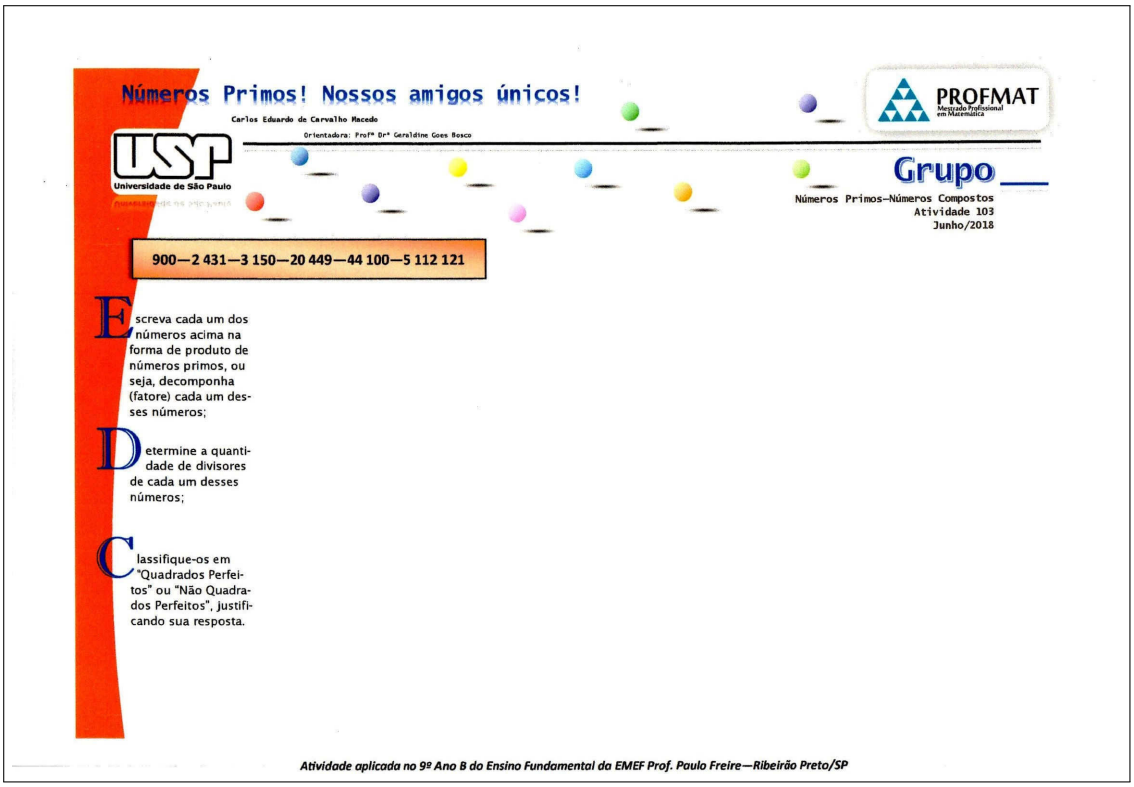
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP

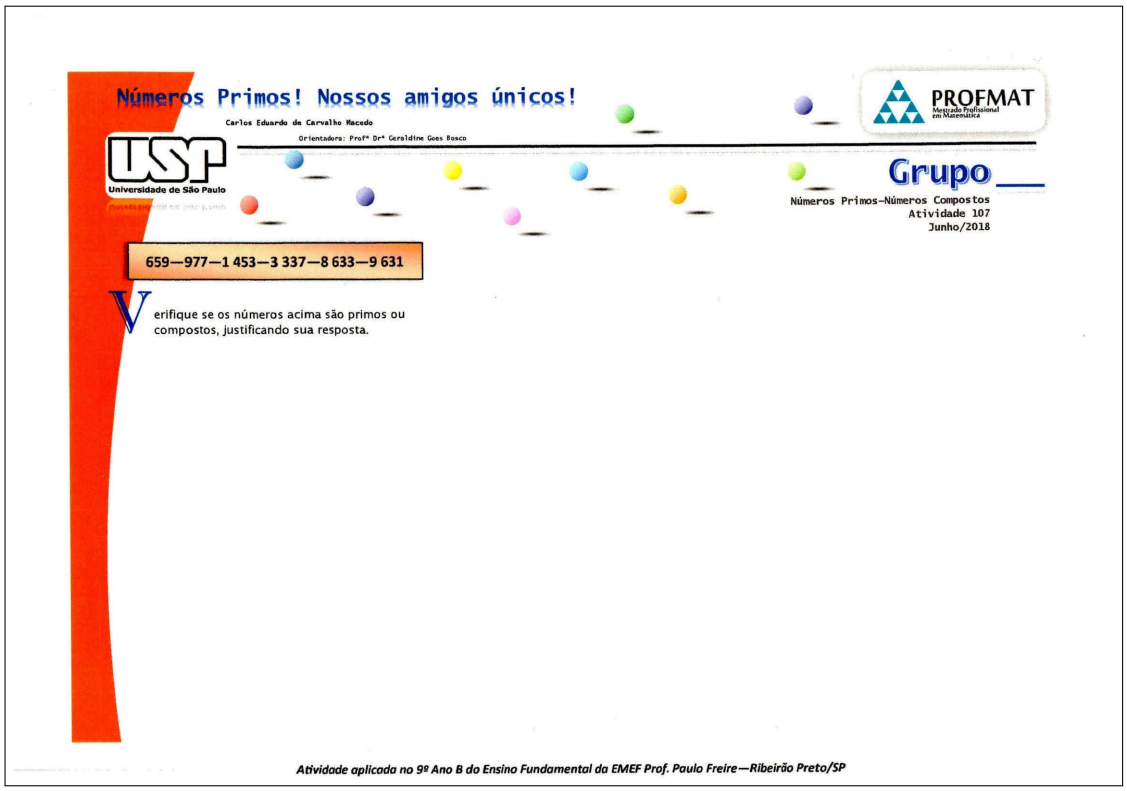

Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Determine todas as maneiras de representar cada um dos números numa disposição retangular. Em seguida determine se o número é primo ou composto
11
12
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP

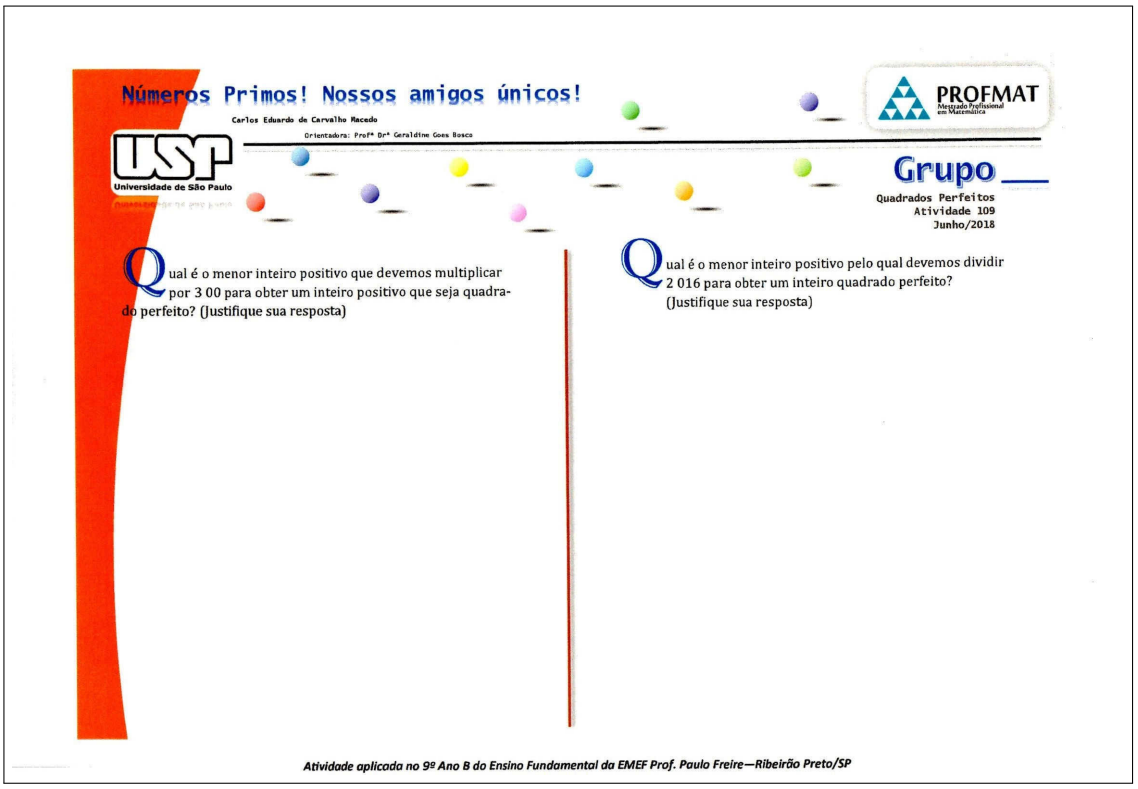

Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Determine todas as maneiras de representar cada um dos números numa disposição retangular.
13
14
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP


Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Determine todas as maneiras de representar cada um dos números numa disposição retangular.
15
16
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP


Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Determine todas as maneiras de representar cada um dos números numa disposição retangular.
17
18
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP


Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Grupo ___
Números Primos-Números Compostos
Atividade 103
Junho/2018
900—2 431—3 150—20 449—44 100—5 112 121
Escreva cada um dos números acima na forma de produto de números primos, ou seja, decomponha (fatore) cada um desses números;
Determine a quantidade de divisores de cada um desses números;
Classifique-os em "Quadrados Perfeitos" ou "Não Quadrados Perfeitos", justificando sua resposta.
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP


Números Primos! Nossos amigos únicos!
Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco
Universidade de São Paulo
PROFMAT
Mestrado Profissional em Matemática
Grupo ___
Números Primos-Números Compostos
Atividade 107
Junho/2018
659—977—1 453—3 337—8 633—9 631
Verifique se os números acima são primos ou compostos, justificando sua resposta.
Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP



Números Primos! Nossos amigos únicos!

Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco

Universidade de São Paulo

PROFMAT Mestrado Profissional em Matemática

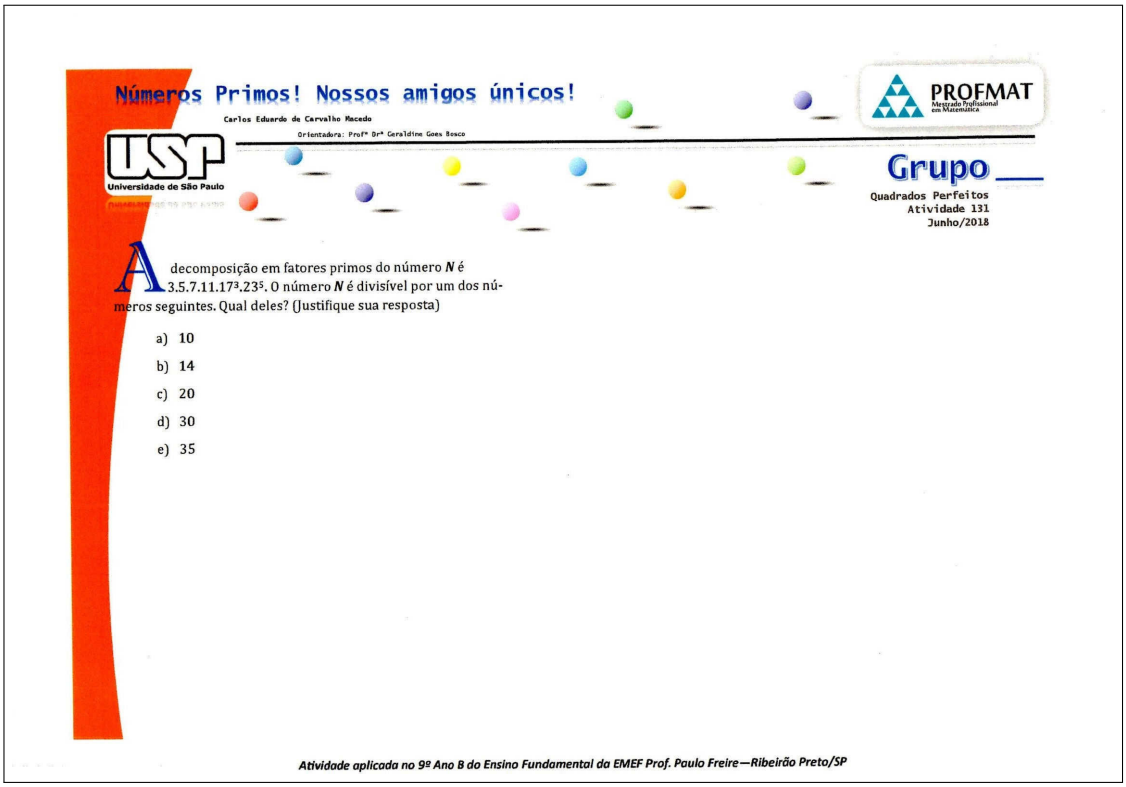
Grupo ___

Quadrados Perfeitos
Atividade 109
Junho/2018

Qual é o menor inteiro positivo que devemos multiplicar por 3 00 para obter um inteiro positivo que seja quadrado perfeito? (Justifique sua resposta)

Qual é o menor inteiro positivo pelo qual devemos dividir 2 016 para obter um inteiro quadrado perfeito? (Justifique sua resposta)

Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP



Números Primos! Nossos amigos únicos!

Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco

Universidade de São Paulo

PROFMAT Mestrado Profissional em Matemática

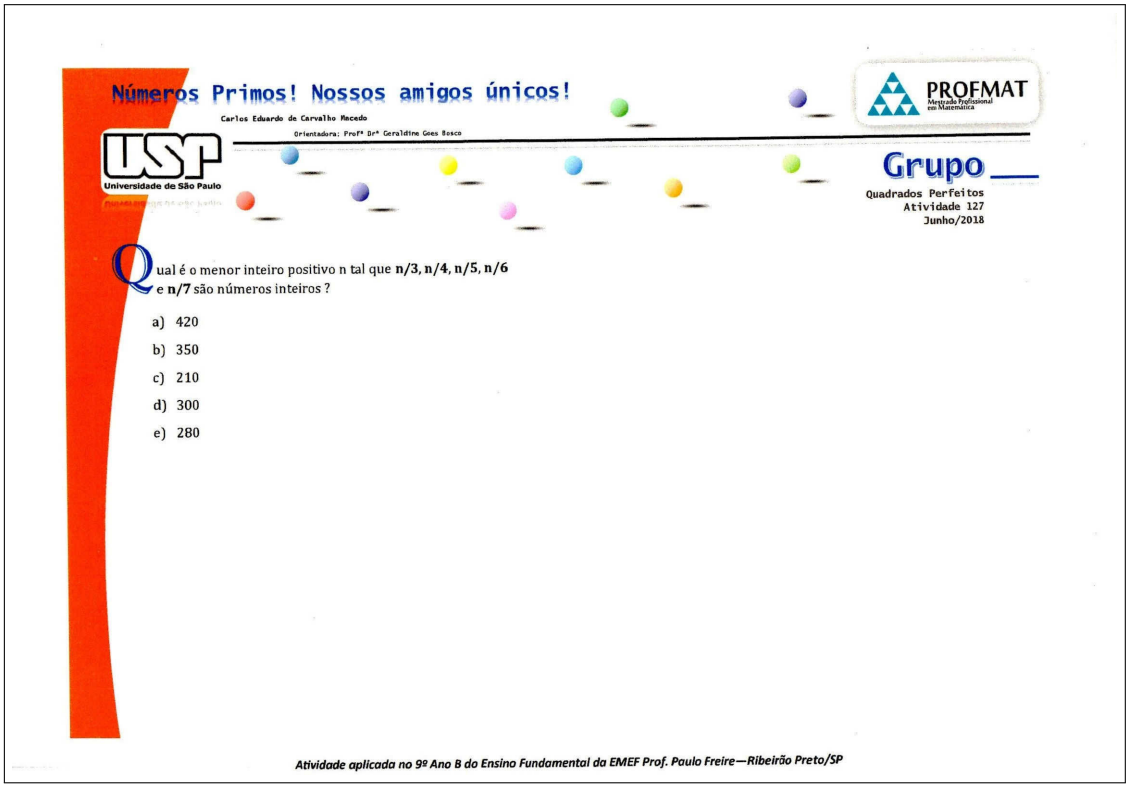
Grupo ___

Quadrados Perfeitos
Atividade 131
Junho/2018

A decomposição em fatores primos do número N é $3.5.7.11.17^3.23^5$. O número N é divisível por um dos números seguintes. Qual deles? (Justifique sua resposta)

a) 10
b) 14
c) 20
d) 30
e) 35

Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP



Números Primos! Nossos amigos únicos!

Carlos Eduardo de Carvalho Macedo
Orientadora: Profª Drª Geraldine Goes Bosco

USP Universidade de São Paulo

PROFMAT Mestrado Profissional em Matemática

Grupo ___

Quadrados Perfeitos
Atividade 127
Junho/2018

Qual é o menor inteiro positivo n tal que **n/3, n/4, n/5, n/6** e **n/7** são números inteiros ?

a) 420
b) 350
c) 210
d) 300
e) 280

Atividade aplicada no 9º Ano B do Ensino Fundamental da EMEF Prof. Paulo Freire—Ribeirão Preto/SP


ICMC
USP
SÃO CARLOS