UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
MESTRADO EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

O problema da primalidade: alguns testes e uma proposta de situação de aprendizagem

Nickson Queiroz

São Carlos – SP
Fevereiro de 2021

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
MESTRADO EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

O problema da primalidade: alguns testes e uma proposta de situação de aprendizagem

Nickson Queiroz

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional, da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do Título de Mestre.

Orientador: Prof. Dr. João Carlos Vieira Sampaio.

São Carlos – SP
Fevereiro de 2021

Queiroz, Nickson

O problema da primalidade: alguns testes e uma proposta de situação de aprendizagem. / Nickson Queiroz -- 2021.
112f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): João Carlos Vieira Sampaio
Banca Examinadora: João Carlos Vieira Sampaio, Eliris Cristina Rizziolli, Paulo Antonio Silvani Caetano
Bibliografia

1. Ensino de matemática. 2. Proposta pedagógica. 3. Números primos. I. Queiroz, Nickson. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Mestrado Profissional em Matemática em Rede Nacional

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Nickson Queiroz, realizada em 09/02/2021.

Comissão Julgadora:

Prof. Dr. João Carlos Vieira Sampaio (UFSCar)

Profa. Dra. Eliris Cristina Rizziolli (UNESP)

Prof. Dr. Paulo Antonio Silvani Caetano (UFSCar)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional.

Dedicatória

Dedico este trabalho a todos os meus familiares, companheiros de programa/profissão e alunos. Cada um dos quais, com suas parcelas de contribuições, fossem elas acadêmicas, motivacionais e afetivas, foram fundamentais na construção do mesmo.

Simplicidade na qualidade e fugacidade na quantidade.

Epicuro.

Agradecimentos

Agradeço primeiramente ao Departamento de Matemática da Universidade Federal de São Carlos, pela oportunidade de ser aluno de um dos seus programas de mestrado. Um agradecimento especial a todos os meus professores do PROFMAT, pessoas com as quais aprendi muito e que são exemplos de carreira a ser seguida. Neles enxergo cidadãos que são formidáveis academicamente, e que estão seguramente no posto de professores do mais alto nível com os quais já tive o privilégio de me relacionar. São seres altamente empáticos e competentes, alguns bem divertidos por sinal, e que foram essenciais no crescimento acadêmico e pedagógico que obtive.

Em especial, agradeço imensamente ao meu orientador Dr. João Carlos Vieira Sampaio, pela paciência e orientação, no que talvez seja, o momento mais tenso de toda a minha trajetória. Um professor que abriu as portas de sua casa para mim, que esteve presente em todos os momentos durante as conclusões dos créditos das disciplinas, e que agora novamente se faz presente durante a construção desta dissertação. Como esquecer as incríveis palavras muito bem humoradas que ele dizia logo pela manhã, quando acompanhava seu filho, e grande companheiro, até a porta da sala de aula. Como esquecer dos inúmeros cafés que tomamos durante os intervalos de exaustivas aulas, momentos esses que nos permitiam relaxar um pouco. Poder ter o meu nome atrelado de alguma forma ao desse grande ser humano, é motivo de colossal orgulho e satisfação de minha parte.

Não poderia deixar de agradecer ao meu grande professor Dr. Ivo Machado da Costa. Um homem em que não cabem adjetivos para qualificá-lo. Jamais me esquecerei, de todas as aulas extras, que ele gentilmente nos fornecia, afim de tratarmos dos mais relevantes assuntos pertinentes á nossa formação. Um ser humano fantástico, que mesmo nos momentos difíceis que passava, nunca deixava de nos atender com uma paciência e dedicação louvável. E haja paciência viu, pois nossas dúvidas eram bem elementares, algo que pra ele certamente fosse muito trivial, mas que ele prontamente nos atendia. Seu entusiasmo ao lecionar, encanta a todos que tem a oportunidade de assistir suas aulas. Ao grande professor Ivo, saiba que lhe tenho como referência enquanto matemático e pessoa.

Por fim, quero agradecer aos meus colegas de programa Brenda, Guilherme, Erick, Luiz, João Victor, João Paulo, João, Ingrid e Pedro pelas inúmeras horas de estudo, companheirismo e descontração. Um agradecimento notável também á minha namorada Raíssa, que me é fonte de inspiração profissional e pessoal. E encerrando, um agradecimento único aos companheiros de moradia Rodolfo, Priscila, Rodrigo, Arthur, Renann, Moisés e Vitor, que nunca mediram esforços para me auxiliar de qual forma fosse.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Resumo

Este trabalho propõe-se a apresentar algumas das maneiras encontradas por grandes matemáticos, para se trabalhar com o problema da primalidade de um número inteiro. Para tanto, são apresentados algoritmos clássicos e modernos, com foco em exemplos de aplicação. Sugere-se também uma situação de aprendizagem que trabalha com o problema da primalidade sob o olhar da fatoração, buscando mostrar que fatorar corretamente um número, pode se tornar uma ferramenta útil na resolução de outros problemas que não sejam o da primalidade. Por fim, apresenta de uma forma pouco comum, nos materiais da Secretaria Estadual de Educação de São Paulo, maneiras de se trabalhar conceitos matemáticos do Ensino Fundamental.

Palavras-chave: Ensino de Matemática, Prática docente, Números primos.

Abstract

This work proposes to present some forms found by important mathematicians to work with the primality problem of whole number. Therefore, classics and moderns algorithm are presented with a lot examples of application. Different activites to work with the primality problem under the view of factorization are also suggested, indicating that factorizing perfectly a number can be a resourceful tool to solve other problems. Finally, this work presents, in the school supplies of the State Education Department of São Paulo, ways to work with mathematical concepts in the elementary school.

Key Words: Mathematics teaching, Teaching practice; Prime Numbers.

Lista de Figuras

2.1 Giuseppe Peano. 12

2.2 Euclides de Alexandria. 24

2.3 Arquimedes de Siracusa. 24

2.4 Carl Friederich Gauss. 41

2.5 Pierre de Fermat. 53

2.6 John Wilson. 57

2.7 Édouard Lucas e Derrick H. Lehmer. 63

2.8 Marin Mersenne. 63

2.9 Gary Miller e Michael Rabin. 69

3.1 Fluxograma para determinar a primalidade de um número natural n. 87

1 Caderno do Aluno 2020, p.223 106

Lista de Tabelas

3.1 Controle de entradas do jogo. 91

3.2 Cronograma da situação de aprendizagem. 100

1 Os quinze primeiros números primos. 106

2 Tabela de Divisores. 107

3 Fatoração de alguns pseudoprimos na base 2 109

4 Fatoração de outros pseudoprimos na base 2 111

Sumário

1 Introdução **1**

2 O conjunto $\mathbb{Z}$ dos números inteiros **7**

2.1 Noções básicas sobre conjuntos 7

2.2 Axiomas e propriedades básicas de $\mathbb{Z}$ 11

2.2.1 Ordenação em $\mathbb{Z}$ 15

2.2.2 A divisão em $\mathbb{Z}$. 20

2.2.3 Divisibilidade. 20

2.2.4 Divisão euclidiana 23

2.3 Representação posicional de números inteiros 26

2.4 Máximo divisor comum. 30

2.4.1 Mínimo múltiplo comum 34

2.5 Números primos 36

2.6 A aritmética dos restos 40

2.6.1 Congruências 40

2.6.2 Congruências e somas 43

2.6.3 Congruências e produtos 45

2.7 Alguns testes de primalidade 46

2.7.1 O teste de divisibilidade 47

2.7.2 O teste de composição de Fermat 53

2.7.3 O teste de Wilson 56

2.7.4 O teste Lucas-Lehmer 62

2.7.5 O teste probabilístico Miller-Rabin. 69

3 Construção de uma atividade pedagógica 77

3.1 Características do público alvo e escolha do tema 77

3.2 Planejando a atividade pedagógica 79

3.2.1 Etapa 1: Retomada e noções de divisibilidade. 80

3.2.2 Etapa 2: Múltiplos, divisores, mmc e mdc. 82

3.2.3 Etapa 3: Compostos ou primos. 85

3.2.4 Etapa 4: O teorema fundamental da aritmética. 88

3.2.5 Etapa 5: O jogo da fatoração simultânea. 90

3.2.6 Etapa 6: A Fatoração como ferramenta para o cálculo de mdc e mmc. 93

3.2.7 Etapa 7: Problemas que envolvem as ideias de mdc e mmc. 96

4 Considerações finais 101

Referências 104

Apêndices 106

1 Introdução

Em alemão, a palavra *zahl* significa número. É comum que autores de livros de matemática básica e superior, associem o uso da palavra zahl com o símbolo $\mathbb{Z}$, que representa o conjunto dos números inteiros. Segundo [6] um número é o resultado da comparação entre uma grandeza e a unidade. Se essa grandeza for discreta, essa comparação será chamada de uma contagem, e o resultado será um número inteiro. Se essa grandeza for contínua, essa comparação será chamada de medição, e o resultado será um número real.

Por grandeza, entendemos ser tudo aquilo que pode ser contado, medido, pesado, entre outros. Se tal grandeza for discreta, então elas se encaixam naquelas que podem ser contadas, e nos remetem a ideia de quantidades. Sempre que estivermos trabalhando com contagens, os números inteiros não negativos nos fornecerão uma representação bem satisfatória. Mas e os inteiros negativos?

Não nos é muito natural, ao falarmos de números inteiros, ter um modelo mental adequado para a representação de um número negativo. Por tal razão eles sempre foram, de certa forma, vistos como de importância irrelevante para os problemas do cotidiano. O desenvolvimento do comércio, as transações financeiras, a representação de um sentido oposto, entre outros, trataram de dar aos números negativos, um sentido mais prático nas atividades mundanas.

Por outro lado, saindo um pouco da utilidade associada, acreditamos que os números inteiros são belos por si só, e reconhecer a beleza das propriedades referentes a eles, é uma atividade suficiente. Mesmo que eles não tivessem função alguma no nosso cotidiano, estudá-los já seria uma das atividades mais nobres e engrandecedoras que poderiam ser realizadas pelo ser humano. No presente trabalho, espera-se que essas duas formas de olhar para os números inteiros, numa visão mais prática e em outra mais pura, possam ser percebidas.

Ao contemplar as grandes contribuições dos árabes para o desenvolvimento da ciência, não poderíamos deixar de falar dos algarismos indo-arábicos, um peculiar conjunto de dez símbolos (0, 1, 2, 3, 4, 5, 6, 7, 8 e 9) que pode ser misturado em qualquer quantidade, com ou sem repetição, para fornecer-nos um modo eficiente de representar contagens ou ordenações de elementos de quaisquer natureza. Estamos nos referindo à representação posicional decimal dos números inteiros, criada pelos indianos e divulgada pelos árabes.

Dentro do conjunto dos números inteiros não negativos (que para os propósitos do texto são suficientes), temos inicialmente um curioso símbolo 0 (zero), para representar a ausência de unidades. Ao avançar naturalmente no nosso universo numérico, temos o próximo símbolo 1 (um), que nos dá a ideia da unidade. Qualquer outro número inteiro não negativo pode entendido como um múltiplo da unidade. Após o 1, todos os infinitos números inteiros que podem ser frutos da imaginação humana, são classificados em apenas dois conjuntos disjuntos (conjuntos cuja interseção é vazia): os números compostos e os números primos.

Para se ter uma ideia mais clara de números compostos ou primos, faz-se necessário que seja apresentado um conceito muito importante dentro do conjunto dos números inteiros, que é a relação de divisibilidade. Grosso modo, um número inteiro qualquer a divide um outro número inteiro qualquer b quando, ao efetuarmos uma divisão euclidiana (tal divisão ficará clara no decorrer do texto) de b por a, tivermos sempre 0 como resto. Como exemplo, o número inteiro 8 divide o número inteiro 48, pois o resto da divisão euclidiana de 48 por 8 resulta em 0. Se um número inteiro qualquer a divide outro número inteiro qualquer b, então dizemos que a é um divisor de b. Se a é um número inteiro então, 1 divide a e a divide a. Os números 1 e a ficam então conhecidos como os *divisores triviais* de a.

Um número inteiro não negativo será dito composto, se ele tiver algum outro divisor que não sejam os *triviais*. Como exemplo, o número 4 é composto, pois 2 o divide, e sendo assim, ele possui algum outro divisor que não sejam os *triviais* 1 e 4. Obviamente, como os conjuntos dos compostos e dos primos são disjuntos, teremos que um número será primo quando seus únicos divisores forem os *triviais*. O número 2 é primo, pois nota-se que os únicos números que o dividem perfeitamente, são os *triviais* 1 e 2.

Caminhando no sentido crescente dentro do conjunto dos números inteiros não negativos, torna-se cada vez mais trabalhoso descobrir se determinado número é composto ou primo. Pois a medida que o valor absoluto desse número aumenta, fica cada vez mais difícil encontrar candidatos a divisores. Mas por que classificar os números dessa forma? Não seria mais prático classificá-los, por exemplo, em pares ou ímpares?

A resposta à primeira pergunta, pode ser mais bem compreendida, quando conseguimos apreciar o encanto desses números por si só. A beleza inerente dos números primos torna-se mais nítida quando os enxergamos como uma espécie de matéria prima, responsável pela criação de qualquer número inteiro. Pode-se pensar, que em última análise, se formos "quebrando" ou dividindo um número inteiro em partes cada vez menores, chegaremos em um ponto onde tais partes seriam tão fundamentais, que não poderiam mais ser divididas. É esta ideia do *indivisível* que chamamos de números primos, algo como o átomo para Demócrito.

Quanto à segunda pergunta, é fácil ver que classificar os números inteiros não negativos em pares ou ímpares, é realmente bem mais prático, pois temos que responder a uma pergunta muito mais rápida. Se um número inteiro não negativo for par, então 2 vai dividi-lo. Em caso contrário, 2 não vai dividi-lo. E a divisão de um número inteiro por 2, está longe de ser um problema trabalhoso. Essas duas questões vão de encontro com as ideias da praticidade e das aplicações da matemática, e dos amantes desvinculados de praticidades, que estudam matemática por ser prazeroso apenas.

Foi pensando em mesclar esses dois pontos de vista (prático e puro) que o texto dessa dissertação foi produzido. Ao mesmo tempo em que estamos interessados em conhecer mais e melhor as tentativas dos matemáticos, de buscar formas alternativas de responder ao questionamento sobre o caráter de um número inteiro não negativo (ser composto ou primo), também buscamos ver como o estudo desse problema pode contribuir para o desenvolvimento de habilidades referentes a um determinado período da vida escolar de um aluno. Mais precisamente, procura-se estudar de que forma o estudo do problema da determinação da primalidade de um número inteiro não negativo, pode contribuir para que o aluno desenvolva habilidades para resolver também outros problemas relacionados a conteúdos de sua formação na educação

básica. Como exemplos de tais problemas, estão os cálculos e aplicações dos conceitos de mínimo múltiplo comum e máximo divisor comum.

Com esse pensamento, optamos por criar inicialmente um capítulo com algumas ideias fundamentais a respeito da noção de conjunto e suas relações, além de uma breve pincelada em propriedades referentes aos números inteiros. Em seguida, são apresentadas também, de forma sucinta, as ferramentas matemáticas necessárias para se atacar o problema, sob outros pontos de vista, que não sejam a clássica fatoração. Tal capítulo inclui também informações sobre a infinidade dos números primos, bem como ideias relacionadas ao Teorema Fundamental da Aritmética.

A última parte do capítulo começa com a apresentação da fatoração de um número inteiro, que se constitui em um algoritmo clássico que resolve o problema da determinação da primalidade, além de expor os fatores primos dos números que são compostos. Tal algoritmo, apesar de resolver o problema, não se constitui no método mais plausível possível. Em se tratando de métodos não muito eficazes na resolução do problema, é apresentado o Teorema de Wilson, que entre outras aplicações, pode também ser usado para esse fim. Tanto a fatoração quanto o Teorema de Wilson, resolvem integralmente o problema, mas se tem o custo do tempo de execução, que se torna tão maior quanto o número a ser testado.

De modo a dar uma outra visão com relação ao tempo de execução, apresentamos o teste de primalidade Lucas-Lehmer. Esse teste resolve parcialmente o problema, ou seja, apesar de não conseguir determinar a primalidade de um número inteiro qualquer, o faz para uma classe especial deles, conhecidos como números de Mersenne. Para finalizar são apresentados testes de primalidade do tipo probabilístico, que apontam se determinado inteiro a ser testado, é composto ou provavelmente primo, tais como o teste de composição de Fermat e o teste Miller-Rabin. Toda essa parte em que abordam-se os testes, está focada em exemplos de aplicação, realmente afim de mostrar o funcionamento dos mesmos.

Avançando no texto, é feita uma proposta de situação de aprendizagem que aborda o problema da determinação da primalidade através do algoritmo clássico da fatoração. Baseado

em habilidades da Base Nacional Comum Curricular, o problema é utilizado como uma forma de despertar a atenção e a curiosidade dos alunos, além da importância, para o próprio desenvolvimento escolar dos mesmos, de se conhecer uma lista relativamente pequena de números primos, afim de se fatorar um número inteiro dado. Acreditamos que o processo de fatoração, além de ser curioso, melhora as habilidades referentes a divisão euclidiana e é de grande ajuda na resolução de outros problemas que aparecem nas séries/anos posteriores.

Por fim, são feitas algumas considerações finais sobre o trabalho, e apresentados alguns apêndices contendo fatorações de tipos específicos de números inteiros não negativos e uma proposta de avaliação a ser aplicada no fim da situação de aprendizagem, afim de se criar subsídios para uma *análise a posteriori* da situação.

Isso posto, esperamos que o presente trabalho cumpra com seu ideal inicial, de se tornar tanto prático, no sentido de trazer a questão da primalidade para dentro da sala de aula, e utilizar esse problema como uma maneira de se ensinar e aprender matemática básica, mas que também não deixe de ter seu caráter mais puro, de se conhecer as propriedades de números inteiros e admirá-los por si só, servindo assim como um estímulo para as mentes dos amantes da rainha das ciências.

2 O conjunto $\mathbb{Z}$ dos números inteiros

Desde os primórdios das civilizações, o homem, em suas atividades cotidianas ligadas à sua sub-existência, necessitava da ideia de contar, ou seja, representar com símbolos os elementos de uma determinada contagem. Essa forma de contar foi feita de maneiras diferentes, por muitas civilizações, até evoluir para o modo como o fazemos hoje na base decimal e com os algarismos indo-arábicos. De modo a organizar as suas tarefas diárias, o homem também tinha a necessidade de representar qual tarefa executar previamente, ou seja, também surge a necessidade de ordenar as coisas, dizer quem ou o quê tem prioridade e necessita ser feito primeiro, ou o que pode ser deixado em segundo plano. Dizemos então que a necessidade de contar e ordenar é inerente ao ser humano, é um processo natural do homem.

2.1 Noções básicas sobre conjuntos

No decorrer desta seção seremos familiarizados com as noções básicas sobre conjuntos e sua nomenclatura usual. Assim como em [5] e para o propósito do trabalho será feita uma abordagem menos formal de tais noções e na medida do possível, a maioria das afirmações feitas serão acompanhadas de exemplos.

O conceito mais elementar de *conjunto* não é definido, porém é intuitivo pensar em um conjunto como uma *coleção* de objetos. Tais objetos que formam esse conjunto, são conhecidos como *elementos* do conjunto.

Os conjuntos geralmente são representados por letras do alfabeto latino maiúsculas como A, B, C e etc, enquanto que em geral os elementos são representados por letras do alfabeto latino minúsculas tais como a, b, c e etc. Costuma-se colocar os elementos de um conjunto entre chaves $\{\}$. Por exemplo, o conjunto dos números ímpares positivos menores do

que 10, pode ser representado como

$$I = \{1, 3, 5, 7, 9\}.$$

A principal relação entre elementos e conjuntos é conhecida como *relação de pertinência*. De modo geral se um elemento a *pertence* ao conjunto A escrevemos $a \in A$. No conjunto I citado acima temos, por exemplo, que $3 \in I$. Analogamente, se um determinado elemento a *não pertence* ao conjunto A escrevemos $a \notin A$. Novamente, utilizando o conjunto I temos, por exemplo, que $8 \notin I$.

Um conjunto será dito *bem definido* se sempre for possível determinar se um elemento qualquer a, pertence ou não pertence a A. Por exemplo, se A for o conjunto de todos os números ímpares positivos, podemos representá-lo como

$$A = \{1, 3, 5, 7, 9, 11, 13, ...\}$$

e obviamente não se consegue representar todos os elementos $a_i \in A$ pois se trata de um conjunto infinito. Porém A está bem definido, pois é um conjunto que contém *todos* os números ímpares positivos e seja qual for o número inteiro que desejamos saber se, pertence ou não a A, isso é sempre possível. Por exemplo, sabemos que $41047 \in A$, sem precisar exibir todos os elementos de A.

Por vezes, na impossibilidade de representar todos os elementos de um conjunto, torna-se mais viável caracterizá-lo através de uma propriedade comum a todos os elementos pertencentes ao conjunto, o fazendo da seguinte forma

$$X = \{x \text{ tal que } x \text{ tem a propriedade P}\}.$$

No exemplo acima para o conjunto A de todos os números ímpares positivos, como a propriedade *ser ímpar positivo* é comum a todos os elementos do conjunto poderíamos representá-lo

como

$$A = \{a \text{ tal que } a \text{ é ímpar positivo}\}.$$

É comum também, ao estarmos no campo matemático, e fazendo uso da linguagem matemática, trocar as palavras por símbolos ou caracteres mais curtos, sendo assim, é de praxe trocar as palavras *tal que* pelo símbolo "|"ou ";" e a frase *tem a propriedade p* por "$P(x)$", portanto o conjunto X poderia ser escrito como

$$X = \{x \mid P(x)\} \text{ ou também por } X = \{x \ ; \ P(x)\}$$

e durante o texto faremos uso do símbolo ";" para representar *tal que*.

Quando a propriedade P refere-se aos elementos de um conjunto U então o conjunto X escreve-se como

$$X = \{x \in U \, ; \, P(x)\}$$

Existem situações em que o conjunto analisado possui apenas um elemento, quando isso ocorrer o conjunto será chamado de *conjunto unitário* e representado por $X = \{x\}$, como por exemplo, o conjunto dos números pares positivos e menores do que três pode ser representado como $X = \{2\}$. Entretanto, existem situações em que o conjunto não possui nenhum elemento, sendo assim, o conjunto será chamado de *conjunto vazio* e representado pelo símbolo $\varnothing$, como por exemplo, se X é o conjunto dos números ímpares positivos maiores do que um e menores do que três temos que $X = \varnothing$.

Vejamos agora uma maneira de relacionar conjuntos analisados, sejam X e Y dois conjuntos, diz-se que X é *subconjunto* de Y, se todo elemento de X também é elemento de Y, ou equivalentemente, $\forall\, x \in X \Longrightarrow x \in Y$. Também costuma-se dizer que X *está contido* em Y ou equivalentemente Y *contém* X, e representa-se por

$$X \subset Y \text{ ou } Y \supset X.$$

Analogamente, sendo X e Y dois conjuntos, diz-se que X *não é um subconjunto* de Y quando existe pelo menos um $x \in X$ tal que $x \notin Y$, dizemos também que X *não está contido* em Y, ou equivalentemente que, Y *não contém* X, e representamos por

$$X \not\subset Y \text{ ou } Y \not\supset X.$$

Exemplificando as situações acima, sejam $X = \{1, 2, 3\}$ e $Y = \{1, 2, 3, 4, 5, 6, 7\}$ temos que $X \subset Y$, pois $1 \in X$ e $1 \in Y$, $2 \in X$ e $2 \in Y$ e ainda $3 \in X$ e $3 \in Y$, ou seja, $\forall x \in X \Longrightarrow x \in Y$.

Uma ideia não muito intuitiva porém verdadeira é que para todo conjunto X sempre temos $\varnothing \subset X$. Suponha que $\varnothing \not\subset X$, pela definição acima, deveria existir $x \in \varnothing$ tal que $x \notin X$. No entanto, não existe qualquer $x \in \varnothing$. Assim, nossa suposição é absurda. Logo, devemos ter $\varnothing \subset X$.

Sejam ainda dois conjuntos X e Y. Temos X *igual* a Y se, e somente se, $X \subset Y$ e $Y \subset X$. Denota-se por $X = Y$. Se X *não é igual* a Y, denotamos por $X \neq Y$, ou seja, temos $X \not\subset Y$ ou $Y \not\subset X$.

Dado um conjunto X, definimos o *conjunto das partes de X* e denotamos por $P(X)$, o conjunto de todos os subconjuntos de X e em particular sempre temos que $\varnothing \in P(X)$ e $X \in P(X)$. Por exemplo, se $X = \{2, 4, 6\}$ temos

$$P(X) = \{\varnothing, \{2\}, \{4\}, \{6\}, \{2, 4\}, \{2, 6\}, \{4, 6\}, \{2, 4, 6, \}\}$$

e de uma maneira geral, pode-se provar que se o conjunto X possui x elementos, então a cardinalidade de $P(X)$ é dada por 2^x.

Para finalizar essa seção, falaremos de maneira breve sobre algumas operações fundamentais entre conjuntos, as propriedades das operações citadas podem ser encontradas em [6].

Dados, por exemplo, dois conjuntos A e B definimos a *união* dos conjuntos A e B e

representamos por $A \cup B$ o conjunto formado pelos elementos de A junto aos elementos de B. Assim

$$A \cup B = \{x\,;\, x \in A \text{ ou } x \in B\}.$$

Por exemplo, se $A = \{8, 9, 10\}$ e $B = \{9, 10, 11\}$ então $A \cup B = \{8, 9, 10, 11\}$.

Analogamente, dados dois conjuntos A e B definimos a *interseção* dos conjuntos A e B e representamos por $A \cap B$ o conjunto formado pelos elementos em comum de A e B. Assim

$$A \cap B = \{x\,;\, x \in A \text{ e } x \in B\}.$$

Por exemplo, se $A = \{8, 9, 10\}$ e $B = \{9, 10, 11\}$ então $A \cap B = \{9, 10\}$.

Por fim, dados dois conjuntos A e B definimos a *diferença* entre os conjuntos A e B e representamos por $A - B$ o conjunto formado pelos elementos de A que não estão em B. Assim

$$A - B = \{x\,;\, x \in A \text{ e } x \notin B\}.$$

Por exemplo, se $A = \{8, 9, 10\}$ e $B = \{9, 10, 11\}$ então $A - B = \{8\}$.

2.2 Axiomas e propriedades básicas de $\mathbb{Z}$

Nesta seção iremos fazer um estudo do conjunto dos números inteiros e suas principais propriedades, que fundamentam os testes de primalidade que serão apresentados no próximo capítulo. Consideraremos conhecido um subconjunto de destaque dentro do conjunto dos números inteiros: o conjunto dos números naturais que será representado pelo símbolo $\mathbb{N}$, e costumeiramente apresentado como

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

No final do século XIX, os matemáticos preocupados em deixar sua ciência em bases

bem sólidas, começaram a repensar todos os conceitos que estudavam há tempos, e a partir disso a ideia de número foi intensamente trabalhada. Giuseppe Peano, um grande matemático italiano, se encarregou de nos apresentar a caracterização dos números naturais baseada em quatro axiomas (proposições auto evidentes que são tomadas como ponto de partida em uma teoria, sem que seja necessário demonstrá-las), que ficaram conhecidos como os *axiomas de Peano*. Neste trabalho tais axiomas serão enunciados, porém para uma verificação do modo como as operações e propriedades dos números naturais foram deduzidas a partir desses axiomas, sugerimos que seja visto [6].

Figura 2.1: Giuseppe Peano.

Fonte: [10].

A partir dos axiomas de Peano são definidas duas operações entre números naturais sendo uma operação de adição $(+)$ e outra de multiplicação $(\cdot)$. Após essa definição, e para os propósitos apresentados no presente trabalho, os axiomas podem ser enunciados da seguinte forma:

P(1): Existe um único número natural, representado pelo símbolo 1, que não é sucessor de nenhum outro número natural.

P(2): Se n é um número natural, então seu **sucessor** $n+1$ também é um número natural.

P(3): Se dois números naturais m e n têm o mesmo sucessor, isto é, se $m+1=n+1$, então $m=n$.

P(4): Seja $X \subset \mathbb{N}$, se

- $1 \in X$ e
- $\forall\, n,\ n \in X \Rightarrow n + 1 \in X$,

então $X = \mathbb{N}$.

Em [2] encontramos que *o conceito de número inteiro originou-se do conceito bem mais antigo de número natural, cuja criação objetivava resolver problemas de contagem. Os números negativos têm sido considerados esporadicamente desde a antiguidade, mas sempre com muita desconfiança por parte dos matemáticos até que, a partir do desenvolvimento das atividades mercantis que ocorriam na Europa no final da Idade Média, sentiu-se a necessidade de considerar os inteiros relativos e com eles efetuar operações*.

Assim como pode-se ver em [4] assumiremos portanto, que existe um conjunto denominado $\mathbb{Z} = (\mathbb{N} \cup \{0\}) \cup (-\mathbb{N})$, onde $-\mathbb{N}$ é o conjunto dos simétricos dos elementos de $\mathbb{N}$, cujos elementos são chamados de números inteiros, tendo um maior destaque os elementos 0 (zero) e 1 (um) e munido de duas operações, a adição $(+)$ e a multiplicação $(\cdot)$. Sendo a e b dois números inteiros, representaremos por $a + b$ a soma de a e b e $a \cdot b$ ou ab o produto de a e b e assumiremos também que os inteiros e as operações de adição e multiplicação satisfazem os seguintes axiomas:

1. *Fechamento de* $\mathbb{Z}$: Sejam $a, b \in \mathbb{Z}$ então $a + b \in \mathbb{Z}$ e $a \cdot b \in \mathbb{Z}$.
2. *Leis comutativas*: $\forall\, a, b \in \mathbb{Z}$ tem-se $a + b = b + a$ e $a \cdot b = b \cdot a$.
3. *Leis associativas*: $\forall\, a, b, c \in \mathbb{Z}$ tem-se $(a+b)+c = a+(b+c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
4. *Leis de existência de elementos neutros*: $\forall\, a \in \mathbb{Z}$ tem-se $a + 0 = a$ e $a \cdot 1 = a$.
5. *Lei distributiva* (da multiplicação em relação à adição): $\forall\, a, b, c \in \mathbb{Z}$ temos que $a \cdot (b + c) = a \cdot b + a \cdot c$.

6. *Lei da existência de inversos aditivos*: $\forall\, a \in \mathbb{Z}$ existe $b = (-a)$ tal que $a + b = 0$. Sendo $a, b \in \mathbb{Z}$ define-se $a - b = a + (-b)$

7. *Lei do cancelamento da multiplicação*: Se $a, b, c \in \mathbb{Z}$, com $c \neq 0$ e tais que $a \cdot c = b \cdot c$, então $a = b$.

A partir dos axiomas apresentados acima, podemos deduzir duas propriedades interessantes sobre os números inteiros.

Proposição 2.1. *Cada número inteiro a tem um único inverso aditivo, ou seja, para cada $a \in \mathbb{Z}$ existe um único $a' \in \mathbb{Z}$ tal que $a + a' = 0$.*

Demonstração. Seja $a \in \mathbb{Z}$. Se $a', a'' \in \mathbb{Z}$ são tais que $a + a' = 0$ e $a + a'' = 0$, então a associatividade e a comutatividade da adição, juntamente com o fato de 0 ser elemento neutro para tal operação, dão-nos

$$a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = (a + a') + a'' = 0 + a'' = a'' \Leftrightarrow a' = a''.$$ □

Proposição 2.2. $\forall\, a \in \mathbb{Z}$ *tem-se* $a \cdot 0 = 0$.

Demonstração. A existência do elemento neutro da adição e a distributividade da multiplicação em relação a adição, nos dão que

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

Somando $-(a \cdot 0)$ aos membros extremos da igualdade, e utilizando a existência da unicidade do inverso aditivo, da associatividade, da comutatividade e da existência do elemento neutro da adição, obtemos

$$a\cdot 0+(-a\cdot 0) = (-a\cdot 0)+a\cdot 0+a\cdot 0 \Leftrightarrow 0 = -(a\cdot 0)+a\cdot 0 = -(a\cdot 0)+(a\cdot(0+0)) = -(a\cdot 0)+(a\cdot 0+a\cdot 0) = (-(a\cdot 0)+a\cdot 0)+a\cdot 0 = 0+a\cdot 0 = a\cdot 0 \Leftrightarrow 0 = a\cdot 0 \Leftrightarrow a\cdot 0 = 0.$$ □

2.2.1 Ordenação em $\mathbb{Z}$

Assim como em [2] e [4] e utilizando o subconjunto $\mathbb{N} \subset \mathbb{Z}$ iremos admitir que em $\mathbb{Z}$ valem os seguintes axiomas:

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

9. *Lei da Tricotomia*: Para cada $a \in \mathbb{Z}$ vale uma, e somente uma das afirmações:

$$a \in \mathbb{N}\,,\ a = 0\,,\ -a \in \mathbb{N}.$$

Denotando, como já é hábito, $a > 0$, no lugar de $a \in \mathbb{N}$, pode-se reescrever os axiomas de ordenação da seguinte maneira:

- Se $a > 0$ e $b > 0$, então $a + b > 0$ e $a \cdot b > 0$.
- Para cada $a \in \mathbb{Z}$, tem-se uma e somente uma das afirmações:

$$a > 0\,,\ a = 0\,,\ -a > 0.$$

Sendo a e b inteiros quaisquer dizemos, por definição, que $a < b$ (a é menor do que b), ou que $b > a$ (b é maior do que a), se $b - a > 0$. Escrevemos $a \leqslant b$ (a é menor ou igual que b) quando $a < b$ ou $a = b$ e escrevemos $a \geqslant b$ (a é maior ou igual que b) quando $a > b$ ou $a = b$. Assumiremos também que a relação "menor ou igual que"é uma relação de ordem, pois possui as seguintes propriedades:

- É reflexiva: $\forall\, a \in \mathbb{Z},\ a \leqslant a$.
- É antissimétrica: $\forall\, a, b \in \mathbb{Z},\ a \leqslant b$ e $b \leqslant a \Rightarrow a = b$.
- É transitiva: $\forall\, a, b, c \in \mathbb{Z},\ a \leqslant b$ e $b \leqslant c \Rightarrow a \leqslant c$.

Muitas propriedades da ordenação dos números inteiros podem ser demonstradas utilizando os axiomas de ordenação e as propriedades das operações de adição e multiplicação. Listamos abaixo algumas dessas propriedades.

Proposição 2.3. *Vale a transitividade na relação "menor do que", ou seja,* $\forall\ a, b, c \in \mathbb{Z}$, $a < b$ *e* $b < c \Rightarrow a < c$.

Demonstração. $a < b \Rightarrow b - a > 0$ e $b < c \Rightarrow c - b > 0 \Leftrightarrow c - a = c - b + b - a > 0 \Rightarrow c - a > 0 \Rightarrow a < c$. □

Proposição 2.4. *Sendo* $a, b, c \in \mathbb{Z}$,

1. *Se* $a < b$ *e* $c > 0$, *então* $a \cdot c < b \cdot c$;
2. *Se* $a < b$ *e* $c < 0$, *então* $a \cdot c > b \cdot c$.

Demonstração. 1. $a < b \Rightarrow b - a > 0$. Assim, como $c > 0$ e pelo fato de $\mathbb{N}$ ser fechado para a multiplicação, temos

$b \cdot c - a \cdot c = (b - a) \cdot c > 0 \Rightarrow b \cdot c - a \cdot c > 0 \Leftrightarrow a \cdot c < b \cdot c$.

2. $a < b \Rightarrow b - a > 0$.

   De $c < 0 \Rightarrow c + (-c) < 0 + (-c) \Rightarrow c - c < -c \Rightarrow 0 < -c \Rightarrow -c > 0$.

   Assumindo que $(-a) \cdot (-c) = a \cdot c$ e utilizando novamente o fato de $\mathbb{N}$ ser fechado para a multiplicação, temos

   $a \cdot c - b \cdot c = (-a) \cdot (-c) + b \cdot (-c) = -c \cdot ((-a) + b) = -c \cdot (b - a) > 0 \Leftrightarrow a \cdot c > b \cdot c$.

□

Na demonstração da proposição 2.4 assumimos que $(-a) \cdot (-c) = a \cdot c$, porém essa afirmação pode ser demonstrada de algumas maneiras, e para o modo como o faremos, precisamos antes de alguns resultados auxiliares, quais sejam, em primeiro o fato de que $(-1) \cdot (-1) = 1$ e depois que $(-1) \cdot a = -a$.

Para demonstrar que $(-1)\cdot(-1) = 1$, começamos nos atentando que pela proposição 2.2 temos $0 \cdot 0 = 0$ e pela existência do inverso aditivo temos que $1 + (-1) = 0$.

Daí, utilizando a propriedade distributiva da multiplicação sobre a adição e o fato de 1 ser o elemento neutro da multiplicação temos que

$((1 + (-1)) \cdot ((1 + (-1)) = 0 \Leftrightarrow 1 \cdot 1 + 1 \cdot (-1) + (-1) \cdot 1 + (-1) \cdot (-1) = 0 \Leftrightarrow 1 - 1 - 1 + (-1) \cdot (-1) = 0 \Leftrightarrow -1 + (-1) \cdot (-1) = 0 \Leftrightarrow (-1) \cdot (-1) = 1.$

Agora, para demonstrarmos que $(-1) \cdot a = -a$, inicialmente começamos a considerar que $((-1) + 1) \cdot a = 0 \cdot a = 0$, e utilizando a propriedade distributiva da multiplicação em relação a adição, a existência do inverso aditivo e dos elementos neutros da multiplicação e da adição tem-se

$((-1)+1)\cdot a = 0 \Leftrightarrow (-1)\cdot a+1\cdot a = 0 \Leftrightarrow (-1)\cdot a+a = 0 \Leftrightarrow (-1)\cdot a+a+(-a) = 0+(-a) \Leftrightarrow (-1)\cdot a+0 = (-a) \Leftrightarrow (-1)\cdot a = -a.$

Finalmente para provar que $(-a)\cdot(-c) = a\cdot c$, basta observarmos que $(-a)\cdot(-c) = ((-1)\cdot a)\cdot((-1)\cdot c) = (-1)\cdot(-1)\cdot a\cdot c = 1\cdot a\cdot c = a\cdot c.$

Continuemos agora com a apresentação do último axioma que caracteriza, de forma única, o conjunto dos números inteiros, conhecido como *Princípio da Boa Ordenação*. Antes porém, precisamos da definição que segue.

Diremos que um subconjunto S de $\mathbb{Z}$ é *limitado inferiormente*, se existir $c \in \mathbb{Z}$ tal que $c \leqslant x$ para todo $x \in S$. Diremos que $a \in S$ é um *menor elemento* de S se $a \leqslant x$ para todo $x \in S$. Convenciona-se que $\varnothing$, apesar de não possuir nenhum elemento, é limitado inferiormente, tendo qualquer número como cota inferior.

Observa-se também que, se existir um menor elemento em um subconjunto S de $\mathbb{Z}$ ele deve ser único. Suponha que a e a' são ambos menores elementos de S. Pela definição de menor elemento, devemos ter $a \leqslant a'$ e $a' \leqslant a$. No entanto $a \leqslant a'$ e $a' \leqslant a$ implica que $a = a'$.

Por exemplo, sabemos que $\mathbb{Z} \subset \mathbb{Z}$, porém não existe $c \in \mathbb{Z}$ tal que $c \leqslant x$ para todo

$x \in \mathbb{Z}$. Assim $\mathbb{Z}$ não é limitado inferiormente e nem possui um menor elemento. Analogamente $-\mathbb{N} \subset \mathbb{Z}$ não é limitado inferiormente, pois não existe $c \in \mathbb{Z}$ tal que $c \leqslant x$ para todo $x \in -\mathbb{N}$. Por outro lado $\mathbb{N} \subset \mathbb{Z}$ é limitado inferiormente, pois existe $c \in \mathbb{Z}$ (por exemplo $c = -13$) tal que $-13 \leqslant x$ para todo $x \in \mathbb{N}$. Tem-se que 1 é o menor elemento de $\mathbb{N}$. O último axioma, que caracteriza os números inteiros, é apresentado abaixo tal como feito em [2]:

10. *Princípio da Boa Ordenação*: Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Em particular, como qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente por 1, temos que todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento. Por exemplo, seja $A = \{12, 13, 14\}$ temos claramente que $A \subset \mathbb{N}$, $A \neq \varnothing$ além de ser limitado inferiormente por 1. Logo, pelo princípio da boa ordenação, temos que A possui um menor elemento. Pode-se ver, nesse exemplo, que tal elemento é 12.

O princípio da boa ordenação é muito utilizado em demonstrações de propriedades de $\mathbb{Z}$. Por vezes, é visto até em demonstrações de propriedades de números que não pertencem a $\mathbb{Z}$ (uma linda demonstração da irracionalidade de $\sqrt{2}$ utilizando o princípio da boa ordenação pode ser encontrada em [4]). Para ilustrar o uso desse princípio, daremos uma demonstração (assim como em [2]) da proposição abaixo, que é muito útil em outras demonstrações.

Proposição 2.5. *Não existe* $n \in \mathbb{Z}$ *tal que* $0 < n < 1$

Demonstração. Vamos supor, por absurdo, que $\exists\, n$ tal que $0 < n < 1$. Sendo assim, o conjunto $S = \{x \in \mathbb{Z};\, 0 < x < 1\}$ é não vazio, além de ser limitado inferiormente. Portanto, pelo princípio da boa ordenação, S possui um menor elemento a, com $0 < a < 1$. Ao multiplicar essa desigualdade por a temos

$$0 < a < 1 \Leftrightarrow 0 < a^2 < a \Leftrightarrow 0 < a^2 < a < 1.$$

Logo $a^2 \in S$ e $a^2 < a$, o que é uma contradição ao fato de a ser o menor elemento de S. Portanto deve-se ter $S = \varnothing$, e com maior razão, não existe $n \in \mathbb{Z}$ tal que $0 < n < 1$. □

Para finalizar essa seção apresentaremos a operação de potenciação e o fatorial de um número natural n. Dados dois números inteiros $a \neq 0$ e n, definimos a operação de *potenciação* como segue:

$$a^n = \begin{cases} \dfrac{1}{a^n}, & se\ n < 0; \\ 1, & se\ n = 0; \\ a, & se\ n = 1; \\ \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n}, & se\ n > 1. \end{cases}$$

Por exemplo, para $a = 3$ e $n = -4$ temos $3^{-4} = \dfrac{1}{3^4} = \dfrac{1}{3 \cdot 3 \cdot 3 \cdot 3} = \dfrac{1}{81}$.

Uma observação a ser feita é a de que o número 0^0 não é definido. A proposição abaixo lista algumas propriedades da potenciação, cujas demonstrações podem ser encontradas em [6].

Proposição 2.6. *Sejam* $a, b, n, m \in \mathbb{Z}$ *com* $a \neq 0$ *e* $b \neq 0$ *tem-se:*

- $1^n = 1$;
- $a^n \cdot a^m = a^{n+m}$;
- $a^n \div a^m = a^{n-m}$;
- $(a^n)^m = a^{n \cdot m}$;
- $a^n \cdot b^n = (a \cdot b)^n$.

Diremos que o *fatorial* de um número natural n, simbolizado por $n!$ é o produto de todos os inteiros positivos menores ou iguais que n. Por definição $0! = 1$ e de uma maneira geral tem-se que $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$.

2.2.2 A divisão em $\mathbb{Z}$.

Inciaremos esta seção falando sobre as restrições ao efetuarmos uma divisão de um número inteiro por outro inteiro não nulo em $\mathbb{Z}$. Suponha que se queira fazer a divisão do inteiro 4 pelo inteiro 2, e neste caso, temos que o resultado dessa divisão é um número inteiro, a saber 2. Porém, se ao invés de dividirmos o inteiro 4 pelo inteiro 2, quiséssemos dividir 4 por 3, o nosso resultado não seria um número inteiro. Em outro impasse estaríamos ao tentar dividir 4 por 5. O resultado novamente seria um número não inteiro. Sendo assim, nem sempre é possível dividir um inteiro por outro em $\mathbb{Z}$, e expressaremos isso através da relação de divisibilidade. Mesmo quando não existir tal relação de divisibilidade, veremos como sanar esse problema utilizando a *divisão euclidiana.*

2.2.3 Divisibilidade.

Dados dois números inteiros a e b, diremos que a *divide* b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Nesse caso, diremos também que a é um *divisor* ou um *fator* de b ou ainda, que b é um *múltiplo* de a. A negação de $a \mid b$ é $a \nmid b$, significando que não existe nenhum número inteiro c tal que $b = c \cdot a$. Quando $a \neq 0$ (e somente neste caso) dizemos também que b é divisível por a e neste caso, o inteiro c é chamado de *quociente* de b por a e é indicado por $c = \dfrac{b}{a}$.

Pela definição dada acima, temos que $0 \mid 0,\ \pm 1 \mid 0,\ \pm 2 \mid 0, ...$, pois

$0 = 0 \cdot 0$ e $0 \in \mathbb{Z}$,

$0 = 0 \cdot 1$ e $0 = 0 \cdot (-1)$ e $0 \in \mathbb{Z}$ e

$0 = 0 \cdot 2$ e $0 = 0 \cdot (-2)$ e $0 \in \mathbb{Z}$.

E de maneira geral $\forall\, a \in \mathbb{Z}$ temos $a \mid 0$, ou seja, todo número inteiro divide 0 (isto será de fato justificado na proposição 2.7). Assim, 0 tem infinitos divisores.

Ainda, pela definição temos que $\pm 1 \mid 6,\ \pm 2 \mid 6,\ \pm 3 \mid 6$ e $\pm 6 \mid 6$, pois

$6 = 6 \cdot 1$ com $6 \in \mathbb{Z}$ e $6 = -6 \cdot (-1)$ com $-6 \in \mathbb{Z}$,

$6 = 3 \cdot 2$ com $3 \in \mathbb{Z}$ e $6 = -3 \cdot (-2)$ com $-3 \in \mathbb{Z}$,

$6 = 2 \cdot 3$ com $2 \in \mathbb{Z}$ e $6 = -2 \cdot (-3)$ com $-2 \in \mathbb{Z}$ e

$6 = 1 \cdot 6$ com $1 \in \mathbb{Z}$ e $6 = -1 \cdot (-6)$ com $-1 \in \mathbb{Z}$.

Logo, os divisores de 6 são $-6, -3, -2, -1, 1, 2, 3$ e 6.

A proposição a seguir estabelece algumas propriedades úteis da divisibilidade:

Proposição 2.7. *Sejam* $a, b, c \in \mathbb{Z}$. *Tem-se que:*

1. $1 \mid a$, $a \mid a$ *e* $a \mid 0$;
2. $0 \mid a \Leftrightarrow a = 0$;
3. *A relação de divisibilidade é transitiva, ou seja, se* $a \mid b$ *e* $b \mid c$ *então* $a \mid c$.

Demonstração. (1.) $1 \mid a \Leftrightarrow \exists\, c \in \mathbb{Z}$ tal que $a = c \cdot 1$. Tomando $c = a$ o resultado segue.

$a \mid a \Leftrightarrow \exists\, c \in \mathbb{Z}$ tal que $a = c \cdot a$. Tomando $c = 1$ o resultado segue.

$a \mid 0 \Leftrightarrow \exists\, c \in \mathbb{Z}$ tal que $0 = c \cdot a$. Tomando $c = 0$ o resultado segue.

(2.) Inicialmente vamos supor que $0 \mid a$. Assim, $\exists\ c \in \mathbb{Z}$ tal que $a = c \cdot 0$. Pela proposição 2.2 conclui-se que $a = 0$. Reciprocamente, supondo que $a = 0$, basta observarmos que $0 \mid 0$, como foi provado no item anterior quando vimos que $a \mid 0\ \forall\, a \in \mathbb{Z}$.

(3.) Primeiramente $a \mid b$ e $b \mid c \Leftrightarrow \exists\ d, e \in \mathbb{Z}$ tais que $b = d \cdot a$ e $c = e \cdot b$. Assim

$$c = e \cdot b = e \cdot (d \cdot a) = (e \cdot d) \cdot a \Leftrightarrow a \mid c.$$

□

Para exemplificar o uso do item 3. da proposição 2.7, pode-se ver que $3 \mid 15$ pois $15 = 5 \cdot 3$ e $15 \mid 75$ pois $75 = 5 \cdot 15$. Assim, por transitividade, devemos ter que $3 \mid 75$, o que

de fato é válido pois $75 = 25 \cdot 3$.

A próxima proposição será de grande utilidade para fundamentar a demonstração da existência de uma infinidade de números primos. Tal demonstração será feita posteriormente, com o decorrer do texto.

Proposição 2.8. *Sejam* $a, b, c \in \mathbb{Z}$*, tais que* $a \mid (b \pm c)$*. Tem-se que* $a \mid b \Leftrightarrow a \mid c$**.**

Demonstração. Supor que $a \mid (b + c) \Leftrightarrow \exists\, d \in \mathbb{Z}$ tal que $b + c = d \cdot a$. Agora, se $a \mid b \Leftrightarrow \exists\, e \in \mathbb{Z}$ tal que $b = e \cdot a$. Assim

$$b + c = d \cdot a \Leftrightarrow e \cdot a + c = d \cdot a \Leftrightarrow c = d \cdot a - e \cdot a \Leftrightarrow c = (d - e) \cdot a \Leftrightarrow a \mid c.$$

Supondo ainda que $a \mid (b + c) \Leftrightarrow \exists\, d \in \mathbb{Z}$ tal que $b + c = d \cdot a$. Agora, se $a \mid c \Leftrightarrow \exists\, f \in \mathbb{Z}$ tal que $c = f \cdot a$. Assim

$$b + c = d \cdot a \Leftrightarrow b + f \cdot a = d \cdot a \Leftrightarrow b = d \cdot a - f \cdot a \Leftrightarrow b = (d - f) \cdot a \Leftrightarrow a \mid b.$$

Por outro lado, se $a \mid (b - c) \Leftrightarrow \exists\, g \in \mathbb{Z}$ tal que $b - c = g \cdot a$. Agora, se $a \mid b \Leftrightarrow \exists\, e \in \mathbb{Z}$ tal que $b = e \cdot a$. Assim

$$b - c = g \cdot a \Leftrightarrow e \cdot a - c = g \cdot a \Leftrightarrow -c = g \cdot a - e \cdot a \Leftrightarrow -c = (g - e) \cdot a \Leftrightarrow a \mid -c \Leftrightarrow a \mid c.$$

Por fim, supondo que $a \mid (b - c) \Leftrightarrow \exists\, g \in \mathbb{Z}$ tal que $b - c = g \cdot a$. Agora, se $a \mid c \Leftrightarrow \exists\, f \in \mathbb{Z}$ tal que $c = f \cdot a$. Assim

$$b - c = g \cdot a \Leftrightarrow b - f \cdot a = g \cdot a \Leftrightarrow b = g \cdot a + f \cdot a \Leftrightarrow b = (g + f) \cdot a \Leftrightarrow a \mid b.$$

□

Por exemplo, temos que $4 \mid 84$, o que a proposição 2.8 nos diz, é que se separarmos 84 em duas parcelas, tais que uma delas é divisível por 4, necessariamente a outra também o será. Sendo assim, seja $84 = 12 + 72$ temos que se $4 \mid (12 + 72)$ então $4 \mid 12$ se, e somente se, $4 \mid 72$, o que de fato se verifica, pois $12 = 3 \cdot 4$ e $72 = 18 \cdot 4$. E analogamente, se $84 = 104 - 20$ temos que $4 \mid (104 - 20)$ então $4 \mid 104$ se, e somente se $4 \mid 20$, o que novamente é verdadeiro pois $104 = 26 \cdot 4$ e $20 = 5 \cdot 4$.

Para o que se segue, precisamos definir a importante noção de *módulo* ou *valor absoluto* de um número inteiro. Seja $a \in \mathbb{Z}$, define-se

$$|a| = \begin{cases} a, & se\ a \geqslant 0; \\ -a, & se\ a < 0. \end{cases}$$

Nota-se que $\forall\, a \in \mathbb{Z}$ tem-se $|a| \geqslant 0$ e $|a| = 0$ se, e somente se, $a = 0$.

Por exemplo, pela definição, $|17| = 17$, pois $17 > 0$ e $|-29| = -(-29) = 29$, pois $-29 < 0$

Algumas propriedades do módulo de um inteiro a, cujas demonstrações podem ser encontradas em [2], estão listadas na proposição a seguir

Proposição 2.9. $\forall\, a, b \in \mathbb{Z}$ *e* $r \in \mathbb{N}$, *tem-se*

- $|a \cdot b| = |a| \cdot |b|$;
- $|a| \leqslant r$ *se, e somente se,* $-r \leqslant a \leqslant r$;
- $-|a| \leqslant a \leqslant |a|$.

2.2.4 Divisão euclidiana

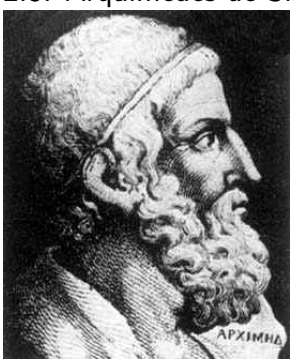
O algoritmo da Divisão Euclidiana, como seu nome aponta, está descrito numa das maiores obras primas da antiguidade. Trata-se de uma coleção de livros que descreve e fundamenta a Geometria Plana, a Geometria Espacial e a Teoria dos Números de uma maneira jamais vista até então. Fortemente baseada na Lógica, a obra é intitulada *Os Elementos* e foi escrita pelo matemático grego Euclides (aproximadamente 325 - 265 a.C.).

Antes de darmos uma demonstração do algoritmo da divisão euclidiana em $\mathbb{Z}$, semelhante àquela feita em [2], precisamos de um resultado auxiliar, conhecido como *propriedade arquimediana*, em homenagem ao seu idealizador, o exímio matemático grego Arquimedes (287 a.C. - 212 a.C.).

Figura 2.2: Euclides de Alexandria.

Fonte: [10].

Figura 2.3: Arquimedes de Siracusa.



Fonte: [10].

Proposição 2.10. *(Propriedade Arquimediana): Sejam* $a, b \in \mathbb{Z}$*, com* $b \neq 0$*. Então* $\exists\ n \in \mathbb{Z}$ *tal que* $n \cdot b > a$*.*

Demonstração. Se $b \neq 0$ então $|b| \neq 0$, e pela proposição 2.5 temos que $|b| \geqslant 1$, logo

$$(|a| + 1) \cdot |b| \geqslant |a| + 1 > |a| \geqslant a \Leftrightarrow (|a| + 1) \cdot |b| > a$$

Na desigualdade acima, se tivermos $b > 0$ basta tomarmos $n = |a|+1$ e assim teremos $n \cdot b > a$. E caso tenhamos $b < 0$ basta tomarmos $n = -(|a| + 1)$ e novamente tem-se $n \cdot b > a$. □

Para nos ajudar a entender melhor a demonstração que será dada do algoritmo da divisão euclidiana, faremos alguns exemplos numéricos de algumas situações que lá aparecerão.

Inicialmente, vamos supor que tenhamos que analisar o valor lógico da seguinte propo-

sição $6 \geqslant |4|$, o que claramente é verdadeiro, pois $|4| = 4$ e $6 \geqslant 4$. Notemos que a veracidade dessa afirmação, nos permite dizer que $\exists\, s \in \mathbb{N} \cup \{0\}$ tal que $6 = |4| + s$ e $0 \leqslant s < 6$. De fato tomando $s = 2$ temos $6 = |4| + 2$, e a condição $0 \leqslant s$ inicialmente se justifica pois se $s = 0$ ainda é válido que $6 \geqslant |4|$, e $s < 6$ deve acontecer pois, se fosse $s \geqslant 6$, por exemplo $s = 10$, teríamos $6 = |4| + 10 \Leftrightarrow -4 = |4|$, o que é um absurdo, pois $\forall\, a \in \mathbb{Z}$ tem-se $|a| \geqslant 0$.

Agora, vamos supor que $a, b \in \mathbb{Z}$ tais que $a = 5$ e $b = 3$, e consideremos o conjunto $S = \{x \in \mathbb{Z};\, x = 5 - 3 \cdot y \text{ e } y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$. Note que para que S fique bem definido devemos ter $y \leqslant 1$, e os primeiros elementos $x \in S$ são dados por $x = 5 - 3 \cdot 1 = 2$, $x = 5 - 3 \cdot 0 = 5$ e etc. Logo o conjunto pode ser reescrito na forma $S = \{2, 5, 8, 11, ...\}$.

Estamos agora em condições de demonstrar o importante

Teorema 2.11. *(Divisão Euclidiana): Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Existem dois únicos números inteiros q e r tais que, $a = b \cdot q + r$, com $0 \leqslant r < |b|$.*

Demonstração. Consideremos o conjunto $S \subset \mathbb{Z}$ tal que

$$S = \{x \in \mathbb{Z};\, x = a - b \cdot y \text{ e } y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela propriedade arquimediana (proposição 2.10), existe $n \in \mathbb{Z}$ tal que $n \cdot (-b) > -a$ logo $a - b \cdot n > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação temos que S possui um menor elemento r. Suponhamos então que $r = a - b \cdot q$. Por definição de S sabemos que $r \geqslant 0$ e vamos mostrar que $r < |b|$. Suponhamos por absurdo que $r \geqslant b$. Portanto existe um $s \in (\mathbb{N} \cup \{0\})$ tal que $r = |b| + s$, com $0 \leqslant s < r$. Notemos que $s \in S$ pois de $r = |b| + s \Leftrightarrow s = r - |b| \Leftrightarrow s = a - b \cdot q - |b| = a - (q \pm 1) \cdot b$ e por outro lado $s < r$ contradizendo o fato de r ser o menor elemento de S. Logo $r < |b|$.

Unicidade: Suponha que $a = b \cdot q + r = b \cdot q' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leqslant r < |b|$ e $0 \leqslant r' < |b|$. Assim $-|b| < -r \leqslant -r + r' \leqslant r' - r \leqslant r' < |b| \Leftrightarrow -|b| < r' - r < |b|$, e pela proposição 2.9 temos $|r - r'| < |b|$.

Por outro lado de $b \cdot q + r = b \cdot q' + r' \Leftrightarrow b \cdot (q - q') = r' - r$, o que implica que

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

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

□

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de a por b, e ainda, da divisão euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a.

Para exemplificar, ao efetuar a divisão euclidiana de 84 por 5 obtemos que $84 = 5 \cdot 16 + 4$ e ao efetuar a divisão euclidiana de -84 por 5 obtem-se $-84 = 5 \cdot (-17) + 1$.

Uma observação importante cabe neste momento, pelo teorema 2.11, se $a > 0$ é um inteiro, então os possíveis restos da divisão de um número qualquer por a são os números $0, 1, 2, ..., a - 1$. Assim sendo, para $a = 2$ e dado um número $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:

1. o resto da divisão de n por 2 é 0, isto é, $\exists\, q \in \mathbb{Z}$ tal que $n = 2 \cdot q$; ou

2. o resto da divisão de n por 2 é 1, ou seja, $\exists\, q \in \mathbb{Z}$ tal que $n = 2 \cdot q + 1$.

Portanto, pode-se afirmar que os números inteiros dividem-se em duas classes, a dos números da forma $2 \cdot q$, chamados de *números pares*, e a dos números da forma $2 \cdot q + 1$, chamados de números ímpares.

2.3 Representação posicional de números inteiros

De um modo universal os números inteiros positivos são representados através de um *sistema de numeração decimal e posicional*, fruto de um processo histórico que se desenvolveu através dos séculos.

O sistema de numeração é decimal quando a base de representação são potências do número 10, ou seja, quando os *algarismos* do número representam múltiplos de potências de 10, e a palavra posicional tem o sentido de dizer que a posição ocupada pelo algarismo no número, é um fator fundamental no valor absoluto que esse algarismo recebe.

Por exemplo, ao escrevermos o número 9973 em sua *expansão decimal* obtém-se que

$$9973 = 9 \cdot 1000 + 9 \cdot 100 + 7 \cdot 10 + 3 \cdot 1 = 9 \cdot 10^3 + 9 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0$$

e tem-se a ideia de que o algarismo 9 colocado mais à esquerda do número, tem o valor absoluto de 9000, enquanto que o 9 imediatamente a direita representa o valor de 900, ou seja, a posição ocupada pelo algarismo determina seu valor dentro do número representado. Sendo assim, enunciaremos o teorema principal dessa seção, enfatizando que uma demonstração desse teorema utilizando o método de *Indução Completa* pode ser encontrada em [2], enquanto que outra demonstração utilizando uma sequência finita de divisões euclidianas pode ser encontrada em [4].

Teorema 2.12. *Sejam dados os números inteiros* a *e* b*, com* $a > 0$ *e* $b > 1$*. Existem números inteiros* $n \geqslant 0$ *e* $0 \leqslant r_0, r_1, ..., r_n < b$*, com* $r_n \neq 0$*, univocamente determinados, tais que,* $a = r_n \cdot b^n + r_{n-1} \cdot b^{n-1} + ... + r_2 \cdot b^2 + r_1 \cdot b^1 + r_0$.

Para realizarmos a expansão de um inteiro a numa dada base b escolhe-se um conjunto S de b símbolos

$$S = \{s_0, s_1, ..., s_{b-1}\},$$

com $s_0 = 0$, para representar os números de 0 á $b - 1$.

Um número inteiro não negativo na base b escreve-se na forma $a_n a_{n-1} ... a_1 a_0$, com $a_n, a_{n-1}, ... a_1, a_0 \in S$, e n variando, dependendo de a. Portanto podemos escrever

$$a = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + ... + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0.$$

Por exemplo, para $b = 2$ temos

$$S = \{0, 1\}$$

e para $b = 10$ tem-se

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

Como habitualmente, será utilizada a notação $[a_n a_{n-1}...a_1 a_0]_b$ para simplificar que o número $a_n a_{n-1}...a_1 a_0$ está na base b. Assim

$$[a_n a_{n-1}...a_1 a_0]_b = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + ... + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0$$

Como é natural usarmos a base 10, iremos representar $[a_n a_{n-1}...a_1 a_0]_{10}$ simplesmente por $a_n a_{n-1}...a_1 a_0$, deixando a representação $[a_n a_{n-1}...a_1 a_0]_b$ apenas para os casos em que a base $b \neq 10$.

Para determinar a expansão de um número inteiro $a > 1$ na base b, devemos aplicar, sucessivamente, a divisão euclidiana de a por b como segue

$$a = b \cdot q_0 + r_0, \;\; r_0 < b,$$

$$q_0 = b \cdot q_1 + r_1, \;\; r_1 < b,$$

$$q_1 = b \cdot q_2 + r_2, \;\; r_2 < b,$$

e assim por diante. Como $a > q_0 > q_1 > ...$, deveremos, em um certo ponto, ter $q_{n-1} < b$ e, portanto, de

$$q_{n-1} = b \cdot q_n + r_n,$$

decorre que $q_n = 0$, o que implica que $0 = q_n = q_{n+1} = q_{n+2} = ...$, e, portanto, $0 = r_{n+1} = r_{n+2} = ...$

Temos, então, que

$$a = r_n \cdot b^n + r_{n-1} \cdot b^{n-1} + ... + r_1 \cdot b + r_0.$$

Para exemplificar o uso do algoritmo descrito acima, vamos escrever o número 2020 na base 2. Pela divisão euclidiana, tem-se

$$2020 = 2 \cdot 1010 + 0,$$

$$1010 = 2 \cdot 505 + 0,$$

$$505 = 2 \cdot 252 + 1,$$

$$252 = 2 \cdot 126 + 0,$$

$$126 = 2 \cdot 63 + 0,$$

$$63 = 2 \cdot 31 + 1,$$

$$31 = 2 \cdot 15 + 1,$$

$$15 = 2 \cdot 7 + 1,$$

$$7 = 2 \cdot 3 + 1,$$

$$3 = 2 \cdot 1 + 1,$$

$$1 = 2 \cdot 0 + 1.$$

Logo

$$2020 = 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0,$$

e, consequentemente, $2020 = [11111100100]_2$

2.4 Máximo divisor comum.

São dados dois números inteiros a e b, que podem ser iguais ou diferentes. Um número inteiro d é dito um *divisor comum* de a e b se $d \mid a$ e $d \mid b$.

Por exemplo, os números $\pm 1, \pm 2$ e ± 4 são os divisores comuns de 8 e 28.

Diz-se que um número inteiro $d \geqslant 0$ é um *máximo divisor comum* (mdc) de a e b, se possuir as seguintes propriedades:

1. d é um divisor comum de a e b, ou seja, $d \mid a$ e $d \mid b$.

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

Pelo exemplo acima, nota-se que o mdc de 8 e 28 é 4, pois $4 \mid 8$ e $4 \mid 28$, satisfazendo a propriedade (1), e ainda $\pm 1 \mid 4$, $\pm 2 \mid 4$ e $\pm 4 \mid 4$, satisfazendo assim a propriedade (2).

Assumiremos que sempre existe o mdc entre dois números inteiros a e b, um prova desse fato pode ser encontrada em [2], e o representaremos como (a, b). Novamente utilizando que o mdc de 8 e 28 é 4 a partir de agora isso será apresentado como $(8, 28) = 4$. Observa-se também, que dados $a, b \in \mathbb{Z}$, a existência de (a, b), nos permite ver que $(a, b) = (-a, b) = (a, -b) = (-a, -b)$, assim para o cálculo de (a, b) consideraremos sempre a e b não negativos. Por fim, notemos que (a, b) não depende da ordem em que a e b são tomados, assim $(a, b) = (b, a)$.

A proposição a seguir lista algumas propriedades interessantes do (a, b).

Proposição 2.13. *$\forall\, a, b \in \mathbb{Z}$ tem-se que:*

1. $(0, a) = |a|$;

2. $(1, a) = 1$;

3. $(a, a) = |a|$;

4. $(a, b) = 0 \Leftrightarrow a = b = 0$;

5. $a \mid b \Leftrightarrow (a, b) = |a|$.

Demonstração. (1.) Inicialmente $|a|$ é um divisor comum de 0 e $|a|$, pois $|a| \mid 0$ e $|a| \mid a$. Por outro lado sabe-se que $\forall\, c \in \mathbb{Z}$ temos que $c \mid 0$ e se c é um divisor comum de 0 e $|a|$ temos que $c \mid |a|$ e $c \leqslant |a|$. Logo $(0, a) = |a|$.

(2.) Pela proposição 2.7 tem-se $1 \mid a$ e $1 \mid 1$, logo 1 é um divisor comum de 1 e a. Como os únicos divisores de 1 são ± 1 e $\pm 1 \mid a$, segue que $(1, a) = 1$.

(3.) Primeiramente $|a| \mid a$. Por outro lado, se c é um divisor de a temos que $c \mid |a|$. Logo $(a, a) = |a|$.

(4.) Para começar se $(a, b) = 0$ então $0 \mid a$ e $0 \mid b$, porém o único número divisível por 0 é o próprio 0, logo $a = b = 0$. Reciprocamente, se $a = b = 0$ então $(a, b) = 0$, pois esse é um divisor comum de a e b e é o único número divisível por todos os divisores de 0.

(5.) Se $a \mid b$ então $|a| \mid b$ e como $|a| \mid a$ temos que $|a|$ é um divisor comum de a e b. Se c é um divisor comum de a e b, então c divide $|a|$, o que mostra que $|a| = (a, b)$. Reciprocamente, se $(a, b) = |a|$ segue que $|a| \mid b$, logo $a \mid b$. □

A existência do (a, b) nos permite apresentar um algoritmo capaz de calcular (a, b). O funcionamento desse algoritmo conhecido como *algoritmo de Euclides*, cuja demonstração pode ser encontrada em [2], pode ser sintetizado na prática como segue:

Sejam dois números inteiros $a \geqslant 1$ e $b \geqslant 1$ com $b \leqslant a$ e vamos supor que precisa-se calcular (a, b). Pela divisão euclidiana, temos que

$$a = b \cdot q_1 + r_1.$$

Se $r_1 = 0$ então $(a, b) = b$, caso contrário, novamente pela divisão euclidiana, fazemos

$$b = r_1 \cdot q_2 + r_2.$$

Se $r_2 = 0$ então $(a, b) = r_1$, caso contrário, prosseguindo enquanto for possível, teremos

$$r_1 = r_2 \cdot q_3 + r_3,$$

$$r_2 = r_3 \cdot q_4 + r_4,$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n,$$

$$r_{n-1} = r_n \cdot q_{n+1} + r_{n+1}.$$

Assim chegará um momento, que para algum n, teremos $r_n \mid r_{n-1}$ e com igual razão $r_{n+1} = 0$ logo conclui-se que $(a, b) = r_n$.

Um exemplo numérico, pode tornar as coisas mais claras, calculemos o $(1218, 648)$. Pela divisão euclidiana temos que

$$1218 = 648 \cdot 1 + 570,$$

$$648 = 570 \cdot 1 + 78,$$

$$570 = 78 \cdot 7 + 24,$$

$$78 = 24 \cdot 3 + 6,$$

$$24 = 6 \cdot 4.$$

O algoritmo também pode ser apresentado de outra maneira como $(1218, 648) = (648, 570) = (570, 78) = (78, 24) = (24, 6) = 6$.

Logo, $(1218, 648) = 6$.

Por curiosidade, de $(1218, 648) = 6$. temos então que $\frac{1218}{648} = \frac{203}{108}$, sendo esta última uma fração irredutível, e tal que $(203, 108) = 1$. Vejamos, usando o algoritmo de Euclides, se $(203, 108) = 1$. Da divisão euclidiana, vêm que

$$203 = 108 \cdot 1 + 95,$$

$$108 = 95 \cdot 1 + 13,$$

$$95 = 13 \cdot 7 + 4,$$

$$13 = 4 \cdot 3 + 1,$$

$$4 = 1 \cdot 4.$$

Analogamente, pode-se representar os cálculos acima como $(203, 108) = (108, 95) = (95, 13) = (13, 4) = (4, 1) = 1$.

Pelo algoritmo de Euclides, vemos que de fato, $(203, 108) = 1$. Quando o mdc de dois números inteiros for 1 diremos que os números em questão são *primos entre si*. Assim 203 e 108 são primos entre si.

Observe que, no exemplo acima, o algoritmo de Euclides fornece-nos:

$1 = 13 - 4 \cdot 3$

$4 = 95 - 13 \cdot 7$

$13 = 108 - 95 \cdot 1$

$95 = 203 - 108 \cdot 1$

Donde se segue que

$1 = 13 - 4 \cdot 3 = 13 - (95 - 13 \cdot 7) \cdot 3 = 13 - 95 \cdot 3 + 13 \cdot 21 = 13 \cdot 22 + 95 \cdot (-3) = (108 - 95 \cdot 1) \cdot 22 + 95 \cdot (-3) = 108 \cdot 22 + 95 \cdot (-22) + 95 \cdot (-3) = 108 \cdot 22 + 95 \cdot (-25) = 108 \cdot 22 + (203 - 108 \cdot 1) \cdot (-25) = 108 \cdot 22 + 203 \cdot (-25) + 108 \cdot 25 = -25 \cdot 203 + 47 \cdot 108,$

e portanto, $1 = -25 \cdot 203 + 47 \cdot 108$.

Note que conseguimos, através do uso do algoritmo de Euclides de trás para frente, escrever $1 = (203, 108)$ como um múltiplo de 203 mais um múltiplo de 108, e isso ocorre em geral. Vê-se que esse algoritmo também nos fornece um meio de escrever o mdc de dois números, como uma soma de múltiplos dos dois números em questão ou, caso prefira, uma combinação linear dos números dados.

2.4.1 Mínimo múltiplo comum

Dados dois números inteiros a e b, diz-se que um número inteiro é um *múltiplo comum* de a e b se ele for simultaneamente múltiplo de ambos os números. Em qualquer caso, os números $a \cdot b$ e 0 são sempre múltiplos comuns de a e b.

Por exemplo, temos que 24 é um múltiplo comum de 6 e 8, e que 36 é um múltiplo comum de 3 e 4. Analogamente, tem-se que 15 não é um múltiplo comum de 4 e 5, pois apesar de ser múltiplo de 5, não é múltiplo de 4, e pela definição há a necessidade de ser um múltiplo simultâneo de ambos os números.

Um número inteiro $m \geqslant 0$ será dito um *mínimo múltiplo comum (mmc)* dos inteiros a e b caso goze das seguintes propriedades:

1. m é um múltiplo comum de a e b, ou equivalentemente, $a \mid m$ e $b \mid m$.
2. se c é um múltiplo comum de a e b, então $m \mid c$.

No exemplo acima vimos que 24 é um múltiplo comum de 6 e 8, satisfazendo assim a propriedade (1.) da definição de mmc. O próximo múltiplo comum de 6 e 8 já é o número 48, e temos que $24 \mid 48$, o que mostra também a validade da propriedade (2.). Portanto 24 é o mmc de 6 e 8.

O mínimo múltiplo comum de dois inteiros a e b será denotado por $[a, b]$. É possível provar que, se existe o mínimo múltiplo comum de a e b, então ele é único. Prova-se também

que $[a, b] = [-a, b] = [a, -b] = [-a, -b]$, portanto, ao efetuar o cálculo do mmc entre dois números inteiros, podemos sempre considerá-los não negativos, e por fim, verifica-se que se $[a, b] = 0 \Leftrightarrow a = 0$ ou $b = 0$.

Uma forma de efetuar o cálculo do mmc de dois números inteiros, é pela fatoração desses números em potências de números primos (o teorema que descreve tal algoritmo estará colocado tão logo falemos sobre fatoração). Dados dois números inteiros a e b se tivermos $(a, b) = 1$ então $[a, b] = a \cdot b$. Caso seja $(a, b) \neq 1$, então fatoramos ambos os números. O mmc de a e b será o produto dos fatores primos (sendo p um primo, considera-se $p^0 = 1$), elevados ao seu maior expoente.

Verificamos anteriormente, pela definição, que $[6, 8] = 24$. Vejamos como ficaria o cálculo utilizando o algoritmo descrito acima. Inicialmente

$6 = 2 \cdot 3$ e $8 = 2^3$, portanto $[6, 8] = 2^3 \cdot 3 = 24$

Verifiquemos agora qual o $[48, 175]$. Temos

$48 = 2^4 \cdot 3$ e $175 = 5^2 \cdot 7$. Notemos que os fatores primos de 48 e 175 são diferentes, logo temos $(48, 175) = 1$ e com isso $[48, 175] = 48 \cdot 175 = 8400$.

Por fim, vejamos agora qual o $[56, 95]$. Temos

$56 = 2^3 \cdot 7$ e $95 = 5 \cdot 19$. Notemos que os fatores primos de 56 e 95 são diferentes, logo temos $(56, 95) = 1$ e com isso $[56, 95] = 56 \cdot 95 = 5320$

O método apresentado acima é apenas uma das formas de se realizar o cálculo do mmc de dois números inteiros. Uma maneira alternativa, pode ser vista na proposição a seguir, cuja demonstração pode ser apreciada em [2].

Proposição 2.14. *Dados dois números inteiros* a *e* b*, temos que* $[a, b]$ *existe e*

$$[a, b] = \frac{|a \cdot b|}{(a, b)}.$$

2.5 Números primos

Nessa seção falaremos de modo breve sobre números primos e compostos e algumas de suas propriedades. Será feita a opção de definir os números primos apenas para inteiros não negativos, porém nada impede que o conceito possa ser definido para todos os números inteiros.

Um número inteiro maior do que 1 e que só possui como divisores positivos 1 e ele próprio (divisores triviais) é chamado de *número primo*. Matematicamente, um inteiro $p > 1$ será primo se **apenas** $1 \mid p$ e $p \mid p$.

A condição de ser maior do que 1, se justifica, pelo fato de que 1 é o único inteiro positivo que possui apenas um divisor, a saber, o próprio 1. Por outro lado, todos os outros inteiros $n > 1$ tem no mínimo dois divisores, 1 e n.

Por exemplo, o inteiro positivo 2 é o primeiro número primo, pois apenas $1 \mid 2$ e $2 \mid 2$, e mais ainda, 2 é o único número primo par pois, qualquer outro número par $m = 2 \cdot q$ é divisível por 2, além de ser divisível por 1 e por si próprio (m), tendo então, no mínimo, três divisores, impossibilitando assim que seja primo.

Da definição de números primos, decorrem as seguintes propriedades elencadas na proposição abaixo:

Proposição 2.15. *Sejam* p, q *números primos e* $a, b \in \mathbb{Z}$*, tem-se:*

1. *Se* $p \mid q$*, então* $p = q$*;*
2. *Se* $p \nmid a$*, então* $(p, a) = 1$*;*
3. *Se* $p \mid a \cdot b$*, então* $p \mid a$ *ou* $p \mid b$*;*
4. *Se* $p, p_1, ..., p_n$ *são números primos e, se* $p \mid p_1 \cdot ... \cdot p_n$*, então* $p = p_i$ *para algum* $i = 1, ..., n$.

Demonstração. (1.) Como $p \mid q$, e sendo q primo, pela definição, temos que $p = 1$ ou $p = q$. Sendo p primo, novamente pela definição, tem-se que $p > 1$, eliminando portanto a opção $p = 1$ e restando somente que $p = q$.

(2.) Seja $(p, a) = d$, assim temos que $d \mid p$ e $d \mid a$. De $d \mid p$, tem-se que $d = 1$ ou $d = p$. Mas $d \neq p$, pois por hipótese, $p \nmid a$ e consequentemente, $d = 1$.

(3.) Mostremos que, se $p \mid a \cdot b$ e $p \nmid a$, então $p \mid b$.

Se $p \mid a \cdot b$, então $\exists\ e \in \mathbb{Z}$ tal que $a \cdot b = e \cdot p$.

Se $p \nmid a$ então $(a, p) = 1$, e utilizando o algoritmo de Euclides, encontramos $m, n \in \mathbb{Z}$ tais que

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

Pela comutatividade e multiplicando por b ambos os lados da igualdade acima temos que

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

Substituindo $a \cdot b$ por $e \cdot p$ nesta última igualdade, temos que

$$b = e \cdot p \cdot m + b \cdot n \cdot p = p \cdot (e \cdot m + b \cdot n)$$

e portanto, $p \mid b$.

(4.) Para uma demonstração dessa propriedade, utilizando Indução Finita, vide [2].

□

Para dar continuidade, um número inteiro maior do que 1 e que não é primo será dito *composto*. Portanto, se um inteiro $n > 1$ é composto, existirá um divisor positivo n_1 de n tal que $1 < n_1 < n$. Logo existirá um número natural n_2 tal que

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

Por exemplo, para os inteiros positivos menores ou iguais que 10 tem-se que os números $2, 3, 5$ e 7 são primos, enquanto que $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$ e $10 = 2 \cdot 5$ são compostos.

Uma proposição que se encontra na coleção *Os Elementos* de Euclides nos diz que *todo número natural* $n > 1$*, ou é primo, ou se escreve como produto de números primos*, fixando a importância dos números primos como blocos de construção de qualquer número natural. Uma analogia um tanto grosseira, nos diz que os números primos estão para os números naturais no mundo matemático, assim como os átomos estão para a matéria no mundo real.

Por exemplo, o número 19 é natural, e o que a proposição de Euclides nos diz é que só há duas opções para ele, ou ele é primo, ou então um produto de primos, e não é difícil constatar que 19 é primo. Por outro lado, o número 38 também é natural, e como não é primo (pois é par), a proposição nos diz que ele pode ser decomposto em um produto de fatores primos, e de fato, $38 = 2 \cdot 19$.

Ainda a respeito dessa proposição de Euclides, é possível provar que a escrita desse número natural é única a menos da ordem dos fatores. Com esta informação adicional, o resultado de Euclides pode ser reformulado no seguinte teorema, cuja demonstração pode ser encontrada em [4], [1] e [2].

Teorema 2.16. *(**Teorema Fundamental da Aritmética**): Dado um número inteiro* $n > 1$*, existem um número* $r > 0$*, números primos* $p_1 < ... < p_r$ *e* $\alpha_1, ..., \alpha_r \in \mathbb{N} \cup \{0\}$*, tais que*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r},$$

além disso, esta escrita é única.

Assim, dados $m, n \in \mathbb{Z}$ com $m > 1$ e $n > 1$ quaisquer, podemos escrever

$$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r} \text{ e } n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r},$$

usando o mesmo conjunto de primos $p_1, p_2, ..., p_r$.

Por exemplo, os números $8316 = 2^2 \cdot 3^3 \cdot 7 \cdot 11$ e $16250 = 2 \cdot 5^4 \cdot 13$ podem ser escritos, respectivamente, $8316 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7 \cdot 11 \cdot 13^0$ e $16250 = 2 \cdot 3^0 \cdot 5^4 \cdot 7^0 \cdot 11^0 \cdot 13$, com os mesmos primos $2, 3, 5, 7, 11$ e 13.

Apresentado o Teorema Fundamental da Aritmética, podemos enunciar o teorema que descreve um algoritmo para o cálculo do mdc e do mmc entre números inteiros.

Teorema 2.17. *Se* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$ *e* $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}$, *com* $\alpha_i, \beta_i \geqslant 0$ *e* $p_i \in \mathbb{P}$, *distintos, então*

1. $(a, b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot ... \cdot p_r^{\delta_r}$, *onde* $\delta_i = \min\{\alpha_i, \beta_i\}$.
2. $[a, b] = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot ... \cdot p_r^{\gamma_r}$, *onde* $\gamma_i = \max\{\alpha_i, \beta_i\}$.

Pondo fim a essa seção observa-se que após começar a estudar os números primos, e perceber as belíssimas propriedades dos mesmos, os matemáticos começaram a se perguntar se haveria um número infinito deles. Euclides desconfiava que essa afirmação era necessariamente verdadeira, porém sabia que mostrá-los todos era uma tarefa impossível. De posse de um axioma da Lógica, que esclarece que de uma afirmação verdadeira não se pode deduzir uma falsa, o astuto Euclides provou que existem infinitos primos sem precisar mostrar todos eles. Esse é o conteúdo do teorema a seguir:

Teorema 2.18. *Existe uma infinidade de números primos.*

Demonstração. Suponha que exista apenas uma quantidade finita de números primos $p_1, p_2, ..., p_r$. Obviamente, é natural o número $p_1 \cdot p_2 \cdot ... \cdot p_r$. Portanto pelos axiomas de Peano, existe e também é um número natural, o seu sucessor $p_1 \cdot p_2 \cdot ... \cdot p_r + 1$. Façamos

$$n = p_1 \cdot p_2 \cdot ... \cdot p_r + 1.$$

Temos que n é maior do que todos os $p_1, p_2, ..., p_r$. Assim, se n for primo, ele é um primo que está fora da lista finita que supomos. Logo nossa suposição inicial de que a lista $p_1, p_2, ..., p_r$ continha todos os primos não se sustenta.

Se n for composto, então algum dos $p_1, p_2, ..., p_r$ divide n. Suponhamos que, entre os $p_1, p_2, ..., p_r$, um p_o seja esse tal primo que divide n. Assim $p_o \mid (p_1 \cdot p_2 \cdot ... \cdot p_r + 1)$ e $p_o \mid p_1 \cdot p_2 \cdot ... \cdot p_r$. Logo, pela proposição 2.8, tem-se que $p_o \mid 1$. Como o único divisor positivo de 1 é o próprio 1, tem-se que $p_o = 1$. Porém $p_o = 1$ é um absurdo, pois p_o é primo e por definição $p_0 \neq 1$. Logo p_o é um primo que não está na lista finita que supomos, acarretando novamente que nossa lista finita de primos, não está completa.

□

Essencialmente, o que a demonstração acima nos diz é que em qualquer caso, ao supor que o conjunto dos números primos é finito, conseguimos encontrar um primo que lá não esteja. Por exemplo, vamos supor que o conjunto $\mathbb{P} = \{2, 3, 5, 7, 11, 13\}$ possui todos os números primos que existem. O número $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$ é um número natural, logo seu sucessor $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1 = 30031$ também o é. Tem-se o seguinte, se 30031 fosse primo (de fato não é), ele seria um primo não pertencente ao conjunto $\mathbb{P}$ e teríamos um novo primo. E caso contrário, se 30031 for composto, tem que existir um novo primo que o divide e que não está em $\mathbb{P}$. E é exatamente isso que ocorre, pois $30031 = 59 \cdot 509$, e curiosamente, encontramos não apenas um, mas dois novos primos que não estão em $\mathbb{P}$.

2.6 A aritmética dos restos

Nesta seção, apresentaremos uma das ideias mais interessantes da Teoria dos Números, introduzida pelo alemão Carl Friederich Gauss $(1777-1855)$ em seu famoso livro *Disquisitiones Arithmeticae*, de 1801. A importância dessa grande ideia se dá, pois através dela, Gauss desenvolveu uma aritmética dos restos da divisão por um número inteiro positivo fixado.

2.6.1 Congruências

Seja m um inteiro positivo. Diremos que dois números inteiros a e b são *congruentes módulo* m se a e b possuírem mesmo resto quando divididos por m. Quando os inteiros a e

Figura 2.4: Carl Friederich Gauss.

Fonte: [10].

b são congruentes módulo m, simbolizaremos esta situação como segue:

$$a \equiv b \mod m.$$

Quando a e b não são congruentes módulo m, escreve-se

$$a \not\equiv b \mod m.$$

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \mod 1$, quaisquer que sejam $a, b \in \mathbb{Z}$. Isso torna desinteressante a aritmética dos restos módulo 1. Portanto, consideraremos sempre $m > 1$.

Por exemplo:

- $16 \equiv 9 \mod 7$, pois os restos das divisões euclidianas de 16 e de 9 por 7 são os mesmos, a saber, tais restos são iguais a 2.
- $54 \equiv 19 \mod 5$, pois os restos das divisões euclidianas de 54 e de 19 por 5 são os mesmos, a saber, tais restos são iguais a 4.
- $31 \not\equiv 17 \mod 4$, pois o resto da divisão euclidiana de 31 por 4 é 3, enquanto o resto da divisão euclidiana de 17 por 4 é 1.

Para mostrar que $a \equiv b \bmod m$ não é necessário efetuar a divisão de a e de b por m para depois comparar os seus restos, é suficiente utilizar a proposição a seguir.

Proposição 2.19. *Sejam* $a, b, m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que* $a \equiv b \bmod m$ *se, e somente se,* $m \mid b - a$.

Demonstração. Pela divisão euclidiana, podemos escrever

$$a = m \cdot q_1 + r_1 \text{ e } b = m \cdot q_2 + r_2,$$

onde $0 \leqslant r_1 < m$ e $0 \leqslant r_2 < m$. Sem perda de generalidade, podemos supor $r_1 \leqslant r_2$, e subtraindo a de b tem-se que

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

Logo, $m \mid b - a$ se, e somente se, $m \mid r_2 - r_1$. Por ser $0 \leqslant r_2 - r_1 < m$, segue que $m \mid b - a$ se e somente se $r_2 - r_1 = 0$, ou seja, se e somente se $r_2 = r_1$. □

Para exemplificar vamos supor que quiséssemos verificar se $258 \equiv 1049 \bmod 35$. O que a proposição 2.19 nos diz é que não precisamos efetuar a divisão de 258 e de 1049 por 35 para ver se seus restos são iguais, basta verificarmos se $35 \mid (1049 - 258)$, ou equivalentemente, verificar se $35 \mid 791$. Pela divisão euclidiana temos que $791 = 35 \cdot 22 + 21$ e com isso constata-se que $35 \nmid 791$, logo $258 \not\equiv 1049 \bmod 35$

Note que todo número inteiro n é congruente módulo m ao seu resto pela divisão euclidiana por m, pois a divisão euclidiana de n por m nos dá que

$$n = m \cdot q + r \Rightarrow r - n = m \cdot (-q) \Rightarrow m \mid r - n \Rightarrow n \equiv r \bmod m,$$

com $q \in \mathbb{Z}$ e $0 \leqslant r < m$, e portanto, n é congruente módulo m a um dos números $0, 1, 2, ..., m - 1$. Além disso, dois desses números distintos não são congruentes módulo m. Portanto, para achar o resto da divisão de um número inteiro a por m, basta achar o número

natural r dentre os números $0, 1, 2, ..., m-1$ que seja congruente à a módulo m.

A proposição abaixo nos diz que a congruência módulo m é reflexiva, simétrica e transitiva.

Proposição 2.20. *Seja* $m \in \mathbb{N}$. *Para todos* $a, b, c \in \mathbb{Z}$, *tem-se que*

1. $a \equiv a \bmod m$.

2. *Se* $a \equiv b \bmod m$, *então* $b \equiv a \bmod m$.

3. *Se* $a \equiv b \bmod m$ *e* $b \equiv c \bmod m$, *então* $a \equiv c \bmod m$.

Demonstração. (1.) Se $a \equiv a \bmod m$ então pela proposição 2.19 temos que $m \mid a - a \Leftrightarrow m \mid 0$. E como $\forall\, m \in \mathbb{Z}$ tem-se $m \mid 0$, o resultado segue.

(2.) Se $a \equiv b \bmod m$ então pela proposição 2.19 temos que $m \mid b-a \Leftrightarrow b-a = m \cdot e$ com $e \in \mathbb{Z}$. De $b - a = m \cdot e \Leftrightarrow -b + a = m \cdot (-e) \Leftrightarrow a - b = m \cdot (-e) \Leftrightarrow m \mid a - b \Leftrightarrow b \equiv a \bmod m$.

(3.) Se $a \equiv b \bmod m$ então pela proposição 2.19 temos que $m \mid b-a \Leftrightarrow b-a = m \cdot d$ com $d \in \mathbb{Z}$. Por outro lado, se $b \equiv c \bmod m$ então novamente pela proposição 2.19 temos que $m \mid c - b \Leftrightarrow c - b = m \cdot e$ com $e \in \mathbb{Z}$. Assim

$$c - a = (c - b) + (b - a) = m \cdot e + m \cdot d = m \cdot (e + d) \Leftrightarrow m \mid c - a \Leftrightarrow a \equiv c \bmod m.$$

□

2.6.2 Congruências e somas

Uma grande e poderosa utilidade da noção de congruência é o fato de ser uma relação de equivalência compatível com a operação de adição. Isso quer dizer que as congruências de mesmo módulo somam-se e subtraem-se membro a membro tal qual as igualdades. Antes de

demonstrarmos esse importante fato sobre congruências e somas, precisamos de um resultado auxiliar da relação de divisibilidade.

Proposição 2.21. *Se* $a, b, c \in \mathbb{Z}$ *são tais que* $a \mid b$ *e* $a \mid c$*, então para todo* $x, y \in \mathbb{Z}$ *temos que* $a \mid (x \cdot b + y \cdot c)$.

Demonstração. $a \mid b$ e $a \mid c$ implicam que existem $f, g \in \mathbb{Z}$ tais que $b = f \cdot a$ e $c = g \cdot a$. Logo,

$$x \cdot b + y \cdot c = x \cdot (f \cdot a) + y \cdot (g \cdot a) = (x \cdot f + y \cdot g) \cdot a \Leftrightarrow a \mid (x \cdot b + y \cdot c).$$

□

Por exemplo, tomando na proposição 2.21, $a = 3, b = -93, c = 21$, $x = 8$ e $y = 12$ temos que $3 \mid -93$ já que $-93 = 3 \cdot (-31)$ e $3 \mid 21$ pois $21 = 3 \cdot 7$, logo devemos ter que $3 \mid (8 \cdot (-93) + 12 \cdot 21) \Leftrightarrow 3 \mid (-744 + 252) \Leftrightarrow 3 \mid -492$. O que de fato ocorre, visto que $-492 = 3 \cdot (-164)$.

Estamos agora em condições de provar a proposição a seguir:

Proposição 2.22. *Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 1$*. Tem-se que se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$*, então* $a + c \equiv b + d \bmod m$.

Demonstração. Como $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$. Logo, pela proposição 2.21, temos

$$m \mid (b - a) + (d - c) \Leftrightarrow m \mid (b + d) - (a + c) \Leftrightarrow a + c \equiv b + d \bmod m.$$

□

Por exemplo, sejam $a = 7, b = 22, c = 47, d = 62$ e $m = 5$ pela proposição 2.22 tem-se que como $7 \equiv 22 \bmod 5$ e $47 \equiv 62 \bmod 5$ então $7 + 47 \equiv 22 + 62 \bmod 5 \Leftrightarrow 54 \equiv 84 \bmod 5$.

A próxima proposição nos diz que, para as congruências, vale o cancelamento com relação a adição.

Proposição 2.23. *Sejam* $a, b, c, m \in \mathbb{Z}$*, com* $m > 1$*. Tem-se que*

$$a \equiv b \bmod m \Leftrightarrow a + c \equiv b + c \bmod m.$$

Demonstração. Se $a \equiv b \bmod m$ e como $c \equiv c \bmod m$, a proposição 2.22 nos dá que $a+c \equiv b+c \bmod m$. Reciprocamente, se $a+c \equiv b+c \bmod m$, então $m \mid b+c-(a+c) \Leftrightarrow m \mid b+c-a-c \Leftrightarrow m \mid b-a \Leftrightarrow a \equiv b \bmod m$. □

Por exemplo, na proposição 2.23 tomando $a = 19, b = 3, c = -4$, e $m = 8$ temos que de $19 \equiv 3 \bmod 8 \Leftrightarrow 15 \equiv 19 + (-4) \equiv 3 + (-4) \equiv -1 \bmod 8$.

2.6.3 Congruências e produtos

Analogamente ao analisado na seção anterior, a relação de congruência é compatível com a operação de multiplicação, nos dizendo que, tal qual as igualdades, as congruências de mesmo módulo multiplicam-se membro a membro. Tal propriedade é colocada no resultado abaixo:

Proposição 2.24. *Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 1$*. Tem-se que se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$*, então* $a \cdot c \equiv b \cdot d \bmod m$.

Demonstração. Como $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$, logo existem $e, f \in \mathbb{Z}$ tais que $b - a = m \cdot e$ e $d - c = m \cdot f$. Por outro lado, como

$$a \cdot c - b \cdot d = a \cdot (c - d) + d \cdot (a - b) = a \cdot (-f \cdot m) + d \cdot (-e \cdot m) = m \cdot (-f \cdot a - e \cdot d).$$

Logo, $m \mid a \cdot c - b \cdot d \Leftrightarrow a \cdot c \equiv b \cdot d \bmod m$. □

Por exemplo, tomando $a = -3, b = 1, c = 7, d = 11$ e $m = 4$ na proposição 2.24, e como $-3 \equiv 1 \bmod 4$ e $7 \equiv 11 \bmod 4$, então $-21 \equiv -3 \cdot 7 \equiv 1 \cdot 11 \equiv 11 \bmod 4$.

Faz-se necessário analisar alguns exemplos. Como $4 \cdot 9 - 4 \cdot 5 = 16$ e $8 \mid 16$, temos que $4 \cdot 9 \equiv 4 \cdot 5 \bmod 8$, e, no entanto, $9 \not\equiv 5 \bmod 8$. Por outro lado, $7 \cdot 13 - 7 \cdot 5 = 56$ e $8 \mid 56$, temos que $7 \cdot 13 \equiv 7 \cdot 5 \bmod 8$, e, $13 \equiv 5 \bmod 8$. No primeiro exemplo tínhamos que $(4, 8) = 4$ e a congruência não foi satisfeita, já no segundo exemplo $(7, 8) = 1$, e a última congruência foi satisfeita. Desconfiamos que os números analisados serem primos entre si, é um fator preponderante para aplicarmos o cancelamento multiplicativo. E isso, de fato é o que ocorre, como mostra o seguinte resultado.

Proposição 2.25. *Sejam* $a, b, c, m \in \mathbb{Z}$*, com* $m > 1$ *e* $(c, m) = 1$*. Temos que*

$$a \cdot c \equiv b \cdot c \Leftrightarrow a \equiv b \bmod m.$$

Demonstração. $a \cdot c \equiv b \cdot c \bmod m \Leftrightarrow m \mid b \cdot c - a \cdot c \Leftrightarrow m \mid c \cdot (b - a)$. Como, por hipótese, $(c, m) = 1$, temos que $m \mid b - a \Leftrightarrow a \equiv b \bmod m$. □

Por fim, repetidas aplicações da proposição 2.24 fornecem-nos o seguinte resultado:

Proposição 2.26. *Se* $a \equiv b \bmod m$*, então* $a^n \equiv b^n \bmod m$*, para todo* n *natural.*

Por exemplo, para $a = 8, b = -4, m = 6$ e $n = 3$ temos que $8 \equiv -4 \bmod 6$, logo pela proposição 2.26 devemos ter $8^3 \equiv (-4)^3 \bmod 6$, o que de fato ocorre, pois $8^3 \equiv 512 \equiv 2 \bmod 6$ e $(-4)^3 \equiv -64 \equiv 2 \bmod 6$.

2.7 Alguns testes de primalidade

Durante esta seção seremos familiarizados com a aplicabilidade de alguns algoritmos e testes de primalidade que utilizam da matemática apresentada nas seções anteriores. As

propriedades e relações mostradas anteriormente são válidas para todos os números inteiros. Apesar de aqui fazermos uso de tais propriedades, em sua maioria, trabalharemos com inteiros não negativos. O principal foco da seção é realmente mostrar como os testes funcionam na prática. Foca-se em exemplos numéricos que tentam responder ao problema de se determinar a primalidade de um inteiro positivo, de modo determinístico (com certeza absoluta) ou probabilístico (com uma probabilidade confiável).

2.7.1 O teste de divisibilidade

O teste de divisibilidade pode ser também enunciado como um algoritmo do tipo determinístico, isto é, este teste realmente determina com toda certeza se um determinado número inteiro não negativo n é composto ou primo. A eficiência desse teste pode ser verificada pela seguinte proposição:

Proposição 2.27. *Se um número inteiro $n > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leqslant n$.*

Demonstração. Sejam n um número composto e p o menor número primo do qual n é múltiplo, então $n = p \cdot b$, onde p e b são menores do que n. Temos dois casos a serem analisados:

1. b é primo. Se b é primo, e sendo p o menor número primo do qual n é múltiplo, temos que $p \leqslant b$, e multiplicando ambos os membros dessa desigualdade por $p > 1$ obtemos que $p^2 \leqslant p \cdot b = n$. Logo $p^2 \leqslant n$.

2. b é composto. Se b é composto então ele será múltiplo de um número primo q tal que $q < b$. Como n é múltiplo de b e b é múltiplo de q, pela relação de transitividade, temos que n é também múltiplo de q. Porém como p é o menor primo do qual n é múltiplo, temos que $p \leqslant q$, e multiplicando ambos os membros dessa desigualdade por $p > 1$ obtemos que $p^2 \leqslant p \cdot q < p \cdot b = n$. Logo $p^2 \leqslant n$.

□

Nota-se que, como todo número inteiro $n > 1$ é primo ou composto, a proposição 2.27 pode ser enunciada de maneira totalmente equivalente como "se um número inteiro $n > 1$ não é múltiplo de nenhum número primo p tal que $p^2 \leqslant n$, então ele é primo."

Suponhamos que fosse preciso descobrir se o número 161 é composto. Pela proposição 2.27 se 161 é composto então ele deve ser múltiplo de algum número primo p tal que $p^2 \leqslant 161$. Uma rápida olhada nos primeiros números primos nos permite verificar que $2^2 = 4$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$, $11^2 = 121$. O próximo primo a ser verificado é 13, porém $13^2 = 169$, e $169 > 161$. Portanto, se 161 for composto, então ele terá que ser múltiplo de algum (alguns) dos primos $2, 3, 5, 7$ ou 11. Pela divisão euclidiana temos

$$161 = 2 \cdot 80 + 1,$$

$$161 = 3 \cdot 53 + 2,$$

$$161 = 5 \cdot 32 + 1,$$

$$161 = 7 \cdot 23,$$

de maneira que 161 é múltiplo de 7 e portanto é um número composto. Percebe-se que nem precisamos testar o primo 11, pois um dos primos $2, 3, 5, 7$ ou 11, já é divisível por 161.

Agora um exemplo um pouco mais trabalhoso, suponha que fosse necessário descobrir se o número 1009 é primo. Ao utilizar a forma equivalente da proposição 2.27 temos que se 1009 não for múltiplo de nenhum número primo p tal que $p^2 \leqslant 1009$, então 1009 é primo. Novamente, uma rápida pesquisa no conjunto dos números primos nos permite verificar que $2^2 = 4$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$, $11^2 = 121$, $13^2 = 169$, $17^2 = 289$, $19^2 = 361$, $23^2 = 529$, $29^2 = 841$, $31^2 = 961$. O próximo primo a ser verificado é 37, porém $37^2 = 1369$, e $1369 > 1009$. Portanto, se 1009 não é múltiplo de nenhum dos primos $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$ ou 31, então 1009 é primo. De fato, pela divisão euclidiana temos

$$1009 = 2 \cdot 504 + 1,$$

$$1009 = 3 \cdot 336 + 1,$$

$$1009 = 5 \cdot 201 + 4,$$

$$1009 = 7 \cdot 144 + 7,$$

$$1009 = 11 \cdot 91 + 8,$$

$$1009 = 13 \cdot 77 + 8,$$

$$1009 = 17 \cdot 59 + 6,$$

$$1009 = 19 \cdot 53 + 2,$$

$$1009 = 23 \cdot 43 + 20,$$

$$1009 = 29 \cdot 34 + 23,$$

e

$$1009 = 31 \cdot 32 + 17.$$

Assim 1009 não é múltiplo de nenhum primo p tal que $p^2 \leqslant 1009$, logo 1009 é primo, e somente a título de curiosidade, é o menor número primo de quatro algarismos. O teste de divisibilidade pode ser enunciado como segue

(Teste de divisibilidade): Seja $n > 2$ um inteiro ímpar. Se ao dividir n por todos os primos p tais que $p^2 \leqslant n$ (obviamente pode-se parar assim que se encontra o primeiro p que divide n), tivermos que os $p_i \nmid n$, $\forall i$ com $i = 1, 2, ..., r$, então n é primo.

Pode-se perceber que apesar de ser um teste determinístico de primalidade, ele é pouco aplicável na determinação da primalidade de inteiros $n > 1$ suficientemente grandes. Isso se diz já que a medida que se precisa conhecer números primos cada vez maiores, é necessário uma lista que contenha suficientes números primos p tais que $p^2 \leqslant n$, para se testar se um deles é divísivel por n, o que já é um trabalho árduo. Mais ainda, mesmo depois de possuir tal lista, para verificar a primalidade desses enormes números , faz-se necessário efetuar muitas divisões euclidianas desses números por tais primos da lista.

A proposição 2.27 fundamenta um dos mais antigos métodos para se obter números primos, conhecido como o crivo de Eratóstenes [1].

Para minimizar o trabalho, os matemáticos passaram a estudar condições para que um determinado número natural n seja divisível por um número primo p. Em [12] podemos encontrar critérios de divisibilidade pelos números primos 2, 3, 5 e 7, além de um problema, com sugestão de solução, propondo o estudo de um critério de divisibilidade por 11. Daremos aqui, critérios de divisibilidade pelos números primos 13, 17 e 19, que podem ser verificados nas próximas três proposições.

Inicialmente recordemos que sendo m um número inteiro não negativo escrito na base decimal, então m pode ser representado como

$$m = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdot ... \cdot + a_1 \cdot 10 + a_0 = 10q + a_0,$$

onde a_0 é o algarismo das unidades, $q = a_n a_{n-1} ... a_1$ e os $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ com $0 \leqslant i \leqslant n$, representam os algarismos do número m. Pode-se então escrever m, em função de seus algarismos, na forma $m = a_n a_{n-1} ... a_1 a_0$.

Proposição 2.28. ***(Divisibilidade por 13)*** *Seja* $n = a_n a_{n-1} ... a_1 a_0$ *um número inteiro, então*

$$13 \mid n \Leftrightarrow 13 \mid a_n ... a_1 + 4 \cdot a_0.$$

Demonstração. Mostremos que $13 \mid (10q + a_0) \Leftrightarrow 13 \mid (q + 4 \cdot a_0)$. Com efeito,

De $13 \mid (10q + a_0) \Rightarrow 10q + a_0 = 13l \Rightarrow a_0 = 13l - 10q$. Assim, $q + 4 \cdot a_0 = q + 4 \cdot (13l - 10q) = q + 52l - 40q = 52l - 39q = 13 \cdot (4l - 3q) = 13l' \Rightarrow 13 \mid (q + 4 \cdot a_0)$, onde $l, l' \in \mathbb{Z}$.

Reciprocamente, se $13 \mid (q + 4 \cdot a_0) \Rightarrow q + 4 \cdot a_0 = 13k \Rightarrow q = 13k - 4 \cdot a_0$. Assim $10q + a_0 = 10 \cdot (13k - 4 \cdot a_0) + a_0 \Rightarrow 10q + a_0 = 130k - 40 \cdot a_0 + a_0 = 130k - 39 \cdot a_0 = 13 \cdot (10k - 3 \cdot a_0) = 13k' \Rightarrow 13 \mid (10q + a_0)$, onde $k, k' \in \mathbb{Z}$. □

Proposição 2.29. ***(Divisibilidade por 17)*** *Seja* $n = a_n a_{n-1}...a_1 a_0$ *um número inteiro, então*

$$17 \mid n \Leftrightarrow 17 \mid a_n...a_1 - 5 \cdot a_0.$$

Demonstração. Mostremos que $17 \mid (10q + a_0) \Leftrightarrow 17 \mid (q - 5 \cdot a_0)$. Com efeito,

De $17 \mid (10q + a_0) \Rightarrow 10q + a_0 = 17l \Rightarrow a_0 = 17l - 10q$. Assim, $q - 5 \cdot a_0 = q - 5 \cdot (17l - 10q) = q - 85l + 50q = -85l + 51q = 17 \cdot (-5l + 3q) = 17l' \Rightarrow 17 \mid (q - 5 \cdot a_0)$, onde $l, l' \in \mathbb{Z}$.

Reciprocamente, se $17 \mid (q - 5 \cdot a_0) \Rightarrow q - 5 \cdot a_0 = 17k \Rightarrow q = 17k + 5 \cdot a_0$. Portanto, $10q + a_0 = 10 \cdot (17k + 5 \cdot a_0) + a_0 \Rightarrow 10q + a_0 = 170k + 50 \cdot a_0 + a_0 = 170k + 51 \cdot a_0 = 17 \cdot (10k + 3 \cdot a_0) = 17k' \Rightarrow 17 \mid (10q + a_0)$, onde $k, k' \in \mathbb{Z}$. □

Proposição 2.30. ***(Divisibilidade por 19)*** *Seja* $n = a_n a_{n-1}...a_1 a_0$ *um número inteiro, então*

$$19 \mid n \Leftrightarrow 19 \mid a_n...a_1 + 2 \cdot a_0.$$

Demonstração. Mostremos que $19 \mid (10q + a_0) \Leftrightarrow 19 \mid (q + 2 \cdot a_0)$. Com efeito,

De $19 \mid (10q + a_0) \Rightarrow 10q + a_0 = 19l \Rightarrow a_0 = 19l - 10q$. Logo, $q + 2 \cdot a_0 = q + 2 \cdot (19l - 10q) = q + 38l - 20q = 38l - 19q = 19 \cdot (2 - q) = 19l' \Rightarrow 19 \mid (q + 2 \cdot a_0)$, onde $l, l' \in \mathbb{Z}$.

Reciprocamente, se $19 \mid (q + 2 \cdot a_0) \Rightarrow q + 2 \cdot a_0 = 19k \Rightarrow q = 19k - 2 \cdot a_0$, Assim, $10q + a_0 = 10 \cdot (19k - 2 \cdot a_0) + a_0 \Rightarrow 10q + a_0 = 190k - 20 \cdot a_0 + a_0 = 190k - 19 \cdot a_0 = 19 \cdot (10k - a_0) = 19k' \Rightarrow 19 \mid (10q + a_0)$, onde $k, k' \in \mathbb{Z}$. □

Para exemplificar o uso desses critérios, faremos um exemplo numérico de aplicação do critério de divisibilidade por 13 apresentado, os outros exemplos envolvendo as outras

proposições podem ser tratados de maneira análoga. Suponha que tivéssemos que saber se $13 \mid 7241$ sem efetuar diretamente a divisão euclidiana, então pela proposição 2.28 pode-se proceder da seguinte forma

$$13 \mid 7241 \Leftrightarrow 13 \mid (724 + 4 \cdot 1) \Leftrightarrow 13 \mid 728 \Leftrightarrow 13 \mid (72 + 4 \cdot 8) \Leftrightarrow 13 \mid 104$$

$$\Leftrightarrow 13 \mid (10 + 4 \cdot 4) \Leftrightarrow 13 \mid 26.$$

Assim, $13 \mid 7241 \Leftrightarrow 13 \mid 26$, e como $26 = 2 \cdot 13$ e $2 \in \mathbb{Z}$, o resultado segue.

O último resultado dessa seção é um *critério de divisibilidade por 7*. Foi dado destaque especial a esse critério, pois o mesmo foi redescoberto no final de 2019, de maneira totalmente independente, por um garoto nigeriano de 12 anos, cujo nome é Chika Ofili, enquanto este realizava seus estudos em casa. Tomaremos a liberdade de, apresentar e demonstrar esse resultado, na forma de uma proposição, designada por Teste de Chika, sendo esta uma maneira que encontramos de homenagear e prestigiar a redescoberta deste curioso jovem.

Proposição 2.31. ***(Teste de Chika)*** *Seja* $n = a_n a_{n-1} ... a_1 a_0$ *um número inteiro, então*

$$7 \mid n \Leftrightarrow 7 \mid a_n ... a_1 + 5 \cdot a_0.$$

Demonstração. Mostremos que $7 \mid (10q + a_0) \Leftrightarrow 7 \mid (q + 5 \cdot a_0)$. Com efeito,

De $7 \mid (10q + a_0) \Rightarrow 10q + a_0 = 7l \Rightarrow a_0 = 7l - 10q$. Logo, $q + 5 \cdot a_0 = q + 5 \cdot (7l - 10q) = q + 35l - 50q = 35l - 49q = 7 \cdot (5l - 7q) = 7l' \Rightarrow 7 \mid (q + 5 \cdot a_0)$, onde $l, l' \in \mathbb{Z}$.

Reciprocamente, se $7 \mid (q + 5 \cdot a_0) \Rightarrow q + 5 \cdot a_0 = 7k \Rightarrow q = 7k - 5 \cdot a_0$, Assim, $10q + a_0 = 10 \cdot (7k - 5 \cdot a_0) + a_0 = 70k - 50 \cdot a_0 + a_0 = 70k - 49 \cdot a_0 = 7 \cdot (10k - 7 \cdot a_0) = 7k' \Rightarrow 7 \mid (10q + a_0)$, onde $k, k' \in \mathbb{Z}$. □

Por exemplo, se quisermos verificar se $7 \mid 2996$ podemos proceder da seguinte maneira:

$7 \mid 2996 \Leftrightarrow 7 \mid (299 + 5 \cdot 6) \Leftrightarrow 7 \mid (299 + 30) \Leftrightarrow 7 \mid 329 \Leftrightarrow 7 \mid (32 + 5 \cdot 9)$ $\Leftrightarrow 7 \mid (32 + 45) \Leftrightarrow 7 \mid 77$. Logo, $7 \mid 2996 \Leftrightarrow 7 \mid 77$, o que de fato se verifica pois, $77 = 7 \cdot 11$ e $11 \in \mathbb{Z}$.

2.7.2 O teste de composição de Fermat

Durante essa seção será apresentado um teste de composição probabilístico, porém com alta probabilidade de determinar a composição de um determinado número inteiro $n > 1$.

De acordo com [11] Pierre de Fermat nasceu em 20 de Agosto de 1601, na cidade de Beaumont-de Lomagne, no sudoeste da França. Sendo filho de um rico mercador de peles, Fermat teve a sorte de receber uma educação privilegiada em um monastério franciscano, seguido por uma passagem pela Universidade de Toulouse. Fermat foi um servidor público dedicado e compassivo, e por vezes, no uso de suas atribuições prestava serviços como juiz à corte francesa. Seus interesses em matemática estavam ligados à geometria analítica, ao cálculo diferencial e claro, à teoria dos números.

Figura 2.5: Pierre de Fermat.

Fonte: [10].

O sucesso do teste de composição de Fermat se baseia no seguinte teorema, conhecido na literatura como *o pequeno teorema de Fermat*.

Teorema 2.32. ***(O pequeno teorema de Fermat)*** *Se p é um número primo e a é um natural que não é divisível por p, então*

$$a^{p-1} \equiv 1 \bmod p$$

Belíssimas demonstrações deste teorema, entre elas a demonstração de Euler, que faz uso do método de indução finita (que não será discutido no texto) e da divisibilidade de coeficientes binomais, podem ser encontradas em [9], [12] e [2].

Foquemos agora em exemplos numéricos de aplicações do teorema 2.32. Inicialmente, sabendo que 17 é um número primo (pois pelo teste de divisibilidade é suficiente testar que ele não é divisível por 2 e nem por 3) e durante boa parte dos exemplos que faremos no texto tomaremos $a = 2$, que sabemos ser o único número primo par, pois $\forall\, p > 2$ primo temos $(2, p) = 1$, satisfazendo assim a condição do a escolhido não ser divisível por p. Assim $(2, 17) = 1$ e portanto pelo teorema de Fermat devemos ter $2^{17-1} \equiv 1 \bmod 17$.

De fato:

$$2^{17-1} = 2^{16} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2 \equiv (-2) \cdot (-2) \cdot (-2) \cdot 2 = -16 \equiv 1 \bmod 17.$$

Agora um segundo exemplo, na seção anterior provamos pelo teste da divisibilidade que 1009 é curiosamente o menor número primo de quatro algarismos, assim, tomando $a = 2$, temos que $(2, 1009) = 1$, portanto pelo pequeno teorema de Fermat devemos ter $2^{1009-1} \equiv 1 \bmod 1009$.

De fato:

$$2^{1009-1} = 2^{1008} = (2^{10})^{100} \cdot 2^8 \equiv 15^{100} \cdot 256 = (15^6)^{16} \cdot 15^4 \cdot 256 \equiv 24^{16} \cdot 50625 \cdot 256$$

$$= 24^9 \cdot 24^7 \cdot 12960000 \equiv 74 \cdot 375 \cdot 12960000 \equiv 1 \bmod 1009.$$

Obviamente ao escolher um número natural n composto, por exemplo, $n = 21$ e tomando $a = 4$, temos que

$$4^{21-1} = 4^{20} = (4^3)^6 \cdot 4^2 \equiv 1^6 \cdot 16 = 1 \cdot 16 = 16 \not\equiv 1 \bmod 21.$$

Uma pergunta interessante a ser feita neste momento, e que seria de extrema relevância é se é válida a recíproca do teorema 2.32, ou seja, dado um número natural $n > 1$ com $(a, n) = 1$ e tal que $\forall\, a \in \mathbb{Z}$ temos $a^{n-1} \equiv 1 \bmod n$, podemos afirmar que n é primo? Uma resposta positiva, seria fantástica pois forneceria mais uma forma de caracterizar os números primos.

Infelizmente, a recíproca do teorema 2.32 não é válida, como mostra o contraexemplo a seguir: Seja n um número composto tal que $n = 341 = 11 \cdot 31$ e $a = 2$ temos

$$2^{341-1} = 2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \bmod 341.$$

Concluímos portanto que ser primo é uma condição suficiente para que a congruência do teorema 2.32 seja satisfeita, porém não é necessário que isso ocorra, pois existem números compostos que satisfazem tal congruência. Números naturais compostos que possuem tal propriedade são conhecidos como números *pseudoprimos* (primos falsos) e como o número a escolhido foi 2, podemos afirmar que 341 é um pseudoprimo na base 2.

Em [9] os pseudoprimos são estudados detalhadamente, inclusive são apresentados números que são pseudoprimos em qualquer base $a > 1$ escolhida. Uma das propriedades apresentadas no texto referenciado é a de que os pseudoprimos na base 2 são infinitos, e apesar desse fato, isso ainda nos diz que o teste de composição de Fermat é bem eficiente, mesmo que existam infinitos pseudoprimos, eles são raros.

Após uma rápida pesquisa em [8] encontramos, por exemplo que a quantidade de números primos existentes até 10^5 é de 9592 e até 10^6 é de 78498. Ao utilizar um programa de computador baseado no teorema 2.32 para a base $a = 2$ (algumas tabelas, contendo

todos os números pseudoprimos na base 2 menores que 10^6 (um milhão) com suas respectivas fatorações encontram-se nos apêndices), encontramos que o número de pseudoprimos até 10^5 é de 78 e até 10^6 é de 245. Sendo assim, a probabilidade de um número n ser primo, dado que ele passa no teste de Fermat para a base $a = 2$ (ou seja $2^{n-1} \equiv 1 \bmod n$) pode ser calculada, para estes dois exemplos citados, respectivamente pelas razões

1. $\dfrac{9592}{(9592+78)} = \dfrac{9592}{9670} \approx 0,9919 \approx 99,19\%,$
2. $\dfrac{78498}{(78498+245)} = \dfrac{78498}{78743} \approx 0,9969 \approx 99,69\%,$

assim conforme [12] o teste de composição de Fermat pode ser enunciado da seguinte forma:

(Teste de Composição de Fermat): Seja $n > 1$ um natural ímpar e seja a um natural que não é divisível por n. Se

- $a^{n-1} \not\equiv 1 \bmod n$ então n é composto;
- $a^{n-1} \equiv 1 \bmod n$ então o teste é inconclusivo.

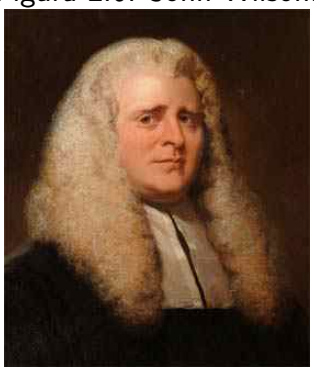
2.7.3 O teste de Wilson

Durante esta seção apresentaremos e demonstraremos o teorema de Wilson, que nos dá como consequência um teste de primalidade do tipo determinístico, pouco aplicável para primos gigantes. John Wilson foi um matemático do século XVIII nascido em 6 de Agosto de 1741 em Applethwaite, Inglaterra. Antes de provarmos o seu grandioso teorema, precisamos de outros dois resultados.

Proposição 2.33. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \bmod m$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{N}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0 \bmod m$.*

Uma demonstração dessa proposição pode ser encontrada em [2].

Figura 2.6: John Wilson.



Fonte: [10].

Exemplifiquemos o uso da proposição 2.33 na forma de um problema como segue.

Inicialmente temos claramente que $18 \equiv 3 \bmod 5$, e suponha que quiséssemos saber se existe algum número natural x que multiplicado por 18 deixa resto 1 quando dividido por 5, ou equivalentemente, se $\exists x \in \mathbb{N}$ tal que $18 \cdot x \equiv 1 \bmod 5$. A proposição 2.33 nos diz que isso é possível, pois $(18, 5) = 1$ e de fato isso ocorre, pois tomando $x = 2$ temos que

$$18 \equiv 3 \bmod 5 \Leftrightarrow 18 \cdot 2 \equiv 3 \cdot 2 \bmod 5 \Leftrightarrow 36 \equiv 6 \equiv 1 \bmod 5.$$

A proposição 2.33 ainda nos diz que se $x = 2$ é uma solução, então qualquer outra solução x_i é tal que $x_i \equiv 2 \bmod 5$, ou seja, poderíamos ter tomado qualquer outro natural que deixa resto 2 na divisão por 5, como por exemplo 7, 12, 17, 22 e etc.

O próximo resultado que será utilizado na demonstração do teorema de Wilson, que também pode ser vista em [2], segue a seguir.

Proposição 2.34. *Se $n > 4$ é um número inteiro, então n é composto se, e somente se, $n \mid (n-2)!$.*

Demonstração. Supondo n composto, inicialmente provaremos que $n \mid (n-1)!$.

De fato, sendo n composto pode-se escrever $n = n_1 n_2$ com $1 < n_1, n_2 < n$. Temos dois casos a serem analisados:

1. $n_1 \neq n_2$.

   Se $n_1 \neq n_2$ podemos supor que $1 < n_1 < n_2$.

   Portanto,

   $$(n-1)! = 1 \cdot ... \cdot n_1 \cdot ... \cdot n_2 \cdot ... \cdot (n-1)$$

   E após uma reordenação dos fatores de $(n-1)!$ temos,

   $$(n-1)! = 1 \cdot ... \cdot n_1 \cdot n_2 \cdot ... \cdot ... \cdot ... \cdot (n-1) = 1 \cdot ... \cdot n ... \cdot ... \cdot ... \cdot (n-1),$$

   o que mostra que $n \mid (n-1)!$, no primeiro caso.

2. $n_1 = n_2$ e $n_1, n_2 > 2$.

   Logo,

   $$(n-1)! = 1 \cdot ... \cdot n_1 \cdot ... \cdot 2n_1 \cdot ... \cdot (n-1)$$

   E após uma reordenação dos fatores de $(n-1)!$ temos,

   $$(n-1)! = 1 \cdot ... \cdot 2n_1 \cdot n_1 \cdot ... \cdot ... \cdot ... \cdot (n-1) = 1 \cdot ... \cdot 2n_1 \cdot n_2 \cdot ... \cdot ... \cdot ... \cdot (n-1)$$

   $$= 1 \cdot ... \cdot 2n \cdot ... \cdot ... \cdot ... \cdot (n-1),$$

   o que mostra que $n \mid (n-1)!$, também no segundo caso.

Agora, de $n \mid (n-1)! \Leftrightarrow n \mid (n-1) \cdot (n-2)!$ e como $(n, n-1) = 1$ devemos ter $n \mid (n-2)!$.

Reciprocamente, se $n \mid (n-2)!$, n não pode ser primo, pois é maior do que os fatores primos de $(n-1)!$. □

Para exemplificar a proposição 2.34 e escolhendo o número composto $n = 6$ devemos ter $6 \mid (6-2)! \Leftrightarrow 6 \mid 4! \Leftrightarrow 6 \mid 24$, o que é verdade pois $24 = 6 \cdot 4$ e $4 \in \mathbb{Z}$.

Estamos agora em condições de enunciar e demonstrar o teorema que embasa o teste de primalidade dessa seção, baseada na demonstração apresentada em [2].

Teorema 2.35. ***(Wilson)*** *Seja* $p \in \mathbb{N}$. *Tem-se* p *um número primo se, e somente se,*

$$(p-1)! \equiv -1 \bmod p.$$

Demonstração. Inicialmente para os números primos $p = 2$ temos que $(2-1)! \equiv 1! \equiv 1 \equiv -1 \bmod 2$ e para $p = 3$ temos $(3-1)! \equiv 2! \equiv 2 \equiv -1 \bmod 3$. Iremos supor $p \geqslant 5$.

Sendo assim $\forall\, i \in \{1, ..., (p-1)\}$ pela proposição 2.33, a congruência $i \cdot X \equiv 1 \bmod p$ possui uma única solução módulo p; ou seja, dado $i \in \{1, ..., (p-1)\}$ $\exists!\, j \in \{1, ..., (p-1)\}$ tal que $i \cdot j \equiv 1 \bmod p$. Por outro lado, se $i \in \{1, ..., (p-1)\}$ é tal que $i^2 \equiv 1 \bmod p$, então $p \mid i^2 - 1 \Leftrightarrow p \mid (i-1) \cdot (i+1) \Leftrightarrow p \mid (i-1)$ ou $p \mid (i+1)$, o que só pode ocorrer se $i = 1$ ou $i = p-1$.

Logo,

$$2 \cdot ... \cdot (p-2) \equiv 1 \bmod p,$$

e portanto,

$$(p-1)! \equiv 1 \cdot 2 \cdot ... \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv (p-1) \equiv -1 \bmod p.$$

Reciprocamente, vimos que para os primos $p = 2$ e $p = 3$ temos válida a congruência $(2-1)! \equiv -1 \bmod 2$ e $(3-1)! \equiv -1 \bmod$ enquanto que para o composto $n = 4$ temos $(4-1)! \equiv 3! \equiv 6 \equiv 2 \bmod 4$.

Supondo $n > 4$ e composto, temos pela proposição 2.34 que $n \mid (n-1)!$ e, portanto, $n \nmid (n-1)!+1$, já que $((n+1)!, (n+1)!+1) = 1$, o que mostra que $(n-1)! \not\equiv -1 \bmod n$. □

Conclui-se portanto que o teste de primalidade de Wilson pode ser enunciado como segue:

(Teste de Wilson): Seja $n \geqslant 2$ um número inteiro. Se $(n-1)! \equiv -1 \bmod n$ então n é primo.

Vejamos duas aplicações do teste para os números $n = 67$ e $n = 83$.

$$(67-1)! = 66! = \underbrace{544344...000000}_{93\,algarismos} \equiv 66 \equiv -1 \bmod 67.$$

Logo 67 é um número primo. Analogamente,

$$(83-1)! = 82! = \underbrace{475364...000000}_{123\,algarismos} \equiv 82 \equiv -1 \bmod 83.$$

E com igual razão, temos que 83 é um número primo.

Obviamente os cálculos envolvendo os fatoriais acima, foram feitos de modo instantâneo com o auxílio de um computador comum, porém mesmo usando tal ferramenta, o cálculo de um fatorial da ordem de 10^6 já é uma tarefa pouco viável. Devido a isso, o teste de Wilson não pode ser considerado aplicável para a verificação da primalidade de números suficientemente grandes, mas a beleza e simplicidade do teorema que é base para o teste que leva seu nome, é algo que fascina e muito os interessados no estudo dos números primos.

Um teorema em teoria dos números conhecido como *Propriedade de Wolstenholme* afirma que, se $n \geq 5$ é número primo, então

$$\binom{2n-1}{n-1} \equiv 1 \bmod n^3.$$

O teorema de Wilson, que nos fornece uma caracterização para os números primos, pode ser utilizado para provar um corolário do teorema de Wolstenholme. Este exemplo de aplicação de tal teorema, pode ser apreciado no resultado a seguir, que humildemente e com uma dose de bom humor, tomaremos a liberdade de apresentar como:

Corolário 2.36. *Pequena Propriedade de Queiroz: Se n é um número primo então*

$$\binom{2n-1}{n-1} \equiv 1 \bmod n$$

.

Demonstração.

$$\binom{2n-1}{n-1} = \frac{(2n-1)!}{(n-1)! \cdot n!} = \frac{(n+(n-1))!}{(n-1)! \cdot n!}.$$

Pelo Teorema de Wilson, se n é primo então $(n-1)! \equiv -1 \bmod n$. Logo

$$\frac{(n+(n-1))!}{(n-1)! \cdot n!} \equiv \frac{(n+(n-1))!}{-1 \cdot n!} = \frac{1 \cdot 2 \cdot 3 \cdot ... \cdot n \cdot (n+1) \cdot (n+2) \cdot ... \cdot (n+(n-1))}{-1 \cdot n!}$$

$$= \frac{n! \cdot (n+1) \cdot (n+2) \cdot ... \cdot (n+(n-1))}{-1 \cdot n!} = -((n+1) \cdot (n+2) \cdot ... \cdot (n+(n-1))$$

$$\equiv -(1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1)) = -(n-1)! \equiv -(-1) = 1 \bmod n.$$

□

Por exemplo, se tomarmos $n = 11$ e $n = 13$ temos, respectivamente, que

$$\binom{2 \cdot 11 - 1}{11 - 1} = \binom{21}{10} = \frac{21!}{10! \cdot (21-10)!} = \frac{21!}{10! \cdot 11!} = 352716 \equiv 1 \bmod 11, \text{ e}$$

$$\binom{2 \cdot 13 - 1}{13 - 1} = \binom{25}{12} = \frac{25!}{12! \cdot (25-12)!} = \frac{25!}{12! \cdot 13!} = 5200300 \equiv 1 \bmod 13.$$

Analogamente, se tomarmos $n = 23$ tem-se

$$\binom{2 \cdot 23 - 1}{23 - 1} = \binom{45}{22} = \frac{45!}{22! \cdot (45-22)!} = \frac{45!}{22! \cdot 23!} = 4116715363800 \equiv 1 \bmod 23.$$

A propriedade acima mencionada, a qual todos os números primos possuem, aumenta a nossa esperança de encontrarmos uma caracterização para esses números. Será que essa propriedade é exclusiva dos números primos? Ou seja, será que algum número composto possui tal propriedade? Podemos analisar a validade da recíproca dessa propriedade, nos perguntando se $\binom{2n-1}{n-1} \equiv 1 \bmod n$ implica em n primo.

Note que, tomando os números compostos $n = 4$ e $n = 6$ tem-se, respectivamente, que

$$\binom{2\cdot 4-1}{4-1} = \binom{7}{3} = \frac{7!}{3!\cdot(7-3)!} = \frac{7!}{3!\cdot 4!} = 35 \equiv 3 \not\equiv 1 \bmod 4, \text{ e}$$

$$\binom{2\cdot 6-1}{6-1} = \binom{11}{5} = \frac{11!}{5!\cdot(11-5)!} = \frac{11!}{5!\cdot 6!} = 462 \equiv 0 \not\equiv 1 \bmod 6.$$

Porém, ao escolher o número composto $n = 9$ tem-se

$$\binom{2\cdot 9-1}{9-1} = \binom{17}{8} = \frac{17!}{8!\cdot(17-8)!} = \frac{17!}{8!\cdot 9!} = 24310 \equiv 1 \bmod 9.$$

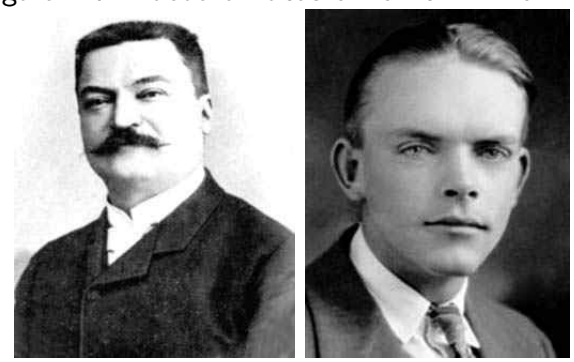
E mais uma vez, análogo ao Pequeno Teorema de Fermat, os números primos foram astutos em não nos revelar os seus segredos.

2.7.4 O teste Lucas-Lehmer

Durante essa seção seremos apresentados a um teste de primalidade muito curioso, que é do tipo determinístico. Todavia ele não testa a primalidade para qualquer número inteiro $n > 1$. o teste Lucas-Lehmer testa a primalidade de números inteiros com uma forma bem peculiar. São inteiros que podem ser escritos, como uma potência n-ésima de 2 subtraída de 1. Conhecidos como *números de Mersenne*, trataremos de analisá-los com bastante apreço no decorrer do texto.

O teste carrega o nome de dois grandes matemáticos. O primeiro deles, Édouard Lucas, nasceu no dia 4 de Abril de 1842, na cidade de Amiens, situada no norte da França. Lucas dedicou sua vida ao estudo da teoria dos números, campo onde fez inúmeras contribuições relevantes. Criou e divulgou mundo afora, um jogo bastante popular, conhecido como a Torre de Hanói (para maiores informações sobre este jogo ver [2]). A segunda personalidade que cravou seu nome no teste foi Derrick Henry Lehmer, um matemático californiano, nascido em 23 de Fevereiro de 1905, em Berkeley, nos Estados Unidos. Aliás vale ressaltar que, a versão do teste que aqui é apresentado, discutido e aplicado, é um aprimoramento de Lehmer para um outro teste de Lucas.

Figura 2.7: Édouard Lucas e Derrick H. Lehmer.



Fonte: [10].

Como dito anteriormente, o teste Lucas-Lehmer é indicado para testar a primalidade dos números de Mersenne, sendo assim faz-se necessário conhecê-los.

Primeiramente Marin Mersenne, foi um padre apaixonado por matemática nascido no dia 8 de Setembro de 1588, na comunidade francesa de Oizé. Mersenne sabia como poucos dividir habilmente seu tempo com as obrigações do exercício do sacerdócio e suas atividades matemáticas.

Figura 2.8: Marin Mersenne.

Fonte: [10].

Os matemáticos já vinham estudando há um bom tempo, números inteiros positivos que podem ser escritos na forma $n(x) = 2^x - 1$ onde $x \in \mathbb{N}$. Para exemplificar, ao selecionarmos $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e substituirmos em $n(x) = 2^x - 1$ obtemos sucessivamente $n(0) = 0$, $n(1) = 1$, $n(2) = 3$, $n(3) = 7$, $n(4) = 15$, $n(5) = 31$, $n(6) = 63$, $n(7) = 127$, $n(8) = 255$ e $n(9) = 511$, dos quais $n(4)$, $n(6)$, $n(8)$ e $n(9)$ são compostos, enquanto que $n(2)$, $n(3)$, $n(5)$ e $n(7)$ são primos.

Mersenne dedicou-se a estudar os números da forma $n(x) = 2^x - 1$ quando x é um número primo, sendo assim, esses números ficaram mais tarde conhecidos como *números de Mersenne*. Utilizando a terminologia mais utilizada na literatura, designaremos os números de Mersenne como

$$M(p) = 2^p - 1,$$

onde p é um número primo.

Ao analisar os exemplos anteriores para alguns valores de $n(x)$ podemos perceber que entre eles existem números compostos e números primos, e sendo assim, caminharemos no sentido de mostrar que para que $n(x)$ tenha alguma chance de ser primo, devemos necessariamente ter x primo. Antes porém necessita-se de um resultado preliminar.

Proposição 2.37. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$*, Temos que* $a - b \mid a^n - b^n$**.**

Uma prova por indução finita dessa proposição pode ser encontrada em [2].

Para exemplificarmos o funcionamento da proposição anterior podemos tomar $a = -2$, $b = 4$ e $n = 3$ e verificarmos que é verdade que

$$(-2 - 4) = (-6) \mid ((-2)^3 - 4^3) = (-8 - 64) = -72,$$

pois $-72 = -6 \cdot 12$ e $12 \in \mathbb{Z}$**.**

O uso desse resultado é fundamental para provarmos a proposição que segue

Proposição 2.38. *Sejam* $a, x \in \mathbb{N}$ *tais que* $a, x > 1$*. Se* $n(x) = 2^x - 1$ *é primo, então* $n(x)$ *é um número de Mersenne. Equivalentemente, se* $n(x) = 2^x - 1$ *é primo, então* x *é primo.*

Demonstração. Suponhamos, por absurdo, que x é composto. Assim $x = i \cdot k$, onde i, k são naturais tais que $1 < i, k < x$. Portanto, pela proposição 2.37, tem-se que

$$2^i - 1 \mid (2^i)^k - 1^k = (2^i)^k - 1 = 2^{i \cdot k} - 1 = 2^x - 1 \Leftrightarrow 2^i - 1 \mid n(x),$$

o que claramente é uma contradição, pois por hipótese $n(x)$ é primo. □

Naturalmente poderia ser perguntado se vale a recíproca dessa proposição, ou seja, se é verdade que x primo implica em $n(x) = 2^x - 1$ ser primo. Infelizmente, a recíproca não é válida, como mostra o contraexemplo a seguir

$$2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89.$$

Os números de Mersenne que são primos, são conhecidos como *primos de Mersenne*, e atualmente os maiores números primos encontrados são todos desse tipo.

Segundo o GIMPS (Great Internet Mersenne Prime Search), um grupo especializado em encontrar primos gigantescos, o maior número primo conhecido é o número de Mersenne $M(82589933) = 2^{82589933} - 1$, que possui 24862048 dígitos e foi descoberto em 21 de Dezembro de 2018 pelo norte-americano Patrick Laroche. (https://www.mersenne.org/, acesso em 28/03/2020.)

Segundo [3] uma sequência numérica definida de maneira recursiva, ou por recorrência, é um procedimento que consiste em especificar um ou mais termos iniciais da sequência, bem como uma *receita* para calcular certo termo em função dos (isto é *recorrendo* aos) termos anteriores a ele. Uma sequência muito conhecida, que é definida recursivamente, é a *sequência de Fibonacci* (para maiores informações sobre essa sequência vide [2]).

Consideremos a seguinte sequência $(S_n)_{n\geqslant 1}$, definida recursivamente por $S_1 = 4$ e $S_n = (S_{n-1})^2 - 2$. Essa sequência aumenta de forma muito rápida, como pode-se perceber ao observar os sete primeiros termos dessa sequência que são calculados a seguir

$S_1 = 4,$

$S_2 = 4^2 - 2 = 14,$

$S_3 = 14^2 - 2 = 194,$

$S_4 = 194^2 - 2 = 37634,$

$S_5 = 37634^2 - 2 = 1416317954,$

$$S_6 = 1416317954^2 - 2 = 2005956546822746114,$$

$$S_7 = 2005956546822746114^2 - 2 = 4023861667741036022825635656102100994.$$

O teste de primalidade Lucas-Lehmer baseia-se no seguinte teorema.

Teorema 2.39. *Seja* $M(p)$ *com* $p > 2$ *um número de Mersenne. Se* $M(p)$ *é primo, então* $M(p) \mid S_{p-1}$. *Equivalentemente, se* $M(p)$ *com* $p > 2$ *é primo, então* $S_{p-1} \equiv 0 \bmod M(p)$.

Uma prova desse teorema pode ser encontrada em [7].

Utilizando alguns dos sete primeiros termos de $(S_n)_{n\geqslant 1}$ calculados acima, faremos alguns exemplos de aplicação do teorema 2.39.

Inicialmente para $p = 3$ temos que $M(3) = 7$ é primo e $S_{3-1} = S_2 = 14$. Pelo teorema 2.39 devemos ter $M(3) = 7 \mid S_2 = 14$. Claramente isso é verdadeiro, pois $14 = 7 \cdot 2$ e $2 \in \mathbb{Z}$. Analogamente para $p = 5$ temos que $M(5) = 31$ é primo e $S_{5-1} = S_4 = 37634$. Pelo teorema 2.39 devemos ter $M(5) = 31 \mid S_4 = 37634$. Novamente isso é verdadeiro, pois $37634 = 31 \cdot 1214$ e $1214 \in \mathbb{Z}$.

Os exemplos para primos maiores vão tornando-se praticamente impossíveis de serem efetuados sem o auxílio de uma boa calculadora. Como dito acima, atualmente esse teste se apresenta-se como uma excelente ferramenta para se encontrar números primos muito grandes. Com o avanço das ferramentas tecnológicos e computacionais, cálculos recursivos utilizando aritmética modular, os quais fundamentam o teste Lucas-Lehmer, não mostram-se um grande empecilho para computadores cada vez mais potentes. Vejamos na prática o funcionamento do teste para os expoentes 11 e 19. Utilizaremos o fato de que todo número inteiro $a > 1$ é congruente ao seu resto módulo n, pois

$$a = n \cdot q + r \Leftrightarrow a - r = n \cdot q \Leftrightarrow n \mid (a - r) \Leftrightarrow a \equiv r \bmod n,$$

para facilitar os cálculos necessários.

Inicialmente $M(11) = 2^{11} - 1 = 2047$, portanto, se $M(11)$ for primo deve-se ter $S_{10} \equiv 0 \bmod 2047$. Pode-se ver que:

$S_1 = 4 \equiv 4 \bmod 2047$,

$S_2 = 4^2 - 2 \equiv 14 \bmod 2047$,

$S_3 = 14^2 - 2 = 194 \equiv 194 \bmod 2047$,

$S_4 \equiv 194^2 - 2 \equiv 788 \bmod 2047$,

$S_5 \equiv 788^2 - 2 \equiv 701 \bmod 2047$,

$S_6 \equiv 701^2 - 2 \equiv 119 \bmod 2047$,

$S_7 \equiv 119^2 - 2 \equiv 1877 \bmod 2047$,

$S_8 \equiv 1877^2 - 2 \equiv 240 \bmod 2047$,

$S_9 \equiv 240^2 - 2 \equiv 282 \bmod 2047$,

$S_{10} \equiv 282^2 - 2 \equiv 1736 \not\equiv 0 \bmod 2047$.

Logo $M(11) = 2^{11} - 1 = 2047$ não é primo.

Já para $M(19) = 2^{19} - 1 = 524287$, se for primo então $S_{18} \equiv 0 \bmod 524287$. Vejamos:

$S_1 = 4 \equiv 4 \bmod 524287$,

$S_2 = 4^2 - 2 = 14 \equiv 14 \bmod 524287$,

$S_3 \equiv 14^2 - 2 \equiv 194 \bmod 524287$,

$S_4 \equiv 194^2 - 2 \equiv 37634 \bmod 524287$,

$S_5 \equiv 37634^2 - 2 \equiv 218767 \bmod 524287$,

$S_6 \equiv 218767^2 - 2 \equiv 510066 \bmod 524287$,

$S_7 \equiv 510666^2 - 2 \equiv 386344 \bmod 524287$,

$S_8 \equiv 386344^2 - 2 \equiv 323156 \bmod 524287$,

$S_9 \equiv 323156^2 - 2 \equiv 218526 \bmod 524287$,

$S_{10} \equiv 218526^2 - 2 \equiv 504140 \bmod 524287$,

$S_{11} \equiv 504140^2 - 2 \equiv 103469 \bmod 524287$,

$S_{12} \equiv 103469^2 - 2 \equiv 417706 \bmod 524287$,

$S_{13} \equiv 417706^2 - 2 \equiv 307417 \bmod 524287$,

$S_{14} \equiv 307417^2 - 2 \equiv 382989 \bmod 524287$,

$S_{15} \equiv 382989^2 - 2 \equiv 275842 \bmod 524287$,

$S_{16} \equiv 275842^2 - 2 \equiv 85226 \bmod 524287$,

$S_{17} \equiv 85226^2 - 2 \equiv 523263 \bmod 524287$,

$S_{18} \equiv 523263^2 - 2 \equiv 0 \bmod 524287$.

Logo $M(19) = 2^{19} - 1 = 524287$ é primo.

Terminamos essa seção apresentando um outro teste de primalidade descoberto por Lucas em 1876. É uma verdadeira recíproca do teorema de Fermat. A demonstração pode ser encontrada em [9].

(Teste de Lucas) Seja $n > 1$. Supõe-se que exista um inteiro $a > 1$ tal que:

- $a^{n-1} \equiv 1 \bmod n$
- $a^m \not\equiv 1 \bmod n$ para $m = 1, 2, ..., (n-2)$.

Então n é primo.

O teste parece perfeito. No entanto exige $n-2$ multiplicações sucessivas por a e a verificação que 1 não é o resto módulo n de nenhuma potência de a inferior a $n-1$. Seriam necessárias demasiadas operações. Acompanhemos o exemplo a seguir, para $a = 2$ e $n = 5$

- $2^{5-1} \equiv 2^4 \equiv 1 \bmod 5$.
- $2^1 \equiv 2 \not\equiv 1 \bmod 5, 2^2 \equiv 4 \not\equiv 1 \bmod 5, 2^3 \equiv 3 \not\equiv 1 \bmod 5$.

Então 5 é primo.

2.7.5 O teste probabilístico Miller-Rabin.

Nessa seção, discutiremos e aplicaremos o teste probabilístico Miller-Rabin para a verificacão da primalidade de um número inteiro $n > 1$. Esse teste, inicialmente determinístico, foi desenvolvido pelo cientista da computação Gary Lee Miller. No entanto, ao se trabalhar números suficientemente grandes, o teste necessita supor verdadeira, a versão generalizada do problema em aberto mais popular da teoria dos números conhecido como a *hipótese de Riemann*, para maiores informações sobre esse problema consultar [8]. Em 1980, o matemático e cientista da computação israelense Michael Oser Rabin, fez algumas modificacões e contribuições no teste, transformando-o no teste probabilístico que aqui apresentaremos. Antes porém precisamos caracterizar alguns números.

Figura 2.9: Gary Miller e Michael Rabin.

Fonte: [10].

Ao falarmos sobre o teste de composição de Fermat, vimos que existem números compostos n que satisfazem a congruência $2^{n-1} \equiv 1 \bmod n$ e $(2, n) = 1$. São os *pseudoprimos na base 2*. De uma maneira geral, números compostos $n > a$ com $(a, n) = 1$ e tais que $a^{n-1} \equiv 1 \bmod n$, são chamados de pseudoprimos na base a.

Por exemplo, sendo $a = 7$ e o número composto $n = 25 = 5 \cdot 5$, temos que

$7^{25-1} \equiv 7^{24} \equiv 19158123138056641 4401 \equiv 1 \bmod 25$, e portanto 25 é um pseudoprimo na base 7.

Uma propriedade semelhante à dos pseudoprimos que é também objeto de estudo pode ser vista a seguir. Sejam $n > 1$ um inteiro composto ímpar e $n - 1 = 2^s \cdot d$, com d ímpar e $s \geqslant 1$. Seja a um inteiro tal que $1 < a < n$, com $(a, n) = 1$. Diz-se que n é um *pseudoprimo forte na base a* quando

- $a^d \equiv \pm 1 \bmod n$, ou então
- $a^{2^r \cdot d} \equiv -1 \bmod n$ para um inteiro r, $1 \leqslant r < s$.

Por exemplo, já observamos que 341 e 25 são pseudoprimos nas bases 2 e 5, respectivamente. Tratemos agora de ver, se eles são pseudoprimos fortes nessas mesmas bases.

Inicialmente para $a = 2$ com $(2, 341) = 1$ temos que

$n = 341 \Leftrightarrow n - 1 = 340 = 2^2 \cdot 85$, com $s = 2$ e $d = 85$ assim,

- $2^{85} \equiv 32 \not\equiv \pm 1 \bmod 341$.
- $r = 1$,

$$2^{2^1 \cdot 85} = 2^{2 \cdot 85} = 2^{170} \equiv 1 \not\equiv -1 \bmod 341.$$

Logo 341 não é um pseudoprimo forte na base 2.

Agora para $a = 7$ com $(7, 25) = 1$ temos que

$n = 25 \Leftrightarrow n - 1 = 24 = 2^3 \cdot 3$, com $s = 3$ e $d = 3$ assim,

- $7^3 = 343 \equiv 18 \not\equiv \pm 1 \bmod 25$.
- $r = 1$,

$$7^{2^1 \cdot 3} = 7^{2 \cdot 3} = 7^6 = 117649 \equiv 24 \equiv -1 \bmod 25.$$

Logo 25 é um pseudoprimo forte na base 7.

Em [9] encontramos que para a formulação do teste Miller-Rabin, que utiliza congruências que definem números pseudoprimos fortes, é prático utilizar a seguinte terminologia:

Se n é um número natural, se $1 < a < n$, se $n - 1 = 2^s \cdot d$, com $s \geqslant 0$, d ímpar, então a é uma *testemunha* para n se,

1. $a^{n-1} \not\equiv 1 \bmod n$, ou então
2. Existe um inteiro r, tal que $0 \leqslant r < s$ e $1 < (a^{2^r \cdot d} - 1, n) < n$.

Se n tem uma testemunha, então n é composto.

Assim, se n é composto, $1 < a < n$ e se a não é uma testemunha para n então $(a, n) = 1$ e n é um pseudoprimo forte na base a. Reciprocamente, se n é ímpar e se n é um pseudoprimo forte na base a, então a não é uma testemunha para n.

Vimos acima que 341 não é um pseudoprimo forte na base 2, mas que 25 é um pseudoprimo forte na base 7, para exemplificar as terminologias acima mostremos que $a = 2$ é uma testemunha para $n = 341$, e que $a = 7$ não é uma testemunha para $n = 25$.

Afim de verificar que $a = 2$ é uma testemunha para $n = 341$ fazemos

1. $$2^{341-1} = 2^{340} \equiv 1 \bmod 340.$$

   O número inteiro a não passou no primeiro teste.

2. $n - 1 = 340 = 2^2 \cdot 85$, com $s = 2$ e $d = 85$. Devemos encontrar o $(2^{2^r \cdot 85} - 1, 341)$ para $r \in \{0, 1\}$, e depois verificar se $1 < (2^{2^r \cdot 85} - 1, 341) < 341$, para algum r.

   Para $r = 0$,

   $$(2^{2^0 \cdot 85} - 1, 341) = (2^{1 \cdot 85} - 1, 341) = (2^{85} - 1, 341) = 31, \text{ e } 1 < 31 < 341.$$

   Logo, existe um inteiro $0 \leqslant r < 2$, tal que $1 < (2^{2^r \cdot 85} - 1, 341) < 341$.

O número a passou no segundo teste. Portanto $a = 2$ é uma testemunha para $n = 341$.

Analogamente afim de verificar que $a = 7$ não é uma testemunha para $n = 25$ fazemos

1.
$$7^{25-1} = 7^{24} \equiv 1.$$

O número a não passou no primeiro teste.

2. $n - 1 = 24 = 2^3 \cdot 3$, com $s = 3$ e $d = 3$. Devemos pois encontrar o $(7^{2^r \cdot 3} - 1, 25)$ para $r \in \{0, 1, 2\}$ e verificar se $1 < (7^{2^r \cdot 3} - 1, 25) < 25$ para algum r.

Para $r = 0$,

$$(7^{2^0 \cdot 3} - 1, 25) = (7^{1 \cdot 3} - 1, 25) = (7^3 - 1, 25) = 1.$$

Para $r = 1$,

$$(7^{2^1 \cdot 3} - 1, 25) = (7^{2 \cdot 3} - 1, 25) = (7^6 - 1, 25) = 1.$$

Para $r = 2$,

$$(7^{2^2 \cdot 3} - 1, 25) = (7^{4 \cdot 3} - 1, 25) = (7^{12} - 1, 25) = 25.$$

Logo, não existe um inteiro $0 \leqslant r < 3$ tal que $1 < (7^{2^r \cdot 3} - 1, 25) < 25$. O número a também não passou no segundo teste. Portanto $a = 7$ não é uma testemunha para $n = 25$.

Segundo [9], no começo do século XX, o Cassino de Monte Carlo atraía aristocratas e aventureiros, possuídos pela irresistível paixão pelo jogo. Os azares da roleta faziam e desfaziam fortunas. Não faltam exemplos de pessoas que tiveram a vida inteiramente transformada quando a sorte os favoreceram e também de outras pessoas que lá encontraram a ruína e tiveram trágicos fins suicídas.

O teste de primalidade Miller-Rabin tem esse espírito de Monte Carlo, ou seja, depende-se do acaso, já que é um teste probabilístico realizado em duas etapas, em que são utilizados

um certo número de testemunhas a escolhidas aleatoriamente, ligadas com congruências semelhantes a aquelas satisfeitas pelos pseudoprimos. Vejamos agora, de modo sucinto, o seu funcionamento.

(**Teste Probabilístico Miller-Rabin**)

1. Escolhe-se, ao acaso, $k > 1$ pequenos inteiros a, tais que $1 < a < n$ e $(a, n) = 1$.

2. Testa-se sucessivamente, para cada base escolhida a, se n satisfaz a condição de definição de um número fortemente pseudoprimo na base a, ou seja, fazendo $n - 1 = 2^s \cdot d$, com d ímpar, $s \geqslant 0$,

   - ou então $a^d \equiv 1 \bmod n$,
   - ou então $a^{2^r \cdot d} \equiv -1 \bmod n$, para um r, $0 \leqslant r < s$.

Se encontrarmos um inteiro a, para o qual as condições acima indicadas não são satisfeitas, n é composto. Em caso contrário, n é provavelmente primo, e a probabilidade que n seja primo é, pelo menos, igual a $(1 - \frac{1}{4^k})$. Obviamente, quanto mais bases a testarmos maior a probabilidade do número ser primo.

Vejamos, na prática, o funcionamento do teste. Suponhamos que precisássemos saber se o número 9973 é primo, e utilizando os caminhos apontados no teste Miller-Rabin, escolheremos ao acaso $k = 3$ inteiros $a = 8$, $a' = 154$ e $a'' = 1117$ e tais que $(8, 9973) = 1$, $(154, 9973) = 1$ e $(1117, 9973) = 1$. Ao executarmos todos os procedimentos, e nenhum dos a, a' e a'' satisfizerem as condições do teste, a probabilidade de 9973 ser primo será de

$$1 - \frac{1}{4^3} = 1 - \frac{1}{64} = \frac{63}{64} \approx 0,9844 \approx 98,44\%.$$

$n = 9973 \Leftrightarrow n - 1 = 9972 = 2^2 \cdot 2493$, com $s = 2$ e $d = 2493$.

Para $a = 8$,

- $8^{2493} \equiv 2798 \not\equiv 1 \bmod 9973$.
- Para $r = 0$ temos $8^{2^0 \cdot 2493} = 8^{1 \cdot 2493} = 8^{2493} \equiv 2798 \not\equiv -1 \bmod 9973$.

Para $r = 1$ temos $8^{2^1 \cdot 2493} = 8^{2 \cdot 2493} = 8^{4986} \equiv 9972 \equiv -1 \bmod 9973$.

Assim $a = 8$ não é uma testemunha da composição de $n = 9973$. Sendo assim $n = 9973$ é um pseudoprimo forte na base $a = 8$.

Para $a' = 154$,

- $154^{2493} \equiv 7175 \not\equiv 1 \bmod 9973$.
- Para $r = 0$ temos $154^{2^0 \cdot 2493} = 154^{1 \cdot 2493} = 154^{2493} \equiv 7175 \not\equiv -1 \bmod 9973$.

  Para $r = 1$ temos $154^{2^1 \cdot 2493} = 154^{2 \cdot 2493} = 154^{4986} \equiv 9972 \equiv -1 \bmod 9973$.

Assim $a' = 154$ não é uma testemunha da composição de $n = 9973$. Sendo assim $n = 9973$ é um pseudoprimo forte na base $a' = 154$.

Para $a'' = 1117$,

- $1117^{2493} \equiv 7175 \not\equiv 1 \bmod 9973$.
- Para $r = 0$ temos $1117^{2^0 \cdot 2493} = 1117^{1 \cdot 2493} = 1117^{2493} \equiv 7175 \not\equiv -1 \bmod 9973$.

  Para $r = 1$ temos $1117^{2^1 \cdot 2493} = 1117^{2 \cdot 2493} = 1117^{4986} \equiv 9972 \equiv -1 \bmod 9973$.

Assim $a'' = 1117$ não é uma testemunha da composição de $n = 9973$. Sendo assim $n = 9973$ é um pseudoprimo forte na base $a'' = 1117$.

Logo, pelo teste Miller-Rabin, $n = 9973$ é provavelmente primo. Tal probabilidade é de aproximadamente $98,44\%$.

Vejamos agora, um segundo exemplo para o número $n = 7387$. Escolheremos ao acaso $a = 16$, $a' = 441$ e $a'' = 2898$ com $(16, 7387) = 1, (441, 7387) = 1$ e $(2898, 1) = 1$. Analogamente, como tomamos $k = 3$, se nenhum dos a, a' e a'' satisfizerem as condições do teste, a probabilidade de 7387 ser primo será de aproximadamente $98,44\%$. Assim

$n = 7387 \Leftrightarrow n - 1 = 7386 = 2^1 \cdot 3693$, com $s = 1$ e $d = 3693$. Como $s = 1$ é suficiente realizarmos apenas a primeira parte do teste, com o acréscimo de verifcarmos se

$a^d \equiv -1 \bmod n$ pois na segunda parte teríamos que utilizar um $0 \leqslant r < s$, logo $r = 0$, e o cálculo correspondente para tal r é a primeira parte do teste. Para $a = 16$,

- $16^{3693} \equiv 2270 \not\equiv 1 \bmod 7387$ e $16^{3693} \equiv 2270 \not\equiv -1 \bmod 7387$

Assim $a = 16$ é uma testemunha da composição de $n = 7387$, e pelo teste Miller-Rabin n é composto. Nota-se que acaba nem sendo necessário testar para $a' = 441$ e $a'' = 2818$, pois já encontramos um inteiro $a = 16$ que não satisfaz as condições do teste.

Para finalizar, segundo [9], o único número composto $n < 25 \cdot 10^9$, que é pseudoprimo forte, simultaneamente nas bases 2, 3, 5 e 7, é o número 3215031751. Então, caso formos testar a primalidade de um determinado número $n < 25 \cdot 10^9$, se n não é igual a 3215031751 e se 2, 3, 5 e 7 não são testemunhas para n, então n é primo.

Grosso modo, ao testar a primalidade de um número menor do que 25000000000 (vinte e cinco bilhões), basta utilizarmos o teste Miller-Rabin para as bases 2, 3, 5 e 7. Caso tais bases não forem testemunhas da composição do número testado, teremos certeza absoluta se tal número é primo, ou seja, nesse caso o teste deixará de ser probabilístico e se tornará determinístico.

Como exemplo, vamos testar o número natural 104588839. Temos claramente que $104588839 < 25000000000$, portanto basta aplicarmos o teste Miller-Rabin e verificarmos que nenhuma das bases 2, 3, 5 e 7 são testemunhas da composição de 104588839. Pois bem:

$n = 104588839 \Leftrightarrow n - 1 = 104588838 = 2 \cdot 52294419$, com $s = 1$ e $d = 52294419$. Assim, temos que

- $2^{52294419} \equiv 1 \bmod 104588839$.

  Portanto 2 não é testemunha da composição de 104588839. Com isso conclui-se que 104588839 é um pseudoprimo forte na base 2.

- $3^{52294419} \equiv -1 \bmod 104588839$.

  Portanto 3 não é testemunha da composição de 104588839. Com isso conclui-se que

104588839 é um pseudoprimo forte na base 3.

- $5^{52294419} \equiv 1 \bmod 104588839$.

  Portanto 5 não é testemunha da composição de 104588839. Com isso conclui-se que 104588839 é um pseudoprimo forte na base 5.

- $7^{52294419} \equiv 1 \bmod 104588839$.

  Portanto 7 não é testemunha da composição de 104588839. Com isso conclui-se que 104588839 é um pseudoprimo forte na base 7.

Logo, 104588839 é um pseudoprimo forte nas bases 2, 3, 5 e 7 simultaneamente. Como o único número composto $n < 25 \cdot 10^9$, que é pseudoprimo forte, simultaneamente nas bases 2, 3, 5 e 7, é o número 3215031751, concluímos que 104588839 é primo.

3 Construção de uma atividade pedagógica

Neste capítulo, iremos abordar e descrever a criação de uma proposta pedagógica, mais precisamente uma Situação de Aprendizagem, apoiada no Teorema Fundamental da Aritmética, e que poderá ser aplicada no Sétimo Ano do Ensino Fundamental. Tal proposta aborda o problema da determinação da primalidade de um número natural, e faz uso da fatoração de um número natural em potências de números primos, para abordar questões que requerem não somente o cálculo, como também aplicações dos conceitos de máximo divisor comum e mínimo múltiplo comum, na resolução de problemas do cotidiano.

3.1 Características do público alvo e escolha do tema

Lecionando há quase uma década na Educação Básica do Estado de São Paulo, particularmente nos anos finais do Ensino Fundamental e no Ensino Médio, não é muito difícil perceber que os estudantes chegam ao 6º ano do Ensino Fundamental repletos de curiosidade e energia, elementos característicos de suas faixas etárias. Ao abordar os conteúdos com entusiasmo e paixão, o professor consegue facilmente perceber o brilho no olhar dos jovens, e sente que ali naquele ambiente, é o momento de trazer à tona problemas diversos, relacionados com o componente curricular ensinado. Porém esse espírito curioso e investigativo, e essa chama do aprender parece ir se arrefecendo com o passar dos anos, e não faltam relatos de profissionais da área, dizendo que os alunos perdem o interesse pelo conteúdo ministrado, e que se tornam mais apáticos ou indiferentes àquilo que lhes está sendo apresentado. Acreditamos que o envolvimento familiar é parte fundamental nessa perda do interesse, pois é notória a participação mais efetiva dos responsáveis em reuniões pedagógicas que envolvem as turmas dos alunos

alocados nos sextos e sétimos anos do Ensino Fundamental, enquanto que tal participação, vai se tornando cada vez menor à medida que o estudante vai evoluindo no seu percurso escolar.

Tal particularidade, não deixa de ser observada na escola estadual em que lecionamos, localizada na região central da cidade de Itirapina, estado de São Paulo. Sendo a única escola de Ensino Médio da cidade e funcionando em todos os três períodos, faz-se necessário uma organização diferenciada para lidar com as questões de logística e transporte dos alunos. Por essas e outras questões o público se difere bastante entre os turnos da escola, tendo cada público sua maneira peculiar de assimilar e desenvolver as atividades relacionadas ao seu aprendizado. Os alunos do período da manhã são em sua maioria, advindos da zona rural da cidade, ao passo que o turno da tarde, tem em grande parte alunos moradores da cidade, e o turno da noite é composto por jovens e adultos que de uma forma ou de outra, já dividem suas atividades escolares com seus compromissos financeiros.

Ao levarmos em conta essa especificidade do público e a possível perda de interesse gradativa dos estudantes, pensamos em desenvolver uma atividade pedagógica, que de antemão, está vinculada a conteúdos específicos do 6º e 7º ano do Ensino Fundamental, porém que pode ser aplicada em qualquer turma da escola, seja em uma retomada de conceitos ou nos períodos de estudos intensivos que são característicos da rede estadual paulista. Acreditamos que a escolha do problema da determinação da primalidade de um número natural, baseado em sua fatoração em potências de números primos, tem esse cárater curioso e investigativo que tanto notamos nos nossos alunos no começo do Ensino Fundamental, e pode ser utilizado tanto para que a chama da curiosidade não se apague, como para reacencê-la, caso esta tenha se apagado.

Quando trabalhado em detalhes no 6º e no 7º ano do Ensino Fundamental, o problema da primalidade de um número natural torna-se de essencial importância, não só para o aprimoramento das habilidades relacionadas ao algoritmo da divisão euclidiana e para uma classificação dos números naturais, como também para a consolidação das noções de *ser divisor ou fator de*, *ser múltiplo de* ou *ser divisível por*, além do cálculo do máximo divisor comum e do mínimo múltiplo comum entre números inteiros, bem como a aplicação desses conceitos

na resolução de problemas contextualizados. Isso posto, procuramos desenvolver uma situação de aprendizagem em que o aluno, ao procurar saber se um determinado número é composto ou primo, se familiarize e entenda o significado e os limites da fatoração de um número natural em potências de números primos, e perceba que realizar com eficácia a fatoração pode enriquecer o seu vocabulário matemático e lhe ajudar a resolver outros problemas que aparecerão em sua trajetória escolar.

3.2 Planejando a atividade pedagógica

Atualmente, em toda a SEDUC (Secretaria da Educação do Estado de São Paulo), tem-se como guia de referência para as habilidades que devem ser desenvolvidas junto aos estudantes do Ensino Fundamental (até o presente momento, o material comum ao Ensino Médio, ainda está em etapa de consulta pública, e por enquanto ainda são oferecidos aos estudantes guias de transição, até que o texto final esteja pronto), um texto chamado *Currículo Paulista* conforme [13]. Este documento, preparado de acordo com a Base Nacional Comum Curricular, fixa quais são as expectativas de aprendizagem dos alunos e quais conteúdos devem ser ministrados por seus professores. Todos os alunos recebem material didático cujas atividades estão embasadas no Currículo Paulista. Portanto, seja qual for o conteúdo que se deve trabalhar na educação pública do estado de São Paulo, ele deve ser necessariamente pautado nas habilidades do Currículo Paulista. O modo como essas habilidades serão trabalhadas é de livre escolha do professor, que relata tudo em seu planejamento bimestral, haja visto que cada escola e cada turma tem suas caracteristícas particulares.

O Currículo Paulista focado no ensino de Matemática está dividido em cinco unidades temáticas: Álgebra, Geometria, Grandezas e Medidas, Números e ainda Probabilidade e Estatística. Optamos por desenvolver uma situação de aprendizagem que trabalhe com a unidade temática dos Números, e que basicamente tem como finalidade desenvolver o pensamento numérico do aluno, o que, além de desenvolver conhecimentos sobre os números e suas relações, envolve a compreensão das operações e seus resultados, reconhecendo o significado ao operar

com um número para obter outros.

Com a aplicação da situação de aprendizagem tem-se como meta, que os alunos desenvolvam ou aprimorem algumas habilidades específicas que se encontram no texto do Currículo Paulista, quais sejam:

- EF06MA05: Classificar números naturais em primos e compostos, estabelecendo relações entre números expressas pelos termos *é múltiplo de*, *é divisor de*, *é fator de*.
- EF06MA06: Resolver e elaborar situações-problema que envolvam as ideias de múltiplo e divisor, reconhecendo os números primos, múltiplos e divisores.
- EF07MA01: Resolver e elaborar situações-problema com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas.

Para que as habilidades citadas sejam desenvolvidas de maneira mais satisfatória possível, foi pensado que a situação de aprendizagem pudesse ser dividida em 7 etapas, as quais realizadas com cautela e acompanhamento constante, podem facilitar o objetivo geral de alcançar as habilidades acima citadas. É importante colocar também, que tais etapas, formam um caminho linear de aprendizagem rumo a assimilação das habilidades, porém uma ou outra etapa, pode ser ajustada ou até removida, de acordo com o interesse da turma e o planejamento do professor. Os prazos para a realização de cada etapa, também podem sofrer alterações, pois eles foram pensados, levando-se em conta, as especificidades de alunos com um nível insatisfatório de conceitos básicos.

3.2.1 Etapa 1: Retomada e noções de divisibilidade.

Para o desenvolvimento dessa primeira etapa da situação de aprendizagem, nota-se que, da maneira como desejamos que os alunos trabalhem com o problema da primalidade de um número natural, faz-se necessário que habilidades referentes aos cálculos dos resultados

de adições e subtrações, bem como multiplicações e divisões euclidianas de números naturais, estejam minimamente desenvolvidas. É importante que o aluno tenha aptidão também em representar o produto de fatores iguais na forma de uma potência de expoentes naturais, além de conseguir observar que, sendo a um número natural, tem-se sempre que $a^0 = 1$. Caso tais habilidades ainda não estejam contempladas, uma retomada delas torna-se fundamental. Um questionário contendo questões de levantamento dos conhecimentos prévios dos estudantes a respeito dessas habilidades, pode ser aplicado antes de começarmos de fato a desenvolver a situação de aprendizagem, sendo portanto sua primeira etapa, a qual pode ser realizada com bastante atenção em 4 aulas. Tal questionário pode conter questões do tipo

1. O que de fato significa dizer que 2 divide 6, ou então que 3 não divide 8? Você conseguiria representar matematicamente essas situações?

   Para a primeira parte da questão é esperado que os alunos tenham a noção de que, ao afirmarem que 2 divide 6, entendam que é possível dividir o número 6, em três grupos, contendo duas unidades, de tal forma que não sobre resto, ou equivalentemente, ao afirmar que 2 divide 6, os estudantes sejam capazes de perceber que para responder a esse questionamento, devem efetuar a divisão euclidiana de 6 por 2 e confirmar que o resto dessa divisão é zero. E que ao afirmar que 3 não divide 8, estejam convencidos de que, a tentativa de dividir o número 8 em grupos com 3 unidades, não é possível de ser realizada, haja visto que sobram duas unidades de resto, ou equivalentemente, devem efetuar a divisão euclidiana de 8 por 3 e notar que o resto é um número diferente de zero. Ao perguntar se conseguem representar matematicamente essas situações, deseja-se que o aluno seja capaz de realizar a divisão euclidiana dos números em questão e que consigam representar $6 = 2 \cdot 3$ ou $6 = 2 \cdot 3 + 0$ e $8 = 3 \cdot 2 + 2$.

2. Qual é o resultado de $3 \cdot 3 \cdot 3 \cdot 5^0$? E de $2 \cdot 2 \cdot 5 \cdot 5$? Você consegue representar essas multiplicações na forma de uma potência?

   Num primeiro momento, o aluno pode estranhar a representação 5^0, porém após a exposição de que no geral, para todo $a \in \mathbb{N}$ tem-se $a^0 = 1$, e sendo 1 elemento neutro

da multiplicação, espera-se que os estudantes sejam capazes de não somente calcular corretamente $3 \cdot 3 \cdot 3 \cdot 3 \cdot 5^0 = 81 \cdot 1 = 81$ e $2 \cdot 2 \cdot 5 \cdot 5 = 100$, como representar $3 \cdot 3 \cdot 3 \cdot 3 \cdot 5^0 = 3^4 \cdot 5^0 = 3^4 = 81$ e $2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2 = 100$.

Ainda no contexto do questionário de conhecimentos prévios, as respostas dadas pelos alunos, podem e devem servir para a elaboração de atividades de retomada do algoritmo da divisão euclidiana e da representação de uma multiplicação em forma de potência, bem como para introduzir e colocar em bases sólidas a noção de divisibilidade. Este momento torna-se oportuno para que termos como *ser divisor de, ser fator de, ser múltiplo de, ser divisível por* sejam apresentados e discutidos em seus muitos detalhes. Feita a aula expositiva desses conteúdos, espera-se que os alunos sejam capazes de justificar que ao afirmar que 2 divide 6, o número 2 é um divisor de 6, ou ainda que, o número 2 é um fator de 6, podendo ser também dito que o número 6 é um múltiplo de 2. O mesmo deve acontecer ao afirmar que 3 não divide 8, ou seja, os alunos necessitam perceber que 3 não é um divisor de 8, ou que 3 não é um fator de 8, ou ainda que 8 não é múltiplo de 3. De uma maneira geral, ao final dessa primeira etapa, o objetivo primordial é que o aluno perceba que ao trabalhar com números naturais quaisquer a e b, fazer afirmações do tipo a *é divisor de* b ou b *é múltiplo de* a, está intimamente ligado a ideia de executar a divisão euclidiana de b por a e observar o resto que aparecerá.

3.2.2 Etapa 2: Múltiplos, divisores, mmc e mdc.

Dentro do conteúdo da relação de divisibilidade, ao se familiarizarem com os termos divisores e múltiplos, já podemos trabalhar conceitos como divisores e múltiplos comuns entre números naturais a e b, bem como as ideias de máximo divisor comum e de mínimo múltiplo comum, com suas respectivas representações (a, b) e $[a, b]$. O trabalho com esses conceitos, se dará na nossa segunda etapa da situação de aprendizagem, a qual acreditamos serem necessárias 4 aulas, afim de realizar as discussões e apresentações das ideias e definições. Para o desenvolvimento dessa etapa da atividade pode-se apresentar questionamentos do tipo:

1. O número 98 é múltiplo do número 7? Você conseguiria representar matematicamente essa situação?

   Esperamos que ao se deparar com esse problema, o aluno perceba que descobrir se o número 98 é múltiplo de 7, é equivalente a descobrir se 7 divide 98, problema esse, que ele já enfrentou durante o questionário de conhecimentos prévios e durante as atividades de retomada. Portanto, para saber se 7 divide 98 e representar matematicamente essa situação, ele deve efetuar a divisão euclidiana de 98 por 7 e verificar se o resto dessa divisão é zero. E ao fazê-lo confirma que $98 = 7 \cdot 14 + 0$ ou $98 = 7 \cdot 14$, logo 7 divide 98 e consequentemente 98 é múltiplo de 7.

2. Quem são os divisores do número 28 e do número 30? Existem divisores comuns entre 28 e 30? Qual deles é o maior? E qual é o menor?

   Nesse primeiro momento, como ainda não foi trabalhado o teorema fundamental da Aritmética, o intuito é que aluno descubra euristicamente, quais são os divisores de 28 e 30, necessariamente, realizando a divisão euclidiana de 28 e 30 pelos possíveis candidatos a divisores. Esperamos que os alunos percebam que a lista dos divisores de um número é finita, e que o maior divisor de um número natural, é ele próprio. Após esta primeira parte da questão, os estudantes serão convidados a listar os divisores de 28 e 30 da seguinte forma

   $\mathrm{d}(28) = \{1, 2, 4, 7, 14, 28\}$

   $\mathrm{d}(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

   Tal representação, em uma lista ordenada, facilita a visualização de divisores comuns entre os números apresentados, bem como a identificação do maior e do menor divisor comum. Aqui, faz-se necessário salientar que o número 1, em qualquer circunstância, será divisor de qualquer número natural, e portanto será sempre o menor divisor comum entre números naturais, iniciando a primeira ideia de números primos entre si, sem que necessariamente usemos essa determinação. É esperado também que os alunos identifiquem o máximo divisor comum entre os números 28 e 30, como sendo um divisor

comum de 28 e 30, com a propriedade adicional de ser divisível por todos os divisores comuns de 28 e 30. Os estudantes podem identificar seus resultados como:

$\mathrm{d}(28e30) = \{1, 2\}$ e $(28, 30) = 2$

3. Existem múltiplos comuns entre os números 4 e 5? Conseguimos identificar qual é o maior? E qual o menor?

   Ao realizar esta atividade, é esperado que os alunos, consigam perceber que números que são múltiplos de 4, são números divisíveis por 4, ou seja, estamos procurando quais são os números que o 4 divide. Mesmo raciocínio pode ser aplicado para o número 5. No decorrer da atividade, seria interessante, que os alunos associassem também a ideia de ser múltiplo com a operação de multiplicação, ou seja, percebam que para obter os múltiplos de um número natural, basta multiplicar esse número por todos os números naturais, relacionando com a tabuada, algo já apresentado a eles nos anos anteriores. Repostas podem ser colocadas na forma:

   $\mathrm{m}(4) = \{0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, ...\}$

   $\mathrm{m}(5) = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, ...\}$

   Aqui, trazemos a tona, a ideia de que, ao multiplicar um número natural por todos os números naturais, afim de obter os seus múltiplos, nossa lista não termina nunca, ou seja, é infinita, pois estamos multiplicando um número, por um conjunto que é infinito, o dos números naturais, justificando portanto as reticências na nossa lista. Ora, se o conjunto dos múltiplos de um número natural é infinito, não conseguimos determinar qual é o maior múltiplo dele, tampouco o maior múltiplo comum de números naturais. Ao observar a lista dos múltiplos comuns entre 4 e 5, nosso objetivo também, é que os estudantes percebam, que os múltiplos comuns entre 4 e 5, são os múltiplos de 20, que também é um conjunto infinito, e pode ser representado como:

   $\mathrm{m}(4e5) = \{0, 20, 40, 60, 80, 100, ...\}$

   Ao questionarmos qual é o menor ou mínimo múltiplo comum entre os números 4 e 5, dependendo da definição que dermos ao mmc, o aluno, ao observar a lista construída,

pode ser tentado a responder que o número 0 é sempre o mínimo múltiplo comum entre números naturais. Tal equívoco, tem sua chance minimizada de ocorrer, se pormos em bases firmes que o mínimo múltiplo comum de dois números naturais, além de ser um múltiplo comum dos dois números naturais, possui a propriedade de dividir qualquer outro múltiplo comum entre esses dois números, e é sabido que 0 é um mmc entre dois números naturais se, e somente se, um dos números apresentados também é 0, pois o único número divisível por 0 é o próprio 0. Caso seja aplicado em turmas posteriores ao 6º ano, podemos simplesmente dizer que desejamos múltiplos positivos. Vencidos esses pormenores, espera-se que a reposta seja colocada na forma $[4,5] = 20$.

3.2.3 Etapa 3: Compostos ou primos.

Abordadas cuidadosamente as ideias associadas a relação de divisibilidade e conceitos como múltiplos comuns, divisores comuns, máximo divisor comum e mínimo múltiplo comum, é chegada a hora de uma terceira etapa da situação de aprendizagem. O objetivo dessa etapa é que os estudantes consigam classificar os números naturais em compostos ou primos, baseados nas ideias apresentadas anteriormente.

Começaremos definindo os números primos como números naturais, maiores do que um, e que possuem a propriedade de apresentar apenas dois divisores, o número um e ele próprio (os divisores triviais). Qualquer número natural, maior do que um, e que tenha mais do que dois divisores não poderá ser primo, sendo então classificado como um número composto. Para fundamentar essa classificação faremos uso de um teorema que envolve a relação de ordem nos números naturais, particularmente, os estudantes precisam ser capazes de reconhecer quando um determinado número natural é *menor ou igual que* outro. Por exemplo, o aluno deve conseguir verificar o valor lógico de afirmações do tipo: $4 \leqslant 4$, $7 < 8$, $9 > 10$ e assim sucessivamente. Exemplos e uma pequena exposição de tais assuntos torna-se imprescindível nesse momento e espera-se que, de uma forma geral, 6 aulas sejam necessárias para abordá-los e desenvolver essa terceira etapa.

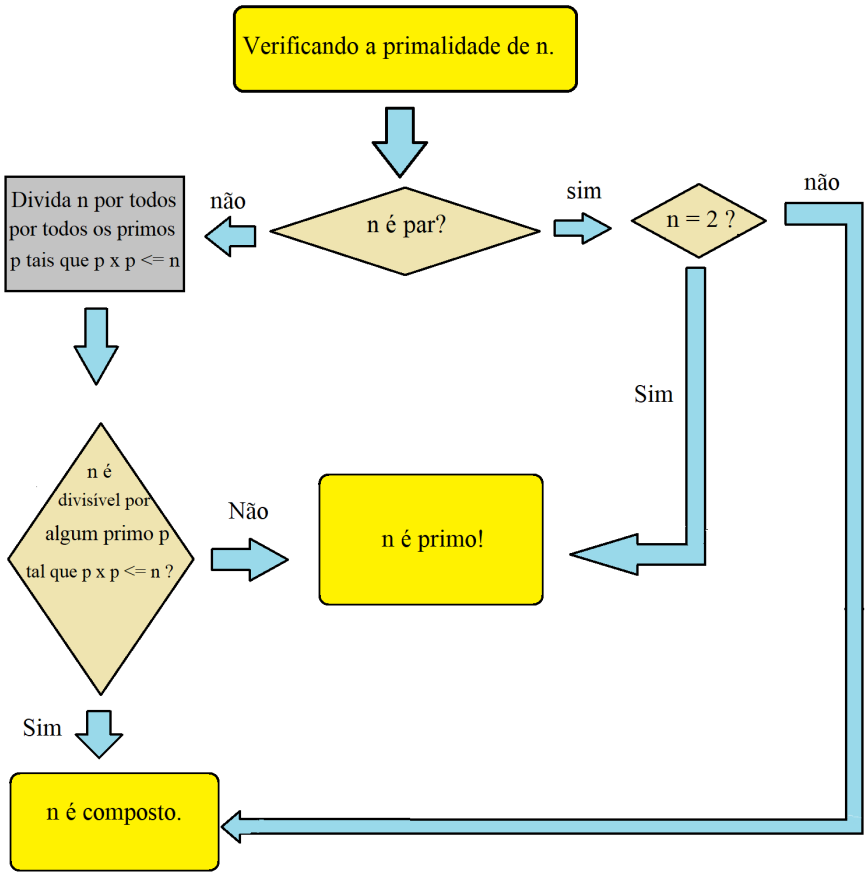
Nosso ponto de partida, estará apoiado no teorema 2.27, que será apresentado de maneira bem acessível, e nos diz que *se um número natural a, maior do que um, é composto, então ele é múltiplo de algum número primo p, tal que* $p^2 \leqslant a$, ou equivalentemente, *se um número natural a, maior do que um, é composto, então existe algum número primo p que o divide e tal que* $p^2 \leqslant a$. Por exemplo, para afirmar que 6 é um número composto, basta verificar se o número primo 2 o divide, já que ele é o único primo que satisfaz a desigualdade $2^2 = 4 \leqslant 6$.

Pela classificação dos naturais, se um número não for composto, ele será primo. Estaremos interessados em mostrar, que de posse de uma lista relativamente pequena de números primos, conseguiremos determinar a primalidade de vários números naturais. Para conseguir tal lista, com no máximo 25 números primos, podemos apresentar e desenvolver com os estudantes o Crivo de Eratóstenes, e aproveitar a apresentação do teorema, para justificar a razão de podermos parar de utilizar o crivo ao encontrar determinados números.

De posse da lista contendo os 25 primeiros números primos, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97 e tendo assimilado bem o conteúdo do teorema, faz-se necessário orientar que, ao tentar resolver o problema da primalidade de algum número natural a, inicialmente devemos procurar quais são os números primos da lista que satisfazem a desigualdade $p^2 \leqslant a$ apresentada, para só depois começarmos a verificar se algum deles é um divisor de a.

É importante notar que as habilidades relacionadas ao cálculo de potências do tipo p^2 não podem ser um empecilho nesse momento, e caso ainda o sejam, expor mais alguns exemplos torna-se necessário. Pode-se iniciar atividades de aplicação do teorema, para números naturais com poucos algarismos e que satisfaçam a desigualdade para algum primo da lista. Nesse momento não é necessário que o estudante realize a fatoração completa do número a ser testado, apenas que encontre algum número primo que o divida. O fluxograma de logo mais, ilustra o modo como esperamos que o aluno trate o problema de determinar a primalidade de um número natural, nessa abordagem inicial.

Figura 3.1: Fluxograma para determinar a primalidade de um número natural n.



Uma sugestão seria começar com questões abordando a característica do número natural proposto (ser composto ou primo) com perguntas cuja dificuldade vai aumentando gradativamente, tais como:

1. O número natural 221 é primo?

   Aqui espera-se que os alunos comecem observando, na lista de números primos obtida com a ajuda do crivo de Eratóstenes, que os números primos 2, 3, 5, 7, 11 e 13 satisfazem a desigualdade $p^2 \leqslant 221$, e em seguida, observando o conteúdo do teorema, os estudantes sejam capazes de perceber que se 221 for composto, algum ou alguns dos primos que satisfazem a desigualdade devem dividi-lo, e comecem a realizar as divisões euclidianas de 221 por cada um desses primos. Se tudo ocorrer dentro dos conformes, devem constatar que $221 = 13 \cdot 17$, ou seja, 13 divide 221 ou que 221 é múltiplo de 13 ou ainda que 221 é divisível por 13, portanto 221 é composto, logo não é primo.

Depois de realizadas atividades de investigação da primalidade de diversos números, é sugerido que os próprios estudantes comecem a escolher números a serem testados, e nesse momento, mesmo que durante a exposição, tenha-se deixado claro os motivos do número 2 ser o único número primo par, aparecerão números pares a serem testados, equívoco esse que não deve ser um problema, pois os alunos constatarão que 2 divide tal número, e com isso, de modo gradativo, se acostumarão com a ideia de não haver a necessidade de se testar números pares. A tendência é que esse equívoco desapareça depois de um curto intevalo de tempo. Os alunos também podem começar a escolher números muito grandes de tal forma que a lista que possuem não contenha um primo que o divida, ou então, escolham um número grande o suficiente para que a determinação de sua primalidade seja um trabalho bem árduo. Em todo caso, a mediação do professor é importante, ao acompanhar as escolhas dos estudantes e minimizar essas situações.

3.2.4 Etapa 4: O teorema fundamental da aritmética.

É chegada a hora, de darmos o próximo passo no desenvolvimento da situação de aprendizagem. Na quarta etapa será feita a apresentação em detalhes do *teorema fundamental da aritmética*. Em nossa experiência com os materiais disponibilizados pela SEDUC, notamos que tal teorema, quando apresentado, é feito de uma maneira não muito detalhado. Acreditamos que a apresentação e discussão desse teorema, que em essência, afirma que qualquer problema referente a números inteiros, pode ser "quebrado"em um problema de fatoração, merece um pouco mais de atenção nessa fase de escolarização dos estudantes. Apresentado e discutido, o teorema servirá para introduzir a ideia da fatoração de um número natural em potências de números primos, mostrar que expressões como *ser divisor de* e *ser fator de* são sinônimas e reforçar a relevância dos números primos, na construção de qualquer número natural.

Para a aplicação dessa quarta etapa da situação de aprendizagem, acreditamos serem necessárias pelo menos 4 aulas, e sugerimos que, atividades de caráter investigativo um pouco mais elaboradas possam ser aplicadas. Uma sugestão de tais atividades é apresentada a seguir.

1. O número 2793 é primo? Caso ele seja composto, exiba sua fatoração em potências de números primos.

   Espera-se que o aluno novamente perceba que os números primos 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47 são possíveis candidatos a serem divisores do número 2793, pois são primos p tais que $p^2 \leqslant 2793$. Efetuando divisões euclidianas, afim de observar algum resto igual a 0, seria interessante solicitar que comecem pelos primos menores. Não demorará muito tempo até que percebam que $2793 = 3 \cdot 931$. Logo 2793 é composto, e a resposta a pergunta inicial, é que o número 2793 não é primo. Sabendo que 2793 é composto, o aluno agora terá que exibir a fatoração em potências de números primos. Já sabemos que um dos fatores primos de 2793 é 3, uma pergunta que o aluno pode ser instigado a fazer é: será que 931 é primo? Se tivermos uma resposta positiva a esse questionamento a fatoração de 2793 estará completa. Para responder a essa pergunta ele deve novamente notar que os números primos 2, 3, 5, 7, 11, 13, 17, 19, 23 e 29 são candidatos a serem divisores de 931, pois são números primos p tais que $p^2 \leqslant 931$. Após mais alguns cálculos conseguirão notar que $931 = 7 \cdot 133$, e portanto 931 é composto. Agora temos que $2793 = 3 \cdot 7 \cdot 133$, e novamente o aluno é instigado a se questionar sobre a primalidade de 133, sendo a cada passo, a lista de números primos candidatos a divisores, um pouco menor. Se 133 for composto, algum(s) dos primos 2, 3, 5, 7 ou 11 irão dividi-lo. Mais alguns cálculos mostram que $133 = 7 \cdot 19$, e agora ambos os fatores são, com certeza, números primos que estão na lista, e a fatoração de 2793 agora está completa. Os passos podem ser resumidos no seguinte esquema:

$$2793 = 3 \cdot 931 = 3 \cdot 7 \cdot 133 = 3 \cdot 7 \cdot 7 \cdot 19 = 3 \cdot 7^2 \cdot 19.$$

As atividades dessa quarta etapa da situação de aprendizagem escancaram a dificuldade que temos em determinar a primalidade de números naturais suficientemente grandes e, mais ainda, de exibir a fatoração completa desses números em um produto de potências de números primos, caso forem compostos. Para minimizar esse problema, propomos, na próxima etapa da situação de aprendizagem, um trabalho de fatoração de números naturais em equipe.

3.2.5 Etapa 5: O jogo da fatoração simultânea.

Para o desenvolvimento da quinta etapa da situação de aprendizagem, faremos uso de estratégias pedagógicas ligadas a aulas, que utilizam de um jogo com conexão significativa junto ao conteúdo escolhido. Tal jogo, onde aborda o problema da determinação da primalidade e da fatoração de um número natural coletivamente. Os estudantes terão participação direta nos objetivos do jogo, e o trabalho em equipe e o protagonismo serão de relevada importância. Acreditamos que 4 aulas serão suficientes para explicar as regras do jogo e jogá-lo efetivamente.

Num primeiro momento, a turma será dividida em duas equipes de no máximo 25 alunos. O número de 25 integrantes foi colocado, de modo a aproveitar ao máximo a lista dos 25 primeiros números primos, encontrados com a aplicação do Crivo de Eratóstenes. Um dos objetivos da situação de aprendizagem é que os alunos se familiarizem com os 25 primeiros números primos, portanto, mesmo que tenha-se menos alunos, seria interessante manter a quantidade de primos. Os alunos devem ter em mãos seus materias básicos como folhas para rascunho, além de lápis e borracha.

Cada integrante de uma equipe recebe um ou mais cartões contendo números primos diferentes dos demais companheiros. São distribuídos os mesmos números primos para cada equipe, e a quantidade de números primos distribuídos, depende do número de participantes. Se tivermos uma quantidade ímpar de alunos, pode-se solicitar, por exemplo, que um integrante de uma das equipes fique com um cartão a mais do que seus companheiros. O importante é que as equipes possuam os mesmos números primos, podendo ser feitas alterações nas quantidades que cada integrante receberá, haja visto, que as turmas podem possuir quantidades bem diferentes de alunos.

Após receberem os primeiros cartões, os alunos receberão uma folha contendo uma tabela. A quantidade de tabelas recebidas é igual a quantidade de números primos que o aluno recebeu. Na primeira coluna dessa tabela é solicitado que os estudantes calculem o quadrado do(s) número(s) primo(s) que eles receberam, e preencha os espaços reservados

com o resultado obtido. A segunda coluna indica a desigualdade que será colocada, e todos terão esta coluna preenchida com o símbolo $\leqslant$ (menor ou igual que). A terceira coluna, deve ser preenchida gradativamente, uma linha por vez, de acordo com números que são ditos pelo professor, e que serão os objetos de investigação com relação a primalidade ou composição. Por fim, a quarta e última coluna, solicita que o aluno analise o valor lógico da desigualdade montada nas três colunas anteriores, da linha em que pertence o número a ser testado, respondendo verdadeiro ou falso. Apenas uma resposta verdadeira, vai permitir que o aluno de fato, teste se algum ou alguns de seus números primos dividem o número da rodada. Depois do preenchimento da primeira coluna, por todos os alunos, a disputa de fato pode começar a acontecer.

Supondo que um determinado aluno recebeu o número primo 37. Inicialmente ele calculará $37^2 = 1369$ e completará toda a primeira coluna com esse número. Suponha também que o professor precisou enunciar, seguidamente, os números 983, 1111, 1521, 1631, 1833, 2003, 223, 811, 337 e 1991, até que o jogo fosse terminado. O aluno que recebeu o número primo 37, participou diretamente, testando o número dito pelo professor, em cinco jogadas, que correspondem as respostas verdadeiras ($1369 \leqslant 1521$, $1369 \leqslant 1631$, $1369 \leqslant 1833$, $1369 \leqslant 2003$, $1369 \leqslant 1991$), dadas às desigualdades. Um possível esboço do completamento dessa tabela, é apresentado a seguir.

Tabela 3.1: Controle de entradas do jogo.

Quadrado do Primo	Desigualdade	Número a ser testado	Verdadeiro (v) ou falso (f)
1369	$\leqslant$	983	F
1369	$\leqslant$	1111	F
1369	$\leqslant$	1521	V
1369	$\leqslant$	1631	V
1369	$\leqslant$	1833	V
1369	$\leqslant$	2003	V
1369	$\leqslant$	223	F
1369	$\leqslant$	811	F
1369	$\leqslant$	337	F
1369	$\leqslant$	1991	V

O jogo tem o seguinte funcionamento: Vamos supor que as equipes sejam denominadas equipe A e equipe B. Cada equipe tem a sua vez de jogar, e uma equipe só começa a jogar quando a outra terminar o seu jogo. Por exemplo se A começou a partida, B só irá jogar quando A terminar. As equipes são representadas por objetos simples, que se deslocam em um tabuleiro com um determinado número de casas. Vence o jogo a equipe que conseguir chegar na casa final do tabuleiro, no menor tempo possível. Ambas necessitam terminar o percurso, independente do tempo gasto. O tempo é cronometrado pelo professor e marcado em local visível (quadro) ao final do percurso de cada equipe.

O objetivo pedagógico do jogo, é utilizar o trabalho em equipe, para agilizar a fatoração de um número natural em potências de números primos, e ao mesmo tempo, utilizar esse processo para avançar nas casas do tabuleiro, afim de vencer o jogo. Assim sendo, os alunos trabalharão com essa fatoração, sob o ponto de vista, de observar se o número falado pelo professor é primo ou composto. Vamos supor que o professor tenha escolhido um número n. Obviamente, o professor deve escolher um número que seja adequado com as condições iniciais da distribuição de números primos aos seus alunos, e que apresente dificuldades semelhantes às duas equipes.

Os alunos completarão o primeiro espaço, na terceira coluna da tabela recebida anteriormente, com o valor desse número n. Se a primeira desigualdade formada na tabela for verdadeira o aluno verificará se o número primo que ele recebeu divide o número n (caso seja falsa, ele não precisa fazer nada, pois haverá um número primo menor do que o dele, que é um possível fator de n), sendo assim, cada estudante tem seu papel fundamental na equipe. No contexto do estudante, cujo quadrado do número primo recebido, ultrapassa o número n a ser testado (a desigualdade é falsa), pensando no trabalho em equipe e no bem comum, pode-se solicitar que ele escolha um número primo recebido por um companheiro de time, e faça também a divisão euclidiana de responsabilidade do colega, porém sem que ele saiba.

O cronômetro é iniciado assim que o professor termina de dizer o número n, e pode ser interrompido a qualquer momento pelos alunos. Se n for primo, o crônometro não será interrompido, até que todos tenham verificado e se manifestado confirmando que nenhum dos

números primos da equipe o divide. Logo sua fatoração estará completa fazendo com que a peça no tabuleiro avance uma casa, e o professor diga outro número que deve ser colocado na segundo espaço da terceira coluna, para que o jogo recomece.

Caso o número n seja composto, algum número primo recebido pelos alunos, irá dividi-lo, ou seja, tal número primo será um fator de n, e o aluno deve se manifestar imediatamente, confirmando a composição de n. A cada vez que se encontra um fator do número n, o cronômetro é parado, e a peça da equipe avança uma casa. Nesse momento, o jogo recomeça, com a inserção do número resultante, após encontrarmos um fator de n, no seu devido espaço na terceira coluna da tabela, para investigação de sua primalidade. Após um número finito de passos, os alunos encontram a fatoração completa de n, obrigando o professor a escolher um novo número a ser testado.

É importante que se diga, que podem aparecer números compostos que possuem mais de um fator do mesmo número primo, ou seja, um aluno com tal número primo, poderá participar mais de uma vez do processo de fatoração. Em todo o caso, ao afirmar que um número é composto, a atenção ao quociente obtido também torna-se fundamental para o desenvolvimento do jogo. Depois de desenvolvida a quinta etapa da situação de aprendizagem, a expectativa é a de que os estudantes tenham compreendido a ideia do teorema fundamental da aritmética, e a realizar a fatoração de números naturais em potências de números primos.

3.2.6 Etapa 6: A Fatoração como ferramenta para o cálculo de mdc e mmc.

Na sexta etapa da situação de aprendizagem, iremos mostrar como utilizar o conhecimento adquirido para trabalhar com questões, em que os alunos tenham que encontrar divisores e múltiplos de um número natural, máximo divisor comum e mínimo múltiplo comum entre dois ou mais números naturais, porém agora, utilizando a fatoração dos números apresentados. Acreditamos que a exposição do conteúdo e a aplicação e discussão de tais questões necessitam de 4 aulas para serem desenvolvidas. As questões podem ser semelhantes ou até as mesmas

trabalhadas na segunda etapa, haja visto, que agora os alunos possuem os resultados e podem comparar com o novo método de resolução apresentado, pode-se trabalhar novamente com questões do tipo:

1. Quem são os divisores do número 28 e do número 30? Existem divisores comuns entre 28 e 30? Qual deles é o maior? E qual é o menor?

   Agora, nessa etapa, ao se depararem com a primeira pergunta, espera-se que os alunos percebam que a fatoração dos números 28 e 30 fornece um caminho para encontrar os divisores desses números, fazendo os expoentes das potências dos primos dessas fatorações, variarem de 0 até o expoente encontrado. Uma forma de resolução, pode ser apresentada da seguinte maneira.

   Como $28 = 2^2 \cdot 7$, os divisores de 28 podem ser obtidos fazendo

   $2^0 \cdot 7^0 = 1 \cdot 1 = 1$,

   $2^1 \cdot 7^0 = 2 \cdot 1 = 2$,

   $2^2 \cdot 7^0 = 4 \cdot 1 = 4$,

   $2^0 \cdot 7^1 = 1 \cdot 7 = 7$,

   $2^1 \cdot 7^1 = 2 \cdot 7 = 14$,

   $2^2 \cdot 7^1 = 4 \cdot 7 = 28$,

   e portanto, os divisores de 28 são 1, 2, 4, 7, 14 e 28.

   Analogamente, como $30 = 2 \cdot 3 \cdot 5$, os divisores de 30 podem ser obtidos fazendo

   $2^0 \cdot 3^0 \cdot 5^0 = 1 \cdot 1 \cdot 1 = 1$,

   $2^1 \cdot 3^0 \cdot 5^0 = 2 \cdot 1 \cdot 1 = 2$,

   $2^0 \cdot 3^1 \cdot 5^0 = 1 \cdot 3 \cdot 1 = 3$,

   $2^0 \cdot 3^0 \cdot 5^1 = 1 \cdot 1 \cdot 5 = 5$,

   $2^1 \cdot 3^1 \cdot 5^0 = 2 \cdot 3 \cdot 1 = 6$,

   $2^1 \cdot 3^0 \cdot 5^1 = 2 \cdot 1 \cdot 5 = 10$,

$2^0 \cdot 3^1 \cdot 5^1 = 1 \cdot 3 \cdot 5 = 15$,

$2^1 \cdot 3^1 \cdot 5^1 = 2 \cdot 3 \cdot 5 = 30$,

e portanto, os divisores de 30 são 1, 2, 3, 5, 6, 10, 15 e 30.

Para a segunda pergunta, sobre os divisores comuns, o aluno pode proceder da mesma maneira que anteriormente, observando as duas listas encontradas e confirmando que 1 e 2 são divisores comuns de 28 e 30. Para a terceira pergunta, sobre qual o mdc de 28 e 30, espera-se que os alunos, ao compararem os números $28 = 2^2 \cdot 7$ e $30 = 2 \cdot 3 \cdot 5$, percebam que $(28, 30) = 2$, pois é um divisor comum de ambos, além de ser divisível pelo outro único divisor comum entre eles, que é o 1. Pode-se também observar a forma fatorada desses números, e perceber que o fator 2 é o único presente em ambas. E finalmente, para a última questão, o aluno deve notar, que sendo 1 elemento neutro da multiplicação, ele sempre será o menor divisor comum entre dois números naturais quaisquer, pois todo número natural n pode ser representado como $n = 1 \cdot n$.

2. Existem múltiplos comuns entre os números 36 e 48? E entre os números 15 e 200? Se sim, qual deles é o mínimo múltiplo comum desse números?

   Baseados na ideia da fatoração, os alunos devem escrever $36 = 2^2 \cdot 3^2$ e $48 = 2^4 \cdot 3$ e notar que o menor múltiplo comum deve ser um múltiplo comum de ambos os números, com a propriedade extra de dividir qualquer um dos outros múltiplos comuns de 36 e 48. Tal múltiplo mínimo é dado por $2^4 \cdot 3^2 = 144$, podendo ser indicado como $[36, 48] = 144$. Sendo assim todos os outros múltiplos comuns de 36 e 48 são da forma $2^m \cdot 3^n$, com $m, n \in \mathbb{N}$ e $m \geqslant 4$ e $n \geqslant 2$. Analogamente, ao escrever $15 = 3 \cdot 5$ e $200 = 2^3 \cdot 5^2$ percebam que o mínimo múltiplo comum de 15 e 200 é dado por $2^3 \cdot 3 \cdot 5^2 = 600$, representando também por $[15, 200] = 600$, para enfim concluir, que os múltiplos comuns de 15 e 200 são da forma $2^l \cdot 3^m \cdot 5^n$, com $l, m, n \in \mathbb{N}$ e $l \geqslant 3$, $m \geqslant 1$ e $n \geqslant 2$.

Trabalhada mais essa etapa, esperamos que as habilidades EF06MA05 e EF06MA06 estejam se desenvolvendo de maneira satisfatória, ou seja, a esta altura, esperamos que os

alunos já consigam classificar os números naturais em primos e compostos, que tenham entendido as relações expressas pelas ideias de divisibilidade e ainda, sejam capazes de escrever um número natural na forma fatorada, utilizando seus fatores primos.

3.2.7 Etapa 7: Problemas que envolvem as ideias de mdc e mmc.

É chegada a hora da sétima e última etapa da situação de aprendizagem, trabalharemos com as aplicações direta desses conceitos, em situações do cotidiano, no intuito de desenvolver um pouco mais da habilidade EF06MA06 e começar a trabalhar com a habilidade EF07MA01. O aluno será convidado, a mobilizar os conhecimentos adquiridos para enfrentar e desenvolver situações problema, envolvendo diretamente os conceitos estudados. Acreditamos que sejam necessárias 6 aulas para o desenvolvimento dessa etapa e sugerimos trabalhar problemas do tipo:

1. Ricardo se acidentou e trincou sua costela esquerda. Ao ser atendido na unidade de saúde de seu bairro, o Doutor Gonzalez lhe receitou duas medicações que devem ser tomadas durante quinze dias consecutivos. A primeira delas, deve ser ingerida de 6 em 6 horas, enquanto que a outra de 8 em 8 horas. Ricardo tomou ambas juntas, as 12:00 horas do mesmo dia, e se questionou se haveria algum horário em que teria que tomá-las juntas novamente. Caso houvesse tal horário, Ricardo gostaria de saber quantas horas terão que passar, para que tal horário chegue. Você consegue ajudar Ricardo nessa missão?

   Inicialmente, ao ler com bastante cuidado e se colocar dentro da situação problema, é provável que o aluno perceba que a ideia de *algo comum* está embutida na questão, pois Ricardo tomou as medicações juntas em um determinado horário, e quer saber se tomará as medicações juntas novamente. Caso consiga encontrar o horário em que tomará as medicações juntas simultaneamente, Ricardo sabe que essa ação ocorrerá novamente, nos dias subsequentes. Assim Ricardo deve encontrar um intervalo de tempo comum entre 6 e 8 horas, além de ser o menor possível. Logo, o intervalo procurado por Ricardo,

em horas, é dado pelo menor múltiplo comum entre os números 6 e 8. A resposta a essa pergunta poderia ser dada, simplesmente criando-se uma tabela e marcando os horários de cada medicação tomada, observando em qual horário comum, ambas as medicações seriam tomadas juntas. No entanto com a ajuda da fatoração, o aluno escreve $6 = 2 \cdot 3$ e $8 = 2^3$, logo $[6, 8] = 2^3 \cdot 3 = 24$, e portanto depois de 24 horas, as medicações serão tomadas juntas novamente, correspondendo portanto as 12:00 do dia seguinte.

2. Mônica possui um terreno retangular de medidas, em metros, dadas por 720 x 540, e que será dividido em lotes quadrados. Tais lotes precisam ter o lado de maior comprimento possível, gerando assim uma área máxima para cada um deles. Mônica, precisa da sua ajuda para resolver esse problema, pois precisa descobrir qual deve ser essa medida do lado de comprimento máximo e em quantos lotes quadrados ela conseguirá dividir o seu terreno.

   Novamente, nessa questão, a ideia de algo comum se faz presente. Como os lotes formados devem ser quadrados, e um quadrado possui lados de mesma medida, Mônica precisa de uma medida comum aos lados do retângulo, e tal que divida 720 e 540 simultaneamente, de modo a aproveitar o máximo possível da área do seu terreno. Se tais medidas, possuírem o comprimento dado pelos divisores comuns de 720 e 540, conseguiremos formar lotes quadrados, mas não necessariamente de área máxima. Por exemplo, o número 1 é um divisor comum de 720 e 540, logo se os lados do terreno, que medem 720 metros, forem divididos em 720 medidas de comprimento 1 metro, e os lados que medem 540, forem divididos em 540 medidas de comprimento 1 metro, teremos toda a área do terreno coberta, e um total de 388800 lotes quadrados de $1\mathrm{m}^2$ de área. Analogamente, o número 2 é um divisor comum de 720 e 540, e se tais lados forem divididos em 360 e 270 medidas, cujo comprimento é 2 metros, teremos 97200 lotes quadrados de $4\mathrm{m}^2$ de área. Assim sendo, além do comprimento da medida ser um divisor comum, ela deve ter o comprimento máximo, nos levando a ideia do máximo divisor comum de 720 e 540. Utilizando a fatoração, o aluno escreve $720 = 2^4 \cdot 3^2 \cdot 5$ e $540 = 2^2 \cdot 3^3 \cdot 5$, e constata que $(720, 540) = 2^2 \cdot 3^2 \cdot 5 = 180$, sendo este o comprimento

do lado solicitado. Portanto, os lados do terreno que medem 720 metros, foram divididos em quatro medidas de 180 metros, e os lados medindo 540 metros, foram divididos em três medidas de 180 metros, formando assim, 12 lotes quadrados de $32400\mathrm{m}^2$ de área, cujo comprimento do lado é 180 metros.

3. O pai de Roberto, está comprando pão e salsicha para fazer cachorro quente. As salsichas vêm em pacotes de 12 unidades, enquanto que os pães vêm em pacotes de 9 unidades. A loja não vende produtos avulsos, e o pai de Roberto deseja a mesma quantidade de salsichas e pães. Ajude o pai de Roberto a descobrir qual o menor número total de salsichas e pães que ele pode comprar.

   Como de praxe, a ideia de algo comum se faz presente, quando o pai de Roberto deseja comprar a mesma quantidade de salsichas e pães. Como as quantidades de salsicha são números múltiplos de 12, e a quantidade de pães são números múltiplos de 9, a quantidade mínima de salsichas e pães compradas se dará no mínimo múltiplo comum de 9 e 12. Utilizando a fatoração de naturais em potências de primos o aluno pode escrever $9 = 3^2$ e $12 = 2^2 \cdot 3$, constatando que $[9, 12] = 2^2 \cdot 3^2 = 36$. Logo, o pai de Roberto deverá comprar, no mínimo, 36 salsichas.

4. Brigite recebeu dois presentes do seu avô. O primeiro presente é um pacote com 18 cookies, e o segundo presente é uma caixa com 12 chocolates. Brigite quer usar todos os cookies e todos os chocolates para preparar sacos de lanche idênticos para levar para a escola. Ajude Brigite a descobrir qual o maior número de sacos de lanche que ela pode preparar. E descreva o que deve conter em cada um dos sacos.

   O fato de Brigite desejar montar sacos de lanche idênticos, nos traz a tona a ideia de algo comum. Portanto, a quantidade de sacos formados deve ser um divisor comum de 18 e 12. Por exemplo, como ambos são pares, o número 2 é um divisor comum de 18 e 12, e assim seriam formados dois sacos com 15 objetos (9 cookies e 6 chocolates). Todavia, o problema nos diz que Brigite quer descobrir qual o maior número de sacos de lanche idênticos que ela pode preparar, nos levando a ideia de que além de ser um divisor comum, ele deve ser o maior deles, ou seja, o máximo divisor comum de 18 e 12.

Pela fatoração, temos que $18 = 2 \cdot 3^2$ e $12 = 2^2 \cdot 3$, nos dando que $(12, 18) = 2 \cdot 3 = 6$. Logo, Brigite conseguirá montar 6 pacotes idênticos de lanche, contendo cada um, 5 objetos (3 cookies e 2 chocolates).

5. Gustavo e Leandro estão em classes diferentes. O professor de Matemática de Gustavo sempre dá provas com 26 perguntas, enquanto que o professor de Matemática de Leandro dá provas mais frequentes com 18 perguntas. Embora as duas classes tenham que fazer um número diferente de provas seus professores disseram aos alunos que as duas classes responderão o mesmo número de perguntas a cada ano. Qual é o número mínimo de perguntas que a classe de Gustavo ou de Leandro pode esperar responder em um ano?

   A condição de Gustavo e Leandro responderem o mesmo número de perguntas a cada ano, nos remete a algo comum entre ambos. E o questionamento de ser o número mínimo de questões que ambos esperam responder, nos leva a confirmar que a resposta se dará no mínimo múltiplo comum entre 18 e 26. Utilizando a fatoração, tem-se $18 = 2 \cdot 3^2$ e $26 = 2 \cdot 13$. Sendo assim $[18, 26] = 2 \cdot 3^2 \cdot 13 = 234$. Portanto, o número mínimo de perguntas que a classe de Gustavo ou Leandro pode esperar responder em um ano é 234.

Ainda, no contexto da sétima etapa da situação de aprendizagem, ao final da discussão e exposição dos exercícios, pode-se solicitar que os estudantes criem suas próprias situações problema, envolvendo os conteúdos estudados, e troquem entre eles, para que os outros colegas também possam ter acesso.

Em cada uma das etapas que foram apresentadas, a avaliação dos estudantes se dará de forma contínua, considerando seu envolvimento, participação e produção das atividades desenvolvidas. Ao final de cada uma das etapas, pode-se também solicitar atividades para serem realizadas em casa, bem como um pequeno relato contendo as opiniões dos mesmos sobre o andamento da etapa. As atividades e suas opiniões sobre cada etapa, deverão ser entregues no início da próxima aula. Tais atividades devem ser corrigidas, comentadas e devolvidas aos alunos posteriormente. A tabela abaixo, ilustra o desenvolvimento completo da

situação de aprendizagem.

Tabela 3.2: Cronograma da situação de aprendizagem.

Etapas	Conteúdos	Tempo Estimado
Etapa 1	Retomada e Noções de Divisibilidade	4 aulas
Etapa 2	Múltiplos, Divisores, mdc e mmc	4 aulas
Etapa 3	Compostos ou Primos, Crivo de Eratóstenes e $p^2 \leqslant n$	6 aulas
Etapa 4	Teorema Fundamental da Aritmética	4 aulas
Etapa 5	Jogo	4 aulas
Etapa 6	Divisores, múltiplos, mmc e mdc com fatoração	4 aulas
Etapa 7	Problemas com mmc e mdc	6 aulas

Após a aplicação completa da situação de aprendizagem, com o intuito de avaliarmos o desenvolvimento das habilidades citadas nos estudantes, além de fazermos a análise *a posteriori* dos resultados, com o objetivo de aperfeiçoarmos a proposta, deixamos como sugestão, uma atividade avaliativa que pode ser encontrada nos apêndices, e que está fundamentada no material disponível á todos os alunos da rede.

4 Considerações finais

É chegada a hora em que uma auto avaliação do trabalho feito se faz necessária. Inicialmente, cabe-nos recordar que com a construção dessa dissertação, o leitor pudesse ter contato direto com aspectos puros e práticos ao se trabalhar com o problema de se determinar a primalidade de um número inteiro. Tal trabalho foi construído para mostrar como tal problema foi sendo trabalhado e discutido pela comunidade científica com o desenvolvimento de ferramentas matemáticas mais sofisticadas, bem como para apresentar uma proposta de situação de aprendizagem, onde os estudantes, ao atacarem o problema fazendo uso da fatoração, possam ser instigados a entender que fatorar um número inteiro, mesmo quando essa tarefa não lhe for trivial, pode ajudá-lo a resolver alguns outros problemas que lhe serão apresentados no decorrer do seu percurso escolar.

Para tanto, inicialmente temos um capítulo onde algumas propriedades e definições do conjunto dos números inteiros são exploradas. Acreditamos que, com o estudo desse capítulo, o leitor certamente poderá obter alguma ideia sobre tais propriedades e definições, mas certamente o capítulo deixa uma sensação de vazio, quando estudado por matemáticos melhor embasados, pois é notável que a falta de demonstração de alguns resultados causa uma certa estranheza. Apesar dessas falhas, há alguns resultados bem interessantes, principalmente sobre critérios de divisibilidade e o famoso Teorema Fundamental da Aritmética.

Ao avançarmos um pouco mais na leitura, encontramos uma parte destinada a analisar alguns dos muitos testes para se determinar quando um número inteiro será composto ou primo. A essa altura, apesar de novamente não estar formalizado como deveria, com todo o rigor matemático necessário, tem-se a impressão que o objetivo principal foi parcialmente atingido. Acreditamos que a maneira como está colocada a teoria e a quantidade de exemplos de aplicação de tais testes, permitirá ao leitor, que se consiga entender o funcionamento dos

mesmos, bem como decidir qual teste usar dependendo do número a ser analisado. Aqui cabe uma observação, de que em um trabalho futuro, também queremos discutir e aplicar o funcionamento de testes de primalidade determinísticos e que são executados em tempo polinomial, tais como o teste AKS (Agrawal-Kayal-Saxena).

Continuando a leitura é chegado o momento em que se propõe a Situação de Aprendizagem. O desenvolvimento desse trabalho iniciou-se em meados de março de 2020, ano muito atípico para todos nós, em que uma terrível pandemia ceifou a vida de milhões de pessoas em todo o mundo. Esse ano, com tudo o que ocorreu, também não passou despercebido no tocante a educação. As aulas presenciais foram suspensas, e as aulas e atividades online, escancararam ainda mais a desigualdade existente em nosso país. Na escola pública estadual onde atuamos, não foi diferente, e com isso a aplicação da situação de aprendizagem não pôde ser realizada, por inúmeros motivos, o que deixou uma profunda sensação de vazio quanto aos resultados que poderiam ser alcançados, bem como hipóteses que seriam confirmadas ou refutadas, quando feita a análise dos resultados da aplicação.

Isso posto, também faz-se necessário dizer, que poderíamos ter sugerido em nossa proposta um número menor de aulas necessárias ao desenvolvimento da mesma, e até termos explorado melhor os outros testes na construção da mesma. Como exemplo pode-se usar os Números de Mersenne e seu teste de primalidade, ao trabalharmos o conceito de função exponencial com os estudantes. Do mesmo modo, pode-se apresentar o teste de Wilson, como uma aplicação extra do conceito de fatorial de um número inteiro. Todos esses detalhes, que são tão importantes, também terão espaço em futuros trabalhos que pensamos em desenvolver. Quanto aos problemas e aplicações da fatoração de um número inteiro, cabe destacar que inicialmente propomos uma situação de aprendizagem, em que tal conceito será usado apenas para cálculos de mdc e mmc, apresentando uma forma alternativa de se chegar a esses resultados, forma essa que não é apresentada nos materiais disponíveis aos alunos da rede. Nada impede por exemplo, e aliás reforça o estudo dos números primos, que o conceito da fatoração possa ser usado como um outro método para se calcular raízes n-ésimas de números reais, bem como também possa ser utilizado para o estudo de funções, representações de pontos e

construção de gráficos no plano cartesiano, com a introdução de algumas funções aritméticas conhecidas, tais como, a função que conta o número de divisores de um número inteiro e a função que soma todos os divisores de um número inteiro. Ambas, dependem da fatoração e podem ser utilizadas para se estudar tais conceitos. Nosso compromisso, é o de que, sempre que possível, possamos apresentar a fatoração aos nossos alunos, sempre iniciando com o problema da primalidade, e a utilizando para estudar o máximo de conceitos matemáticos que pudermos.

Grosso modo, pode-se dizer que os objetivos propostos com a criação da dissertação foram parcialmente atingidos. Acreditamos que o material produzido para explicar o funcionamento dos testes tem sua utilidade na exposição dos mesmos, não que seja algo que não possa ser muito melhor aperfeiçoado, porém cumpre o seu objetivo inicial. A Situação de Aprendizagem proposta fornece uma maneira de se trabalhar com o problema da primalidade sob o olhar da fatoração e ajuda a ensinar vários conceitos importantes tais como relações de divisibilidades, noções de múltiplos, divisores, mdc e mmc. Ela também se dedica a ensinar como utilizar a fatoração para encontrar o mdc e o mmc entre números inteiros, e depois utilizar esses conceitos para resolver alguns problemas do cotidiano que utilizam tal estudo, e por tal motivo cumpre parcialmente seu objetivo. Porém, a não possibilidade de aplicação, nos deixou com uma impressão de que algo muito importante ficou faltando, por isso não nos atreveríamos a dizer que tal dissertação tem os objetivos propostos plenamente desenvolvidos.

O compromisso que fazemos, é que tão logo a pandemia esteja controlada, e que as aulas voltem efetivamente de forma presencial e obrigatória,faremos com que a situação de aprendizagem seja aplicada em sua totalidade, bem como analisados todos os resultados que aparecerem. Com tais dados teremos como analisar realmente nossas hipóteses e termos melhores condições de analisar os objetivos propostos, afim de melhorarmos nossa prática docente, aperfeiçoarmos a proposta e ensinarmos com mais qualidade aos nossos alunos.

Referências Bibliográficas

[1] HEFEZ; A. *Iniciação à Aritmética*. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2012.

[2] HEFEZ; A. *Aritmética*. Sociedade Brasileira de Matemática, Rio de Janeiro, 2016.

[3] CAMINHA; A.M.N. *Fundamentos de Cálculo*. Sociedade Brasileira de Matemática, Rio de Janeiro, 2015.

[4] SAMPAIO; J.C.V e CAETANO; P.A.S. *Introdução à teoria dos números: um curso breve*. EdUFSCar, São Carlos, 2008.

[5] AGUILAR; I. e DIAS; M.S. A construção dos números reais e suas extensões. *Universidade Federal Fluminense*, 2005.

[6] LIMA; E.L. *Números e Funções Reais*. Sociedade Brasileira de Matemática, Rio de Janeiro, 2013.

[7] BRUCE; J.W. A really trivial proof of the lucas-lehmer primality test. *American Mathematical Monthly*, pages 370–371, 1993.

[8] du SAUTOY; M. *A música dos números primos*. Jorge Zahar Editor Ltda, Rio de Janeiro, 2008.

[9] RIBENBOIM; P. *Números Primos: Velhos Mistérios e Novos Recordes*. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2014.

[10] J.ROBERTSON; E. e O'CONNOR. MacTutor History of Mathematics Archive. `https://mathshistory.st-andrews.ac.uk/`, 2020. Accesso em 19-de-novembro-de-2020.

[11] SINGH; S. *O último teorema de Fermat*. Editora Record Ltda, Rio de Janeiro, 2008.

[12] COUTINHO; S.C. *Criptografia*. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2015.

[13] Coordenação SEDUC-SP. *Currículo Paulista Etapa Ensino Médio*. SEDUC-SP, São Paulo, 2020.

Avaliação da Situação de Aprendizagem.

Atividade 1 - Os Números primos -

O nome *primo* vem do latim e significa primeiro. Um número primo só é divisível por 1 e por ele mesmo. É o caso do número 53. Os números naturais que têm mais de dois divisores são chamados *números compostos*.

1. Na tabela abaixo, pinte apenas as janelas com números primos.

Tabela 1: Os quinze primeiros números primos.

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

Atividade 2 - Números Primos e Compostos

A tabela a seguir apresenta a produção de peças de uma empresa. Deverão ser embaladas em pacotes que comportam 2, 3, 4, 5, 6, 7, 9 ou 10 peças, de forma que não sobre nenhuma. Assinale na tabela a seguir, as opções para embalar as peças em cada dia.

Figura 1: Caderno do Aluno 2020, p.223

Produção de peças									
Dia	Quantidade de peças produzidas	Tamanhos de embalagens que podem ser utilizadas sem sobras para embalar as peças							
		2	3	4	5	6	7	9	10
3	38								
4	43								
5	28								
6	40								
7	39								
10	34								
11	35								
12	39								
13	43								
14	45								

1. No dia 6, quais opções de embalagem a fábrica tem para que não sobre nenhuma peça sem embalar? Indique o tamanho das embalagens.

2. Em quais dias a empresa tem somente uma opção para embalar? Qual é o tamanho dessa embalagem?

3. Em todos os dias será possível embalar as peças sem que sobre nenhuma? Explique.

4. Em quais dias a empresa usará embalagens dos tamanhos 5 e 10? Explique.

5. Em quais dias a empresa usará embalagens dos tamanhos sendo todos números ímpares?

Atividade 3 - Descobrindo os múltiplos e divisores

1. No quadro a seguir, pinte em cada linha as janelas com os divisores, conforme indicado:

Tabela 2: Tabela de Divisores.

Divisores de 4	1	2	3	4	5	6	7	8	9	10	11	12
Divisores de 6	1	2	3	4	5	6	7	8	9	10	11	12
Divisores de 12	1	2	3	4	5	6	7	8	9	10	11	12
Divisores comuns (4, 6, 12)	1	2	3	4	5	6	7	8	9	10	11	12
Maior Divisor Comum entre 4, 6 e 12	1	2	3	4	5	6	7	8	9	10	11	12

2. Leia as sentenças a seguir, assinalando V (Verdadeiro) ou F (Falso) e justificando sua resposta

   a) ( ) 50 é múltiplo de 5.

   b) ( ) 79 é divisível por 5.

   c) ( ) 4 é divisor de 25.

   d) ( ) 105 não é divisível por 8.

   e) ( ) 144 não é múltiplo de 3.

3. Encontre os dez primeiros múltiplos de 3. Descreva a estratégia que você utilizou para encontrá-los.

4. Encontre todos os divisores de 36. Descreva a estratégia que você utilizou para encontrá-los.

5. Em uma escola, há 240 alunos no 7º ano, 288 no 8º ano e 120 no 8º ano. Haverá uma semana cultural, em que todos os alunos serão distribuídos em equipes, sem que se misturem alunos de anos diferentes. Qual será o máximo de alunos que pode haver em cada equipe nessas condições?

6. Numa fábrica de retalhos sobraram algumas tiras de 90 cm e outras de 75 cm de comprimento. o patrão deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?

7. O planejamento de urbanização de uma cidade inclui a iluminação pública. Para garantir a luminosidade do ambiente de forma eficiente, segura e que não afete a mobilidade dos pedestres, a distância indicada entre os postes de iluminação é de 35 m. Em uma cidade, será construída uma avenida nova. Além dos postes, será construído um posto de atendimento aos usuários a cada 25 m. Considerando o início da avenida o ponto zero, qual será o primeiro ponto onde haverá tanto o poste de iluminação quanto o posto de atendimento?

8. Escreva os múltiplos de 18 e 24? Qual é o menor múltiplo comum entre 18 e 24?

9. Uma fonte luminosa, geralmente instalada nas praças das cidades, jorra água constantemente para o alto enquanto toca música e acende luzes coloridas. As luzes são programadas para *piscar* em tempos diferentes. Suponhamos que a luz rosa *pisque* a cada 15 segundos e a amarela *pisque* a cada 10 segundos; se num certo instante, elas *piscam* ao mesmo tempo, após quantos segundos elas voltarão a *piscar* simultaneamente?

SÃO PAULO - SP, Secretaria da Educação. São Paulo Faz Escola, Caderno do Aluno, 6º Ano. Vol. 1, 2020. p.223 e 7º Ano. Vol. 1, 2020. p.228 á 230, Matemática.

Fatoração dos Pseudoprimos na base 2 $(\mathrm{psp}(2))$

Tabela 3: Fatoração de alguns pseudoprimos na base 2

$341 = 11 \cdot 31$	$30889 = 17 \cdot 23 \cdot 79$	$121465 = 5 \cdot 17 \cdot 1429$
$561 = 3 \cdot 11 \cdot 17$	$31417 = 89 \cdot 353$	$123251 = 59 \cdot 2089$
$645 = 3 \cdot 5 \cdot 43$	$31609 = 73 \cdot 433$	$126217 = 7 \cdot 13 \cdot 19 \cdot 73$
$1105 = 5 \cdot 13 \cdot 17$	$31621 = 103 \cdot 307$	$129889 = 193 \cdot 673$
$1387 = 19 \cdot 73$	$33153 = 3 \cdot 47 \cdot 257$	$129921 = 3 \cdot 11 \cdot 31 \cdot 127$
$1729 = 7 \cdot 13 \cdot 19$	$34945 = 5 \cdot 29 \cdot 241$	$130561 = 137 \cdot 953$
$1905 = 3 \cdot 5 \cdot 127$	$35333 = 89 \cdot 397$	$137149 = 23 \cdot 67 \cdot 89$
$2047 = 23 \cdot 89$	$39865 = 5 \cdot 7 \cdot 17 \cdot 67$	$149281 = 11 \cdot 41 \cdot 331$
$2465 = 5 \cdot 17 \cdot 29$	$41041 = 7 \cdot 11 \cdot 13 \cdot 41$	$150851 = 251 \cdot 601$
$2701 = 37 \cdot 73$	$41665 = 5 \cdot 13 \cdot 641$	$154101 = 3 \cdot 31 \cdot 1657$
$2821 = 7 \cdot 13 \cdot 31$	$42799 = 137 \cdot 337$	$157641 = 3 \cdot 11 \cdot 17 \cdot 281$
$3277 = 29 \cdot 113$	$46657 = 13 \cdot 37 \cdot 97$	$158369 = 29 \cdot 43 \cdot 127$
$4033 = 37 \cdot 109$	$49141 = 157 \cdot 313$	$162193 = 241 \cdot 673$
$4369 = 17 \cdot 257$	$52633 = 7 \cdot 73 \cdot 103$	$164737 = 257 \cdot 641$
$4371 = 3 \cdot 31 \cdot 47$	$55245 = 3 \cdot 5 \cdot 29 \cdot 127$	$172081 = 7 \cdot 13 \cdot 31 \cdot 61$
$4681 = 31 \cdot 151$	$57421 = 7 \cdot 13 \cdot 631$	$176149 = 19 \cdot 73 \cdot 127$
$5461 = 43 \cdot 123$	$60701 = 101 \cdot 601$	$181901 = 101 \cdot 1801$
$6601 = 7 \cdot 23 \cdot 41$	$60787 = 89 \cdot 683$	$188057 = 89 \cdot 2113$
$7957 = 73 \cdot 109$	$62745 = 3 \cdot 5 \cdot 47 \cdot 89$	$188461 = 7 \cdot 13 \cdot 19 \cdot 109$
$8321 = 53 \cdot 157$	$63973 = 7 \cdot 13 \cdot 19 \cdot 37$	$194221 = 167 \cdot 1163$
$8481 = 7 \cdot 19 \cdot 67$	$65077 = 59 \cdot 1103$	$196021 = 7 \cdot 41 \cdot 683$
$8911 = 7 \cdot 19 \cdot 67$	$65281 = 97 \cdot 673$	$196093 = 157 \cdot 1249$
$10261 = 31 \cdot 331$	$68101 = 11 \cdot 41 \cdot 151$	$204001 = 7 \cdot 151 \cdot 193$
$10585 = 5 \cdot 29 \cdot 73$	$72885 = 3 \cdot 5 \cdot 43 \cdot 113$	$206601 = 3 \cdot 17 \cdot 4051$
$11305 = 5 \cdot 7 \cdot 17 \cdot 19$	$74665 = 5 \cdot 109 \cdot 137$	$208465 = 5 \cdot 173 \cdot 241$
$12801 = 3 \cdot 17 \cdot 251$	$75361 = 11 \cdot 13 \cdot 17 \cdot 31$	$212421 = 3 \cdot 11 \cdot 41 \cdot 157$

$13741 = 7 \cdot 13 \cdot 151$	$80581 = 61 \cdot 1321$	$215265 = 3 \cdot 5 \cdot 113 \cdot 127$
$13747 = 59 \cdot 233$	$83333 = 167 \cdot 499$	$215749 = 79 \cdot 2731$
$13981 = 11 \cdot 31 \cdot 41$	$83665 = 5 \cdot 29 \cdot 577$	$219781 = 271 \cdot 811$
$14491 = 43 \cdot 337$	$85489 = 53 \cdot 1613$	$220729 = 103 \cdot 2143$
$15709 = 23 \cdot 683$	$87249 = 3 \cdot 127 \cdot 229$	$223345 = 5 \cdot 19 \cdot 2351$
$15841 = 7 \cdot 31 \cdot 73$	$88357 = 149 \cdot 593$	$226801 = 337 \cdot 673$
$16705 = 5 \cdot 13 \cdot 257$	$88561 = 11 \cdot 83 \cdot 97$	$228241 = 13 \cdot 97 \cdot 181$
$18705 = 3 \cdot 5 \cdot 29 \cdot 43$	$90751 = 151 \cdot 601$	$233017 = 43 \cdot 5419$
$18721 = 97 \cdot 193$	$91001 = 17 \cdot 53 \cdot 101$	$241001 = 401 \cdot 601$
$19951 = 71 \cdot 281$	$93961 = 7 \cdot 31 \cdot 433$	$249841 = 433 \cdot 577$
$23001 = 3 \cdot 11 \cdot 17 \cdot 41$	$101101 = 7 \cdot 11 \cdot 13 \cdot 101$	$252601 = 41 \cdot 61 \cdot 101$
$23337 = 3^2 \cdot 2593$	$104653 = 229 \cdot 457$	$253241 = 157 \cdot 1613$
$25761 = 3 \cdot 31 \cdot 277$	$107185 = 3 \cdot 5 \cdot 2393$	$256999 = 233 \cdot 1103$
$29341 = 13 \cdot 37 \cdot 61$	$113201 = 11 \cdot 41 \cdot 251$	$258511 = 11 \cdot 71 \cdot 331$
$30121 = 7 \cdot 13 \cdot 331$	$115921 = 13 \cdot 37 \cdot 241$	$264773 = 149 \cdot 1777$

Fatoração dos Pseudoprimos na base 2 $(\mathrm{psp}(2))$

Tabela 4: Fatoração de outros pseudoprimos na base 2

$266305 = 5 \cdot 13 \cdot 17 \cdot 241$	$481573 = 337 \cdot 1429$	$710533 = 487 \cdot 1459$
$271951 = 151 \cdot 801 \cdot 17$	$486737 = 233 \cdot 2089$	$711361 = 7 \cdot 151 \cdot 673$
$272251 = 7 \cdot 19 \cdot 23 \cdot 89$	$488881 = 37 \cdot 73 \cdot 181$	$721801 = 601 \cdot 1201$
$275887 = 263 \cdot 1049$	$489997 = 157 \cdot 3121$	$722201 = 401 \cdot 1801$
$276013 = 19 \cdot 73 \cdot 199$	$493885 = 5 \cdot 7 \cdot 103 \cdot 137$	$722261 = 491 \cdot 1471$
$278545 = 5 \cdot 17 \cdot 29 \cdot 113$	$512461 = 31 \cdot 61 \cdot 271$	$729061 = 349 \cdot 2089$
$280601 = 277 \cdot 1013$	$513629 = 293 \cdot 1753$	$738541 = 67 \cdot 73 \cdot 151$
$282133 = 307 \cdot 919$	$514447 = 359 \cdot 1433$	$741751 = 431 \cdot 1721$
$284581 = 11 \cdot 41 \cdot 631$	$526593 = 3 \cdot 257 \cdot 683$	$742813 = 223 \cdot 3331$
$285541 = 31 \cdot 61 \cdot 151$	$530881 = 13 \cdot 97 \cdot 421$	$743665 = 3 \cdot 31 \cdot 1657$
$289941 = 3 \cdot 127 \cdot 761$	$534061 = 11 \cdot 47 \cdot 1033$	$743665 = 5 \cdot 13 \cdot 17 \cdot 673$
$294409 = 37 \cdot 73 \cdot 109$	$552721 = 13 \cdot 17 \cdot 41 \cdot 61$	$745889 = 353 \cdot 2113$
$294721 = 103 \cdot 2857$	$556169 = 457 \cdot 1217$	$748657 = 7 \cdot 13 \cdot 19 \cdot 433$
$314821 = 13 \cdot 61 \cdot 397$	$563473 = 37 \cdot 97 \cdot 157$	$757945 = 5 \cdot 17 \cdot 37 \cdot 241$
$318361 = 241 \cdot 1321$	$574561 = 13 \cdot 193 \cdot 229$	$769757 = 227 \cdot 3391$
$323713 = 13 \cdot 37 \cdot 673$	$574861 = 7 \cdot 41 \cdot 2003$	$786961 = 7 \cdot 19 \cdot 61 \cdot 97$
$332949 = 3 \cdot 29 \cdot 43 \cdot 89$	$580337 = 499 \cdot 1163$	$800605 = 5 \cdot 13 \cdot 109 \cdot 113$
$334153 = 19 \cdot 43 \cdot 409$	$582289 = 113 \cdot 5153$	$818201 = 101 \cdot 8101$
$340561 = 13 \cdot 17 \cdot 23 \cdot 67$	$587861 = 443 \cdot 1327$	$825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
$341497 = 13 \cdot 109 \cdot 241$	$588745 = 5 \cdot 73 \cdot 1613$	$831405 = 3 \cdot 5 \cdot 43 \cdot 1289$
$348161 = 11 \cdot 31 \cdot 1021$	$604117 = 389 \cdot 1553$	$838201 = 7 \cdot 13 \cdot 61 \cdot 151$
$357761 = 131 \cdot 2731$	$611701 = 151 \cdot 4051$	$838861 = 397 \cdot 2113$
$367081 = 11 \cdot 13 \cdot 17 \cdot 151$	$617093 = 43 \cdot 113 \cdot 127$	$841681 = 19 \cdot 31 \cdot 1429$
$387731 = 43 \cdot 71 \cdot 127$	$622909 = 7 \cdot 23 \cdot 53 \cdot 73$	$847261 = 31 \cdot 151 \cdot 181$
$390937 = 313 \cdot 1249$	$625921 = 31 \cdot 61 \cdot 331$	$852481 = 7 \cdot 193 \cdot 631$
$396271 = 223 \cdot 1777$	$635401 = 13 \cdot 37 \cdot 1321$	$852841 = 11 \cdot 31 \cdot 41 \cdot 61$

$399001 = 31 \cdot 61 \cdot 211$
$401401 = 7 \cdot 11 \cdot 13 \cdot 401$
$410041 = 41 \cdot 73 \cdot 137$
$422659 = 163 \cdot 2593$
$423793 = 17 \cdot 97 \cdot 257$
$427233 = 3 \cdot 53 \cdot 2687$
$435671 = 191 \cdot 2281$
$443719 = 167 \cdot 2657$
$448921 = 11 \cdot 37 \cdot 1103$
$449065 = 5 \cdot 19 \cdot 29 \cdot 163$
$451905 = 3 \cdot 5 \cdot 47 \cdot 641$
$452051 = 251 \cdot 1801$
$458989 = 277 \cdot 1657$
$464185 = 5 \cdot 17 \cdot 43 \cdot 127$
$476971 = 11 \cdot 131 \cdot 331$
$642001 = 401 \cdot 1601$
$647089 = 79 \cdot 8191$
$653333 = 467 \cdot 1399$
$656601 = 3 \cdot 11 \cdot 101 \cdot 197$
$657901 = 307 \cdot 2143$
$658801 = 11 \cdot 13 \cdot 17 \cdot 271$
$665281 = 577 \cdot 1153$
$665333 = 283 \cdot 2351$
$665401 = 11 \cdot 241 \cdot 251$
$670033 = 7 \cdot 13 \cdot 37 \cdot 199$
$672487 = 103 \cdot 6529$
$679729 = 337 \cdot 2017$
$680627 = 107 \cdot 6361$
$683761 = 13 \cdot 149 \cdot 353$
$688213 = 127 \cdot 1419$
$873181 = 661 \cdot 1321$
$875161 = 7 \cdot 31 \cdot 37 \cdot 109$
$877099 = 307 \cdot 2857$
$898705 = 5 \cdot 17 \cdot 97 \cdot 109$
$915981 = 3 \cdot 11 \cdot 41 \cdot 677$
$916327 = 479 \cdot 1913$
$934021 = 11 \cdot 19 \cdot 41 \cdot 109$
$950797 = 23 \cdot 67 \cdot 617$
$976873 = 313 \cdot 3121$
$983401 = 331 \cdot 2971$
$997633 = 7 \cdot 13 \cdot 19 \cdot 577$