UNIVERSIDADE FEDERAL DE ALAGOAS

MESTRADO PROFISSIONAL EM REDE NACIONAL - PROFMAT

UM ESTUDO DO ENSINO DE NÚMEROS PRIMOS NA EDUCAÇÃO BÁSICA

DJALMA GOMES DE FARIAS

Maceió, 2016

DJALMA GOMES DE FARIAS

UM ESTUDO DO ENSINO DE NÚMEROS PRIMOS NA EDUCAÇÃO BÁSICA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Alagoas, coordenado pela Sociedade Brasileira de Matemática, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. André Luiz Flores

Maceió, 2016

Catalogação na fonte

Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

F224e Farias, Djalma Gomes de.
Um estudo do ensino de números primos na educação básica / Djalma Gomes de Farias. – 2016.
95 f. : il.

Orientador: André Luiz Flores.
Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Alagoas. Instituto de Matemática. Programa de Pós Graduação de Mestrado Profissional em Matemática em Rede Nacional. Maceió, 2016.

Bibliografia: f. 91-92.
Anexos: f. 93-95.

1. Matemática – Estudo ensino. 2. Números primos – Ensino e aprendizagem. I. Título.

CDU: 511.313

Folha de Aprovação

DJALMA GOMES DE FARIAS

UM ESTUDO DOS NÚMEROS PRIMOS NA EDUCAÇÃO BÁSICA

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas e aprovada em 01 de abril de 2016.

Banca Examinadora:

Prof. Dr André Luiz Flores - UFAL (Presidente)

Prof. Dr. Amauri da Silva Barros - UFAL

Prof. Dr. Daniel Cordeiro de Morais Filho - UFCG

AGRADECIMENTOS

Primeiramente agradeço a Deus por sempre me dar forças e estar sempre junto de mim em todos os momentos ajudando a vencer todas as dificuldades. A minha esposa Sara Souto Alves, por estar sempre ao meu lado me motivando sempre. Aos meus pais Cícero Nunes de Farias e Maria do Socorro Gomes de Farias, ao meu irmão Edival Gomes de Farias e ao meu filho Pedro Lucas Souto de Farias que sempre me propiciaram tantos momentos bons, dando – me forças e me motivando para prosseguir nos estudos.

A todos os professores com quem tive o prazer de estudar na educação básica e superior, por suas contribuições, fornecendo-me as ferramentas que contribuíram muito para minha vida tanto profissional quanto financeira.

A todos os professores do PROFMAT, por todas as contribuições e paciência durante todo o período do curso.

Aos amigos Jucélio Melo e Rosemere Claudina, com quem convivi por tanto tempo dividindo sempre todas as dificuldades e angústias.

A todos os colegas do PROFMAT, pela forma que me recebeu e por todas as contribuições durante o tempo em que convivemos.

Aos amigos Alex Gomes, José Severino Campos Neto, Ricardo Barros, Ana Maria Cerqueira Paranhos, Cícera Maria, Cícera Jaqueline, Danilo Barbosa,... por todo apoio.

Ao professor Dr. André Flores, por toda paciência e por todas as suas contribuições.

Ao amigo Ledivaldo Gomes de Melo, com quem convivi por mais tempo por todas as contribuições e com quem dividi sempre as dificuldades e angústias.

"*Qualquer tolo pode fazer perguntas sobre os números primos que o mais sábio dos homens não consegue responder"*.

- Godfrey Harold Hardy

RESUMO

É muito comum grande parte dos nossos alunos chegarem ao Ensino Médio com extrema dificuldade com relação ao reconhecimento de um número primo e desconhecendo, quase que totalmente, suas principais propriedades e sua importância. Com base neste contexto, apresentamos neste trabalho algumas das principais propriedades de tais números, dando ênfase, sempre que possível, além de suas aplicações no restante de sua vida escolar, ao seu contexto histórico, visando sempre mostrar sua importância e as motivações de alguns dos importantes matemáticos que se dedicaram ao seu estudo, mostrando assim, a sua beleza e visando aumentar o interesse de nossos alunos em estudar esses tais números tão enigmáticos.

Palavras-chave: Números primos; Ensino; História; Educação.

ABSTRACT

Too often many of our students come to high school with extreme difficulty with regard to the recognition of a prime number and knowing, almost entirely, its main properties and their importance. Based on this context, we present in this paper some of the main properties of such numbers, emphasizing, whenever possible, in addition to its applications in the rest of their school life, their historical context, aiming to show their importance and the motives of some of the important mathematicians who are dedicated to their study, showing its beauty to increase the interest of our students to study these numbers such as enigmatic.

Keywords: Prime Numbers; Education; History; Education.

SUMÁRIO

INTRODUÇÃO

Quando nos deparamos em nossas salas de aula com questões que envolvem divisão exata e também aquelas que envolvem simplificação, é muito comum uma parte considerável de nossos alunos, seja nas séries finais do Ensino Fundamental ou até mesmo no Ensino Médio, demonstrarem possuir uma dificuldade considerável, principalmente quando se trata de números relativamente grandes; onde boa parte dos estudantes só consegue resolver as operações citadas acima se tiverem a ajuda de uma calculadora. Este fato acaba por dificultar ainda mais o aprendizado dos educandos, atrasando também a sequência dos conteúdos a serem vivenciados.

Este obstáculo apresentado por nossos alunos poderia ser sanado, ou pelo menos minimizado, se eles soubessem decompor um número em fatores primos. No entanto, quando citamos que esta operação pode ser facilitada usando esta estratégia, deparamo-nos com outro problema: boa parte deles não sabe ou não lembra o conceito de número primo, e acabam por fazer perguntas como: O que é um número primo? Não é melhor colocar uma lista contendo todos estes números para podermos consultar? Mostram assim total desconhecimento sobre o referido assunto.

O que se pretende com este trabalho é uma maneira de se abordar os números primos de forma um pouco mais abrangente na educação básica, ressaltando, além de sua importância, os seus principais aspectos históricos, visando tornar o seu estudo mais atrativo, servindo, desta forma, como complemento, tendo em vista que o material sobre tal assunto a ser disponibilizado nos livros didáticos da educação básica não é suficiente para que os alunos tenham um bom nível de conhecimento sobre o conteúdo em questão. A fim de contribuir com subsídios epistemológicos e pragmáticos para combater esse problema, o trabalho em questão encontra-se dividido da seguinte maneira:

Capítulo 1: neste capítulo é apresentado e comentado o resultado de um questionário contendo questões elementares sobre os números primos aplicados em algumas escolas do Ensino Fundamental e também do Ensino Médio. Também é feita uma análise sobre a forma de como os números primos são abordados em alguns dos principais livros que são adotados no Ensino Fundamental, e também como são as orientações contidas em documentos como os Parâmetros Curriculares Nacional de Matemática.

Capítulo 2: o que é visto neste capítulo são alguns dos principais conceitos de divisibilidade dos números naturais, onde estão inclusos também a divisão euclidiana, o

máximo divisor comum e o mínimo múltiplo comum de dois números, que serão de suma importância para tornar claro alguns teoremas e proposições que serão encontrados no restante do trabalho, ajudando, desta forma no desenvolvimento desse estudo - daí nota-se a importância deste capítulo.

Capítulo 3: neste capítulo será dada uma atenção especial ao contexto histórico dos números primos, apresentando também alguns dos principais matemáticos que tanto contribuíram para o atual nível de conhecimento sobre os números primos. Serão também apresentadas algumas das principais propriedades e também algumas proposições e teoremas importantes sobre os números primos, existindo também uma seção onde serão apresentados os principais métodos de se verificar se um determinado número é primo ou composto, além de serem apresentadas ao leitor algumas conjecturas importantes.

Capítulo 4: neste capítulo serão apresentadas duas sequências didáticas, sendo uma para o sexto ano e a outra para o nono ano, ambos do Ensino Fundamental, sequências estas que propõe uma maneira alternativa de ensino dos números primos. Também é dedicada uma seção onde são propostos alguns jogos e atividades para que o professor, caso ache necessário, possa utilizar em sua sala de aula, ajudando tanto no desenvolvimento do conteúdo em questão como também servem para torná-los um pouco mais atraente; fazendo, desta forma, com que os alunos tenham um maior interesse no estudo desses números tão importantes e tão enigmáticos.

Anexos: nos anexos está disponibilizada uma tabela que contém todos os números primos menores que o número 2000 que tem a finalidade de mostrar como eles se encontram de maneira aleatória, mostrando que mesmo em conjunto tão pequeno, é difícil desvendar os mistérios de sua distribuição. Serve também de suporte para algumas atividades, caso o professor entenda necessário. Também contém sugestões de alguns livros interessantes sobre os números primos e também de alguns filmes que, caso o professor ache necessário, possa utilizá-los como mais um recurso didático a ser disponibilizado.

1. PCN'S E ANÁLISE DOS LIVROS DIDÁTICOS

É muito comum na educação básica e até mesmo no Ensino Médio boa parte dos alunos demonstrarem grande dificuldade quando se trata de divisão exata e também a simplificação sem o uso de calculadora. Este fato acaba por dificultar ainda mais o aprendizado da Matemática, inibindo também o cumprimento da matriz curricular mínima. Este problema poderia ser facilmente resolvido caso os estudantes soubessem decompor um determinado número em fatores primos. No entanto, boa parte deles não demonstra ter conhecimento do conceito de um número primo.

Analisando essa problemática, foi proposto e aplicado aos alunos do Ensino Básico um questionário contendo as seguintes perguntas:

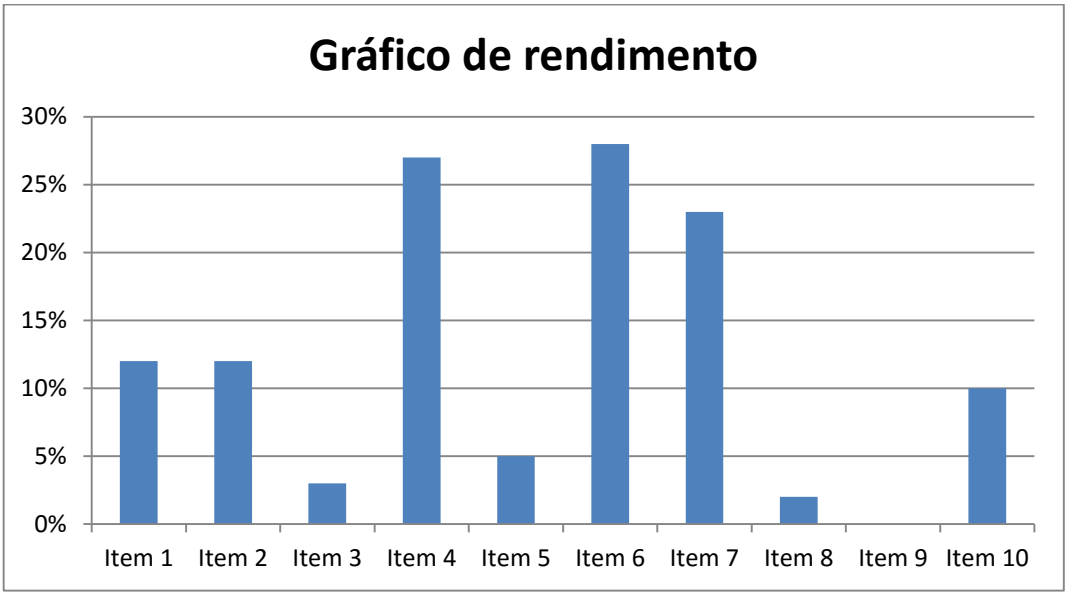
1) O que é um número primo?
2) Qual o menor número natural primo?
3) Liste os dez primeiros números naturais primos?
4) O conjunto dos números primos é finito ou infinito?
5) O número 1 é primo? Justifique.
6) Todos os números primos são ímpares?
7) Existe algum número primo que também é composto?
8) Quais são os fatores primos de 7000?
9) O número 91 é primo? Justifique.
10) O número 180180 é divisível por 2310? Se for qual é o resultado da divisão?

O questionário supracitado teve como objetivo verificar se o educando desenvolveu as seguintes competências:

- saber quais são as principais características de um número primo.
- diferenciar um número primo de um número composto.
- decompor um número composto em fatores primos.
- saber testar um número para verificar se ele é primo ou composto.

O questionário foi aplicado em quatro escolas, contemplando 100 alunos. Duas no estado de Pernambuco, no município das Correntes e duas no estado de Alagoas, nos municípios de Santana do Mundaú e Chã Preta, nas séries finais do Ensino Fundamental (nono ano) e nas séries iniciais do Ensino Médio (primeiro ano), obtendo os seguintes resultados: 12% dos alunos acertaram o item 1, 12% dos alunos o item 2, 3% dos alunos o

item 3, 27% dos alunos o item 4, 5% dos alunos o item 5, 28% dos alunos o item 6, 23% dos alunos o item 7, 2% dos alunos o item 8, nenhum acertou o item 9 e 10% dos alunos o item 10. É possível visualizar esses resultados através do gráfico abaixo:



Analisando a resposta dada pelos alunos, dois itens chamaram mais atenção: o item 2, pois 50% dos alunos que o acertaram não o incluíram na lista dos dez primeiros primos; e o item 10, pois todos os alunos que o fizeram usaram uma quantidade excessiva de cálculos, mostrando não estarem familiarizados com a decomposição em fatores primos.

De maneira geral, observa-se que boa parte dos alunos que responderam o questionário não tem o conhecimento mínimo esperado para a série na qual se encontram sobre os números primos.

1.1. Análise dos livros didáticos

O livro didático em nosso país é comumente usado pelos professores como a ferramenta mais importante para o planejamento de suas aulas, muitas vezes até como a única, resultando assim que as atividades propostas para o educando são, na maioria das vezes, apenas aquelas contidas nessa ferramenta de trabalho. Com base nesse fato será feita a seguir uma análise de como este conteúdo é abordado em alguns dos principais livros didáticos usados atualmente e também em um passado recente, no Ensino Fundamental na rede pública.

No “Projeto Teláris” (2012), de Dante, 6º ano, a abordagem do assunto se inicia com alguns exemplos dos divisores de números naturais e, em seguida, é dada a definição de um número primo. Após isso, é dada uma lista de exercícios contendo cinco questões, sendo que

uma questão em particular chamou bastante à atenção, pois propõe ao aluno que ele tenha sempre em mente os números primos menores do que 30. Na próxima seção é abordado um dos métodos de se verificar se um determinado número é primo, o Crivo de Eratóstenes, onde descreve o funcionamento do crivo e novamente passa uma lista de exercícios contendo três questões. Em seguida é abordada a fatoração de um número natural em fatores primos, são dados alguns exemplos e uma lista com duas questões. Para encerrar, na última parte do capítulo, são dadas aplicações dos números primos no cálculo do máximo divisor comum e do mínimo múltiplo comum.

Na coleção "Matemática Teoria e Contexto" (2012), de Marília Centurión & José Jakubovic, 6° ano, inicia-se o assunto com a definição de um número primo e, em seguida, são dados dois métodos de se verificar se um número é primo: o método das divisões sucessivas e o Crivo de Eratóstenes. Também é dada uma lista contendo onze questões. Em seguida é dedicada uma seção à decomposição em fatores primos, objetivando deixar claro que todo número pode ser decomposto em fatores primos. É dada ainda uma lista contendo sete questões e são propostos três desafios envolvendo números primos. Também, como no livro anterior, são dadas aplicações dos números primos no cálculo do máximo divisor comum e do mínimo múltiplo comum.

Na coleção "Fazendo a Diferença", de Bonjorno & Ayrton (2006), 6º ano, o assunto é iniciado com a descrição do Crivo de Eratóstenes e com a definição de um número primo, com alguns exemplos e uma lista de exercícios contendo quatro questões. Em seguida é abordada a decomposição de um número natural, onde são dados exemplos de decomposição em fatores primos e também uma lista de exercícios contendo sete questões; na última parte também são dadas aplicações dos números primos no cálculo do máximo divisor comum e do mínimo múltiplo comum.

Na coleção "Matemática e Realidade" (2005), de Gelson Iezzi, Osvaldo Dolce e Antonio Machado, 6° ano, a abordagem do assunto começa pelo processo do Crivo, embora esse processo não seja citado diretamente. Em seguida, é apresentada a definição de um número primo e também de um número composto, com uma lista de exercícios contendo seis questões. Logo após, há uma seção dedicada ao reconhecimento de um número primo, a qual informa que há infinitos números primos e descreve um dos métodos para verificar se um número é primo ou composto: o método das divisões sucessivas, seguido de uma lista de exercícios contendo seis questões. Outro capítulo é dedicado à decomposição em fatores primos, informando que todo número natural maior do que 1 pode ser decomposto num produto de fatores primos, são dados alguns exemplos e um exercício totalizando doze

questões sobre o assunto. Como nos outros livros descritos acima, também mostra as aplicações dos números primos no cálculo do máximo divisor comum e do mínimo múltiplo comum.

Na coleção “Descobrindo e Aplicando a Matemática” (2012), de Alceu dos Santos Mazzieiro e Paulo Antônio Fonseca Machado, 6º ano, não foi encontrada nenhuma menção sobre os números primos.

Na coleção “Para Saber Matemática” (2006), de Luiz G. Cavalcante, Juliana Sosso, Fábio Vieira e Ednéia Poli, 5ª série (6º ano), a abordagem do assunto começa pela representação retangular dos números, informando, em seguida, que a representação retangular de um número primo tem sempre um dos lados medindo uma unidade, dando então a definição de um número primo seguido de uma lista contendo 11 questões. Logo após é informado que todo número natural pode ser decomposto em fatores primos, seguido de uma lista contendo 5 questões. Por fim, é mostrado o cálculo do mínimo múltiplo comum pela decomposição em fatores primos.

O que se observa com a análise destes livros, mesmo analisando livros adotados em épocas diferentes, e que a forma como os números primos são abordados é semelhante, verificando-se que não há uma grande preocupação, pelo menos não tão aparente, com a sua conceituação, dando até a falsa impressão de pouca utilidade desse assunto para o restante da vida escolar do educando.

Nota-se também que existe pouca quantidade de informações sobre o contexto histórico dos números primos, não deixando bem claro a sua importância. Não há menção sobre as motivações dos grandes matemáticos do passado que se detiveram a tentar desvendar esses números, deixando assim uma aparência de pouca importância para o leitor menos informado. Como nos diz o PCN:

> ...a História da Matemática também tem se transformado em assunto específico, um item a mais a ser incorporado ao rol de conteúdos, que muitas vezes não passa da apresentação de fatos ou biografias de matemáticos famosos. (PCN, p. 23, 1998).

Entretanto, o que acontece na realidade é que como o contexto histórico é praticamente inexistente na maioria dos livros didáticos adotados, a sua apresentação fica apenas restrita a relatos de pequenos trechos em suas aulas de Matemática, indo de encontro ao que nos diz o PCN:

> ...essa abordagem não deve ser entendida simplesmente que o professor deva situar no tempo e no espaço cada item do programa de Matemática ou contar sempre em suas aulas trechos da história da Matemática, mas que a encare como um recurso didático com muitas possibilidades para desenvolver diversos conceitos, sem reduzi-la a fatos, datas e nomes a serem memorizados. (PCN, p. 43, 1998).

Outro fato que convém ressaltar é que a forma como é abordado a maioria dos exercícios os torna mecânicos, não sendo oferecidos em quantidade suficiente, além disso, os que são oferecidos não oferecem grandes desafios, deixando uma impressão de seu estudo ter pouca relevância.

Um dos recursos a ser utilizado que torna interessante o aprendizado para os alunos são os jogos. No entanto, quando se trata dos números primos, esse recurso não é tão fácil de ser encontrado. Nos livros analisados, nenhum deles ofereceu esse tipo de atividade que é de grande utilidade no processo do ensino-aprendizagem.

Os fatos acima apresentados mostram o quanto é insuficiente à abordagem dos números primos, dada pelos livros didáticos analisados, não mostrando assim toda a importância e beleza desses números tão singulares.

No entanto, por outro lado, convém ressaltar que o PCN de Matemática não deixa bem clara toda a importância e a forma como deve ser abordado o estudo dos números primos. O trecho no qual eles são citados no PCN é descrito a seguir:

> ...ou o conceito de "número primo" podem ser abordados neste ciclo como uma ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores, e não como assunto novo, desvinculado dos demais. (PCN, p. 66, 1998).

Nota-se também que o próprio PCN não estabelece uma forma padronizada de como se trabalhar os números primos de maneira mais organizada, ficando a cargo do currículo a ser adotado por cada instituição de ensino a forma de abordá-los. Como é muito comum que a forma na qual são apresentados os conteúdos seja aquela encontrada nos livros didáticos, entende-se por qual motivo boa parte de nossos alunos têm tanta dificuldade, deixando, às vezes, a impressão de que nunca tiveram contato com os números primos nos anos anteriores. Vemos então a necessidade de uma complementação do conteúdo em questão.

2. DIVISIBILIDADE, DIVISÃO EUCLIDIANA, MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM NO CONJUNTO DOS NÚMEROS NATURAIS.

Os teoremas e as proposições que são apresentados neste capítulo são necessários para facilitar a demonstração de alguns teoremas e proposições que são apresentados no restante do trabalho.

2.1 Divisibilidade

Nesta seção faremos um estudo das noções básicas de divisibilidade no conjunto dos números naturais necessário ao restante deste trabalho.

Definição:

Dados dois números a e b, ambos naturais, com $a \neq 0$, dizemos que a divide b e escrevemos $a|b$, se existir um natural c tal que $b = a \cdot c$. Não se tendo $a|b$ escrevemos $a \nmid b$ significando que não existe nenhum c natural tal que $b = a \cdot c$.

De maneira alternativa, podemos dizer que a é um fator b ou um divisor de b, ou ainda que b é múltiplo de a.

Exemplos: $1|0$; $2|0$; $1|2$; $2|2$; $3 \nmid 5$; $7 \nmid 9$; $4|12$

As proposições 2.1.1 e 2.1.2 abaixo demonstradas são encontradas no livro de HEFEZ(2011).

Proposição 2.1.1 Seja $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. Tem-se que:

i) $1|c$, $a|a$ e $a|0$.

ii) se $a|b$ e $b|c$, então $a|c$.

Demonstração: O item (i) é consequente das seguintes igualdades

$c = 1 \cdot c$, $a = 1 \cdot a$ e $0 = a \cdot 0$.

No item (ii) temos que como $a|b$ e $b|c$, o que implica que existirá um $f, g \in \mathbb{N}$, tais que $b = a \cdot f$ e $c = b \cdot g$. Para concluir a prova, basta substituir o valor de b na segunda equação, logo teremos:

$c = b \cdot g = (a \cdot f) \cdot g = a(f \cdot g)$

Desta forma, conclui-se que $a|c$.

□

Exemplo 1: seja $a = 2$, $b = 4$ e $c = 12$,

Pela proposição acima como $2|4$ e $4|12$; logo $2|12$;

Exemplo 2: seja $a = 5$, $b = 10$ e $c = 30$,

Como $5|10$ e $10|30000$; logo $5|30000$.

Proposição 2.1.2. Se $a, b, c, d \in \mathbb{N}$ com $a, c \neq 0$, então:

$$a|b \text{ e } c|d \Rightarrow a \cdot c | b \cdot d.$$

Demonstração: Se $a|b$ e $b|c$, então existem $f, g \in \mathbb{N}$ tais que, $b = a \cdot f$ e $d = c \cdot g$. Como $b = a \cdot f$, multiplicando b na equação acima por d, temos:

$b \cdot d = (a \cdot f) \cdot (c \cdot d) = (a \cdot c) \cdot (f \cdot g)$,

O que resulta que $a \cdot c | b \cdot d$.

□

As proposições 2.1.3 e 2.1.4 são demonstradas em LANDAU(2002).

Proposição 2.1.3. Sejam $a, b, c \in \mathbb{N}$, $a \neq 0$ e $c \neq 0$ logo temos que Se $a|b$ então $a \cdot c | b \cdot c$.

Demonstração: Como $a \neq 0$ e $c \neq 0$ temos então que $a.c \neq 0$. Assim existe um $q \in \mathbb{N}$ tal que $b = q \cdot a$, logo, multiplicando ambos os termos por c temos que $b \cdot c = q \cdot a \cdot c$. Concluímos assim que $a \cdot c | b \cdot c$.

□

Proposição 2.1.4. Sejam $a, b, c \in \mathbb{N}$ $a \cdot c \neq 0$ logo temos que Se $a \cdot c | b \cdot c$ então $a|b$.

Demonstração: Como $a.c \neq 0$ temos então que se $a \neq 0$ e $c \neq 0$. Logo existirá um $q \in \mathbb{N}$ tal que $b \cdot c = q \cdot a \cdot c$, dividindo ambos os membros da igualdade por c, obtemos que $b = q \cdot a$, mas, como $q \in \mathbb{N}$, temos assim que $a|b$. Assim concluímos que $a|b$.

□

Proposição 2.1.5. Sejam a, b e $c \in$ N, $a \neq 0$ e (a, b) = 1. Se $a|b.c$ e $a \nmid b$ então $a|c$.

Demonstração: Como $a|b \cdot c$ logo irá existir um $k \in$ N tal que $b \cdot c = a \cdot k$. Já que $a \nmid b$ considere agora um $m \in$ N o menor múltiplo comum dos números a e b. Por hipótese temos assim que $b \cdot c$ também é um múltiplo de a. Assim, consequentemente, temos que $b \cdot c \geq m$, logo $a \cdot b | b \cdot c$ e pela proposição 2.4 $a|c$, concluindo assim a demonstração.

□

As proposições 2.1.6 a 2.1.9 são encontradas também no livro de HEFEZ.

Proposição 2.1.6. Sejam $a, b, c \in$ N $a \neq 0,$ tais que $a|(b+c)$. Então $a|b \Leftrightarrow a|c$.

Demonstração: Primeiro iremos mostrar que $a|b \Longrightarrow a|c$.

De $a|(b+c)$, temos que existe um $f \in$ N tal que $b + c = f \cdot a$, e de $a|b$ temos que existe um $g \in$ N tal que $b = a \cdot g$. Substituindo em $b + c = f \cdot a$ temos:

$a \cdot g + c = f \cdot a$.

Como $c \in$ N temos então que $a \cdot f > a \cdot g$, logo $f > g$, assim.

$c = a \cdot f - a \cdot g = a(f - g)$, e portanto $a|c$.

Agora iremos mostrar que $a|c \Longrightarrow a|b$

Usando o mesmo procedimento, temos que se $a|(b+c)$ então existe um $f \in$ N tal que $b + c = f \cdot a$, e de $a|c$ temos que existe um $h \in$ N tal que $c = h \cdot a$, assim substituindo c em $b + c = f \cdot a$ temos:

$b + h \cdot a = f \cdot a$

Como $b \in$ N temos então que $a \cdot f > a \cdot h$, logo $f > h,$ assim.

$b = a \cdot f - a \cdot h = a(f - h)$

Logo $a|b$, concluindo a demonstração.

□

De modo análogo mostra-se que:

Proposição 2.1.7. Sejam $a, b, c \in \mathrm{N}$ $a \neq 0$ e $b \geq c$, tais que $a|(b - c)$. Então,

$$a|b \Leftrightarrow a|c.$$

Exemplo 1: Seja a e $b \in \mathrm{N}$, sabendo que a e b são divisíveis por três, podemos afirmar que $a + b$ também será divisível por 3?

Solução:

Como a e b são divisíveis por 3, podemos afirmar que a é um número da forma $3k$ e b é um número da forma $3w$, com k e $w \in \mathrm{N}$. Logo, teremos,

$a + b = 3\mathrm{k} + 3\mathrm{w} = 3(\mathrm{k} + \mathrm{w})$

Concluímos assim que se a e b forem ambos divisíveis por 3, a sua soma também será divisível por 3.

Exemplo 2: (Banco de questões OBMEP – 2006). Da igualdade $9174532 \cdot 13 = 119268916$ pode-se concluir que um dos números abaixo é divisível por 13. Qual é este número?

a) 119268903 b) 119268907 c) 119268911

d) 11926891 e) 119268923

Solução:

Como 119268916 é divisível por 13, se somarmos ou subtrairmos um múltiplo de 13, também será divisível por 13. Logo, o número procurado é da forma $119268916 \pm \mathrm{k}.13$ com $\mathrm{k} \in \mathrm{N}$, assim, usando o método das tentativas,

Para k = 1, temos:

$119268916 + 1.13 = 119268929$, $119268916 - 1.13 = 119268903$

Portanto a resposta correta é a alternativa a.

Proposição 2.1.8. Se $a, b, c \in \mathrm{N}$ $a \neq 0$, e $x, y \in \mathrm{N}$ são tais que $a|b$ e $a|c$, então $a|(xb+yc)$; e se $xb \geq yc$, então $a|(xb - yc)$.

Demonstração: De $a|b$ e $a|c$ logo irá existir $f, g \in \mathrm{N}$ tais que $b = a \cdot f$ e $c = a \cdot g$. Logo,

$xb + yc = x(a \cdot f) + y\,(a \cdot g) = a(x \cdot f + y \cdot g)$.

Como x, y, f e $g \in \mathrm{N}$, $x \cdot f + y \cdot g \in \mathrm{N}$. Assim $a|(xb + yc)$. E, caso $xb \geq yc$, temos

$xb - yc = x(a \cdot f) - y\,(a \cdot g) = a(x \cdot f - y \cdot g)$

Como $xb \geq yc$ e x, y, f e $g \in \mathrm{N}$, $x \cdot f - y \cdot g \in \mathrm{N}$. Assim $a|(xb - yc)$ provando a proposição dada acima.

Exemplo 1: Seja $a = 4$, $b = 8$, $c = 12$, $x = 2$ e $y = 1$, logo temos que:

$4|8$ e $4|12$, $4|(2 \cdot 8 + 1 \cdot 12)$ e $4|(2 \cdot 8 - 1 \cdot 12)$

Proposição 2.1.9. Dados $a, b, \in \mathrm{N}^*$, temos que:

$$a|b \Longrightarrow a \leq b.$$

Demonstração: Temos que se $a|b$ então existe um $c \in \mathrm{N}^*$ tal que $b = a \cdot c$. Temos também que $a \leq a \cdot c$, com a igualdade existindo apenas para o caso de $c = 1$. Mas como $b = a \cdot c$, então $a \leq b$.

□

2.2. Divisão Euclidiana

A Divisão Euclidiana mais conhecida como divisão com resto é aquela em que um número natural a não necessariamente divide outro número também natural b, fato este já utilizado por *Euclides*, nos seus *Elementos*, mesmo sem enunciá-lo de forma clara, afirma que é sempre possível efetuar a divisão de b por a, com possível resto.

O teorema demonstrado abaixo é encontrado em Hefez.

Teorema 2.2.1 (Divisão Euclidiana). Sejam a e b dois números naturais com $0 < a <$ b. Existem dois únicos números naturais q e r tais que

$$b = a \cdot q + r, \text{ com } r < a.$$

Demonstração: Para fazer esta demonstração suponha, sem perda de generalidade, que $b > a$ e considere, enquanto fizer sentido, os seguintes números.

$b, b - a, b - 2a,...,b - n\cdot a,...$

Usando a propriedade da Boa Ordem, cujo enunciado é: *todo subconjunto não vazio de* N *possui um menor elemento*, o conjunto A formado pelos elementos acima tem um menor elemento r, este pode ser descrito como $r = b - q\cdot a$, com $q \in$ N. Vamos verificar se $r < a$.

Se $a|b$, então $r = 0$ acabando assim a demonstração. Agora se $a \nmid$ b, então teremos que $r \neq 0$, e, portanto, precisamos mostrar que $r < a$. Para isso, suponha que $r \geq a$. Se este fato ocorresse, teríamos dois casos:

1º caso: se $r = a$ então teríamos que $a|b$ encerrando a demonstração.

2º caso: se $r > a$ então existiria um número natural $c < r$ tal que $r = c + a$. Logo, sendo $r = c + a = b - q\cdot a$, o que resultaria em:

$$c = b - (q + 1)\cdot a \in \text{A}, \text{ com } c < r,$$

Contradição, pois neste caso r não seria o menor elemento de A.

Portanto, concluímos que $b = a\cdot q + r$ e $r < a$.

O que precisamos verificar agora é a unicidade. Considere para este fato dois elementos distintos de A, a diferença entre eles, caso eles sejam um múltiplo de a, é pelo menos a. Logo, se $r = b - a\cdot q$ e $r' = b - a\cdot q'$, com $r < r' < a$, teríamos

$$r - r' = (b - a\cdot q) - (b - a\cdot q') = a\cdot q + a\cdot q' = a(q + q') \geq a,$$

o que seria um absurdo. Logo, concluímos que $b - a\cdot q = b - a\cdot q'$, resultando que $a\cdot q = a\cdot q'$ e $q = q'$, concluindo assim a demonstração.

□

Observe também que q e r são também chamados de *quociente* e *resto* respectivamente da divisão de b por a.

Exemplo: Ache o conjunto dos números naturais menores que 100 que deixam resto igual ao quociente quando divididos por 27.

Solução:

Usando a Divisão Euclidiana temos:

$b = a \cdot q + r$, com $a = 27$ e $q = r$, substituindo temos:

$b = 27r + r$, com $0 \leq r \leq 27$ e $b < 100$, logo

$b = 28r$.

Temos também que

$r \in \{1, 2, 3, 4, 5, ..., 27\}$ e $b \in \{28, 56, 84, 112, 140, ..., 746\}$,

mas, como das condições do problema, $b < 100$, temos então que o conjunto procurado é

$\{28, 56, 84\}$

2.3. Máximo Divisor Comum

O máximo divisor comum de dois números a, $b \in \mathbb{N}$, ambos não simultaneamente nulos, é um $d \in \mathbb{N}^*$ tal que ele seja o maior divisor comum (mdc) entre esses números e, consequentemente temos que $d|a$ e $d|b$. Além do que qualquer divisor comum desses números também irá dividir d.

Com a finalidade de simplificar a notação, o máximo divisor comum entre a e b será representado por (a, b).

A definição de máximo divisor comum usado neste trabalho é também encontrada no livro de HEFEZ.

Um número natural d será o máximo divisor comum (mdc) de a e b se possuir as seguintes propriedades:

i) d é um divisor comum de a e b;

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

Proposição 2.3.1. Seja $a \in \mathbb{N}$ e $a \neq 0$ temos que:

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

Demonstração: A demonstração desta proposição é bem simples, pois $a|0$, $a|a$, $1|1$ e $1|a$.

□

Nota-se, assim, que o máximo divisor comum de dois números naturais não simultaneamente nulos sempre existe e é maior do que zero.

Proposição 2.3.2. Seja $a \in \mathrm{N}$ temos que $(a, a + 1) = 1$.

Demonstração: Suponha que $(a, a + 1) = d$, com $d \in \mathrm{N}$, logo pela definição de máximo divisor comum têm que $d|a$ e $d|a + 1$, mas pela proposição 2.1.6 temos que se $d|a$ e $d|a + 1$ então $d|1$, mas como d é um número natural temos que $d = 1$, completando assim a demonstração.

□

Exemplo 1. Calcule o máximo divisor comum entre 14 e 15.

Uma solução:

Calculando os divisores de ambos os números, temos;

Usando a proposição acima temos: $(14, 15) = (14, 14 + 1) = 1$.

Proposição 2.3.3. Seja $a \in \mathrm{N}$ impar temos que $(a, a + 2) = 1$.

Demonstração: Suponha que $(a, a + 2) = d$, com $d \in \mathrm{N}$, logo, pela definição de máximo divisor comum têm que $d|a$ e $d|a + 2$, e também pela proposição 2.6 temos que se $d|a$ e $d|a + 2$ então $d|2$. Logo temos que $d = 1$ ou $d = 2$, mas como a é ímpar, o último caso não pode acontecer, logo $d = 1$, completando assim a demonstração.

□

Exemplo 1. Calcule o máximo divisor comum entre 133 e 135.

Pela proposição acima temos que $(133, 135) = (133, 133 + 2) = 1$.

Proposição 2.3.4. Seja $a, b, \in \mathrm{N}$ e $a \neq 0$ temos que $a|b \Leftrightarrow (a, b) = a$.

Demonstração: Seja $d \in \mathrm{N}$ tal que $(a, b) = d$. Logo, pela definição de máximo divisor comum, temos que $d|a$ e $d|b$ e, por consequência, $d \leq a$ e $d \leq b$. Como $a|b$ pela definição de máximo divisor comum, concluímos que $(a, b) = a$.

Para o caso $(a, b) = a \Rightarrow a|b$ o resultado é óbvio, pois de $(a, b) = a$, temos pela própria definição que $a|a$ e $a|b$, concluindo assim a demonstração.

□

Lema 2.3.1. (*Lema de Euclides*) Sejam $a, b, n, \in$ N com $a < n \cdot a < b$. Se existe $(a, b - n \cdot a)$ então (a, b) existe e $(a, b) = (a, b - n \cdot a)$.

Demonstração: Considere $(a, b - n \cdot a) = d$, com $d \in$ N. Logo, pela definição de máximo divisor comum, $d|a$ e $d|b - n \cdot a$. Como $d|a$, consequentemente $d|n \cdot a$, se $d|b - n \cdot a$, pela proposição 2.1.7, então $d|b$, concluímos assim que d é divisor comum de a e b. Por outro lado, considere que $(a, b) = c$ e por definição, $c|a$ e $c|b$, logo $c|b - n \cdot a + n \cdot a$, resultando que $c|b - n \cdot a$, e pela proposição 2.1.7, $c|d$ o que nos leva a concluir que $c = d$, completando assim a demonstração.

□

Exemplo: Calcule o máximo divisor comum entre 8 e 34.

$(8, 34) = (8, 34 - 4 \cdot 8) = (8, 2) = 2$.

Lema 2.3.2. Sejam $a, b, n \in$ N com $a < n \cdot a < b + n \cdot a$. Se existe (a, b) então $(a, b + n \cdot a)$ existe e $(a, b) = (a, b + n \cdot a)$

Demonstração: Seja $(a, b) = d$, logo temos que $d|a$ e $d|b$, e como consequência $d|b + n \cdot a$. Logo d é um divisor comum de a e $b + n \cdot a$. Por outro lado, considere $(a, b + n \cdot a) = c$, logo $c|a$ e $c|b + n \cdot a$, pelo lema anterior $c|b + n \cdot a - n \cdot a$, ou seja, $c|b$ e como consequência $c|d$, concluindo assim a demonstração.

□

Verificando a existência do Máximo Divisor Comum a partir do algoritmo de Euclides.

Sejam $a, b, \in$ N e supondo, sem perda de generalidade, que $a \leq b$. Caso tenhamos $a = 1$, $a|b$ ou $a = b$, teremos então que $(a, b) = a$.

Suponhamos agora que $1 < a < b$ e também que $a \nmid b$. Assim, pela Divisão Euclidiana temos

$b = a \cdot q_1 + r_1$, com $r_1 < a$

Logo, a partir deste fato, teremos duas possibilidades: $r_1 \mid a$ ou $r_1 \nmid a$. Analisemos cada uma delas:

i) $r_1 \mid a$, logo pelo Lema de Euclides temos que

$$(a, b) = (a, b - a \cdot q_1) = (a, r_1) = r_1$$

Terminando assim o algoritmo.

ii) $r_1 \nmid a$, neste caso teremos que novamente efetuar divisão euclidiana de a por r_1. Logo,

$a = r_1 \cdot q_2 + r_2$, com $r_2 < r_1$

Novamente temos duas possibilidades: $r_2 \mid r_1$ ou $r_2 \nmid r_1$. Logo, analisando, temos:

iii) $r_2 \mid r_1$, logo usando o Lema de Euclides temos:

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

Terminando assim o algoritmo.

iv) $r_2 \nmid r_1$, teríamos que novamente efetuar a divisão, agora de r_1 por r_2, logo:

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

Nota-se que esse processo pode continuar infinitamente, encontrando assim uma sequência de números naturais $a > r_1 > r_2 > \ldots$, não possuindo menor elemento, o que não é possível, pois os números naturais possuem um menor elemento. Desse modo concluímos que para algum $n \in \mathbb{N}$ temos que $r_n \mid r_{n-1}$, o que resulta que $(a, b) = r_n$.

□

Validamos dessa forma a existência do máximo divisor comum a partir do algoritmo de Euclides. Na prática, podemos usar o algoritmo da seguinte maneira:

Primeiro efetuamos a divisão de $b = a \cdot q_1 + r_1$, logo

	q_1	
a	b	
r_1		

Em seguida, continuemos a divisão só agora de $a = r_1 \cdot q_2 + r_2$, logo

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Se continuarmos o processo, obteremos:

	q_1	q_2	...	q_{n+1}
b	a	r_1	...	$r_n = (a, b)$
r_1	r_2	r_3	...	

□

Exemplo 1: Calcule o máximo divisor comum de 180 e 150.

Usando o algoritmo de Euclides, temos:

	1	5
180	150	30
30		

Assim, temos que o máximo divisor comum de 180 e 150 é 30.

Exemplo 2: Calcule o máximo divisor comum de 216 e 203.

Usando o algoritmo de Euclides, temos:

	1	13	2	2
216	201	15	6	3
15	6	3		

Logo, o máximo divisor comum entre 216 e 201 é 3.

De maneira simplificada, podemos dizer que o máximo divisor comum é encontrado quando, pelo algoritmo de Euclides, encontramos o resto zero. Portanto o máximo divisor comum será o último resto da divisão diferente de zero.

2.4. Mínimo Múltiplo Comum

Um número natural $m \neq 0$ é o mínimo múltiplo comum (mmc) de dois números a e b, ambos naturais, se ele for o primeiro múltiplo natural dos dois números, logo irá existir um f e $g \in \mathrm{N}$ e temos que $a.f = m = b \cdot g$, logo ele deve possuir as seguintes propriedades:

i) $a|m$ e $b|m$ (m é múltiplo comum de a e b)

ii) Seja $c \in \mathrm{N}$ um múltiplo comum de a e b, logo também será um múltiplo natural de m.

Das propriedades (i) e (ii) temos que $a \leq m$ e $b \leq m$, $a|c$ e $b|c$, consequentemente $m|c$, logo m será o menor múltiplo natural diferente de zero de a e b.

Com a finalidade de facilitar a notação iremos representar o mínimo múltiplo comum de dois números a e b da seguinte maneira $[a,\ b]$**.**

Exemplo 1: Um corredor dá uma volta em uma pista circular em 30 minutos, outro corredor faz o mesmo percurso em 40 minutos. Se ambos saem ao mesmo tempo na primeira volta, depois de quantos minutos irão se encontrar novamente?

Uma solução:

Como o tempo necessário para que ocorra o próximo encontro será um valor divisível por 30 e 40, basta então para solucionar o problema calcular o mínimo múltiplo comum entre os dois números. Logo:

Múltiplos de 30 = 30, 60, 90, 120, 150, 180...

Múltiplos de 40 = 40, 80, 120, 160, 200...

Ou seja, $[30, 40] = 120$.

Portanto, o primeiro encontro ocorrerá em 120 minutos.

Proposição 2.4.1. Sejam a e b dois números naturais, logo temos que $[a,\ b]$ existe e $[a,\ b](a, b) = a \cdot b$

Demonstração: Temos que $(a, b) = d$, com $d \in \mathrm{N}$ da definição de máximo divisor comum temos que $d|a$ e $d|b$ logo, como consequência $a = d \cdot a'$ e $b = d \cdot b'$, com a'e $b' \in \mathrm{N}$ e também com $(a',b') = 1$.

Temos também que existe um $k \in \mathrm{N}$ tal que $[a,\ b] = a \cdot k$, logo temos que $a|a \cdot k$ e $b|a \cdot k$ logo, como $a = d \cdot a'$ e $b = d \cdot b'$ temos que $d \cdot b' | d \cdot a' \cdot k$ e pela proposição 2.1.4, $b'|a' \cdot k$, mas como $(a',b') = 1$, logo $a' \nmid b'$, assim, pela proposição 2.1.5, temos que $b'|k$. Assim, da

definição de mínimo múltiplo comum, temos que k deve ser o menor múltiplo divisível por $b´$, logo temos que $b´ = k$, logo temos:

$[a, b] = a \cdot k = a \cdot b´$.

Desta forma, temos que;

$[a, b](a, b) = a \cdot b´ \cdot d = a \cdot b$.

Concluindo, desse modo, a demonstração.

□

Exemplo: Calcule o produto entre o máximo divisor comum e o mínimo múltiplo comum entre 6 e 8.

$[6, 8](6, 8) = 6 \cdot 8 = 48$

2.5. Primos entre si (coprimos)

Definição:

Um conjunto de números é chamado de primos ente si ou coprimos quando o único divisor comum entre tais números é o número 1.

Exemplo: Verifique se os números 15 e 22 são coprimos.

Solução:

Divisores de 15: 1, 3, 5 e 15.

Divisores de 22: 1, 2, 11 e 22.

Como o único divisor comum entre 15 e 22 é 1, eles são coprimos.

Dizemos que dois números a e b são chamados coprimos quando satisfaz as seguintes propriedades.

i) $(a, b) = 1$, (1 é o único divisor comum de a e b)

ii) $[a, b] = a \cdot b$ (o menor múltiplo comum de a e b é o produto entre eles).

O item (i) é consequência direta da definição. Para o caso do item (ii) ele é a consequência da proposição 2.4.1. Logo, temos:

$(a, b)[a, b] = a \cdot b.$

Como do item i $(a, b) = 1$, logo substituindo, temos:

$1 \cdot [\, a, b\,] = [\, a, b\,] = a \cdot b$

Proposição 2.5.1. Sejam a e b dois números naturais, eles serão primos entre si se, e somente se, existirem x e y naturais tais que $x \cdot a - y \cdot b = 1$.

Demonstração: Considere $c \in \mathrm{N}$ tal que $c|a$ e $c|b$, e suponha, sem perda de generalidade, que $a > b$, pela proposição 3.1.8 temos que $c|(x \cdot a - y \cdot b)$, com $x \cdot a \geq y \cdot b$, logo irá existir um $k \in \mathrm{N}$ tal que $x \cdot a - y \cdot b = k \cdot c$, mas como a e b são primos entre si temos que $c = 1$, logo $x \cdot a - y \cdot b = k \cdot 1$, o que resulta que $x \cdot a - y \cdot b = k$. Como x, y e $k \in \mathrm{N}$ temos que irão existir valores de x e y tais que $x \cdot a - y \cdot b = 1$.

Agora, por outro lado, considere que existam valores de x e y tais que $x \cdot a - y \cdot b = 1$. Para isso, considere também que $(a, b) = d$. Pela proposição 3.1.8 temos que $d|(x \cdot a - y \cdot b)$, mas $x \cdot a - y \cdot b = 1$, assim $d|1$e consequentemente $d = 1$ concluindo assim a demonstração.

□

Exemplo 1: (Banco de questões OBMEP - 2008 adaptado). Adivinhe – tenho dois números naturais primos entre si. Se eu somar 50 a cada um deles, encontro números de dois algarismos. Se eu subtrair 32 de cada um deles, também encontro números naturais de 2 algarismos. Quais são os números, sabendo que nenhum deles é primo e que o número par é maior que o ímpar?

Uma solução:

Como no enunciado, se somar 50 ou subtrair 32 ainda encontramos números de dois algarismos. Logo, os números procurados serão menores do que 50 e maiores do que 41. Descartando os números 43 e 47, que são primos, os números que nos restam são 42, 44, 45, 46, 48 e 49. Logo os números procurados são 44 e 45, 45 e 46 ou 48 e 49, mas como o número par é menor do que o impar, logo as possíveis soluções são: 44 e 45, 48 e 49.

3. NÚMEROS PRIMOS

Neste capítulo conheceremos um pouco da história dos números primos, além de alguns matemáticos brilhantes que passaram boa parte de sua vida tentando desvendá-los. Iremos ainda estudar algumas propriedades dos números que vêm desafiando a humanidade há mais de dois milênios. Sendo chamado por alguns autores de os "*átomos da aritmética*", os números primos são os números mais importantes devido ao fato de todos os outros números serem formados a partir deles.

Neste capítulo também dedicaremos uma seção para fazer o estudo de alguns dos principais métodos para verificar a primalidade de um número.

3.1. Um breve estudo da história dos números primos.

Desde a idade da pedra, o homem tem buscado, sempre que possível, quantificar e representar os dados usando símbolos. Compreender o mundo que nos rodeia sempre desafiou a humanidade, mesmo em um passado distante quando não se dispunha de nenhum aparato tecnológico para este fim. Para ajudar a compreendê-lo, a Matemática se transformou em uma importante aliada. Como nos diz Sautoy, "*(...) a ferramenta mais poderosa que os homens criaram para navegar no selvagem e complexo mundo em que vivemos é a matemática." (SAUTOY, p. 07, 2013).*

Neste sentido, um dos ramos de estudo da Matemática, a Teoria dos Números forneceu e ainda tem fornecido uma ajuda considerável, estando presente desde quando o ser humano começou a desenvolver a ideia de quantidade em um passado distante até os dias atuais, ganhando grande notoriedade na era moderna, onde matemáticos notáveis e também muitos amadores apaixonados pela Matemática dedicaram boa parte da sua vida estudando este importante ramo da Matemática.

> (...) na história da Matemática, a história da Teoria dos Números tem um lugar especial. Teoria dos números é a "Rainha da Matemática". Como nos diz Gauss no século XIX. Esse apelido não foi dado só pela razão de que a Teoria dos Números é a parte mais bela da Matemática, mas também pelo fato de que ela representa ao mesmo tempo a parte mais antiga e a mais jovem da Matemática. Não somente no nosso tempo, mas sempre foi assim, pelo menos desde o início do tempo moderno. Teoria dos Números, essa área tão antiga, tem um passado profundo, espetacular e

> tem um presente ativo e um futuro que deve ser julgado pelas gerações vindouras. (SHOKRANIAN, p. 01, 2013).

Um capítulo em especial da Teoria dos Números teve um destaque notável durante a sua evolução, não só por sua grande importância, mas também pelos desafios oferecidos à sua compreensão: são os famosos “números primos”, que como nos diz Du Sautoy, “os números primos, os mais importantes da matemática e também os mais enigmáticos”.

Quando nos deparamos com os números primos pela primeira vez, é muito comum relacionarmos com a ideia de parentesco, fato esse que acontece com certa frequência muito possivelmente devido ao significado da palavra na língua portuguesa. Entretanto, em Matemática, a palavra “PRIMO” vem de primeiro, portanto, os números primos são os primeiros, tidos como tais por serem indecomponíveis, eles aparecem na decomposição de todos, tendo sua origem na velha concepção numérica do Grego passado ao Latim. Já os gregos antigos, para ser mais exato, os pitagóricos, usavam algumas denominações para tais números que hoje não são mais usadas, tais como retilíneos, lineares e eutimétricos.

Os números primos são conhecidos e estudados há muito tempo pela humanidade, havendo indícios até de que povos como os egípcios já trabalhavam com tais concepções, mesmo que com pouca organização, há bastante tempo, sendo encontrados alguns indícios no papiro de Rhind (papiro adquirido no Egito cerca de 1650 a.C. pelo egiptólogo escocês A. Henry Rhind). No entanto, convém ressaltar que os primeiros povos a fazerem um estudo de maneira mais organizada sobre os números primos foram os gregos, principalmente um em especial, Euclides, nos seus Elementos. Este contém vários teoremas importantes sobre números primos. Mais adiante serão feitas demonstrações de alguns deles.

No entanto, apesar das contribuições feitas por Euclides serem tão difundidas, acredita-se que quem primeiro trabalhou com a noção de números primos na Grécia foi, muito possivelmente, Pitágoras (estima-se que nasceu por volta de 572 a.C e a sua morte tenha ocorrido por volta de 500 a.C), cerca de 530 a.C.

Mesmo no início do estudo de tais números pelos pitagóricos já existiam algumas polêmicas sobre tais números, como, por exemplo, sobre a primalidade do número dois que não era considerado por muitos pitagóricos como um número primo. Esta polêmica perdurou por muito tempo, tendo acabado apenas na época de Aristóteles e, a partir daquele momento, esse número passou a ser aceito como primo.

Como vimos anteriormente, possivelmente os gregos antigos, apesar das grandes descobertas sobre os números primos, não foram os primeiros a se interessar por suas qualidades únicas, pois além do papiro de Rhind, citado anteriormente, também existem

relatos de indícios mais antigos ainda, encontrados no osso de Ishango, como citado em Marcos Du Sautoy:

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

Tais números vêm desafiando grandes matemáticos que passaram boa parte de sua vida tentando descobrir alguma regularidade, sem muito êxito, em sua distribuição. Como nos dizia o grande matemático inglês Godfrey Harold Hardy (1877 – 1947) "*qualquer tolo pode fazer perguntas sobre os números primos que o mais sábio dos homens não consegue responder"*. As palavras de Hardy nos proferem o quão singular são estes números.

Dentre os grandes matemáticos que mergulharam no universo dos primos podemos citar: Euclides, um pouco de suas contribuições serão relatadas mais adiante, Euler e Gauss.

Leonhard Euler (1707-1783), matemático suíço é considerado um dos maiores matemáticos de todos os tempos, tendo uma ampla produção de trabalhos matemáticos publicados. Tão vasta foi a sua produção que mesmo tendo se passado meio século após a sua morte, seus trabalhos ainda estavam sendo publicados. Euler demonstrava ter muito interesse nos números primos, tendo chegado a produzir tabelas com todos os números primos até números pouco superiores a 100.000, sendo o primeiro a refutar a fórmula que Fermat acreditava produzir sempre números primos. Euler tentava descobrir uma fórmula que gerasse todos os números primos, mas, nesse caso, não obteve muito êxito, como nos diz Du Sautoy:

> Porém, até para o grande Euler foi difícil encontrar uma fórmula simples que gerasse todos os primos. Em 1751, ele escreveu que "há alguns mistérios nos quais a mente humana jamais penetrará. Para nos convencermos desse fato, basta fitarmos as tabelas de primos e percebermos que ali não reina qualquer ordem ou regra". (SAUTOY, p. 47, 2007).

Convém ressaltar que já foi demonstrado que não existe nenhum polinômio que consiga gerar todos os primos. Uma demonstração desse fato pode ser encontrada na Revista do Professor de Matemática da SBM.

Carl Friedrich Gauss (1777-1855), nascido em Brunsweck, na Alemanha, oriundo de uma família de poucas posses formada por trabalhadores braçais, desde criança já demonstrava grande aptidão para matemática, como encontrado em Eves (p. 519, 2004): "diz-se que com a idade de três anos detectou um erro aritmético no borrador de seu pai". Sendo Obcecado por descobrir padrões em números, fez um grande acervo de descobertas originais antes dos 25 anos de idade, sendo considerado o maior matemático do século XIX e

seguramente um dos maiores de todos os tempos, recebendo merecidamente por todos os feitos a alcunha de “O Príncipe dos Matemáticos”. Com relação aos números primos, Gauss, diferentemente de Euler, tentou atacar o problema de maneira diferente: tentou descobrir um padrão nos números primos, descobrindo, aos 15 anos de idade, a conjectura que foi provada independentemente por dois matemáticos, Jacques Hadamard (1865-1963) e Charles-Jean de La Valle Poussin (1866-1962), e que hoje a conhecemos como *Teorema do Número Primo*. O teorema do número primo assegura que os números primos menores que ou iguais a n é aproximadamente $n/ln\ n$.

Mesmo depois de transcorrido tanto tempo e depois de tantos matemáticos brilhantes e também tantos outros amadores terem dedicado parte da sua vida no estudo de tais números, os mistérios sobre a sua distribuição ainda não foram completamente desvendados, sendo isso objeto de estudo de algumas conjecturas que continuam em aberto, sendo oferecida até uma boa quantia em dinheiro para quem conseguir prová-las. Dentre as conjecturas que continuam em aberto, podemos citar as seguintes:

1) Existem infinitos primos de Fermat?
2) Existem infinitos primos da forma $n^2 + 1$?
3) Existem infinitos pares de primos da forma p e $p + 2$?
4) A sequência (1, 1, 2, 3, 5, 8, 13, 21, 34, 55,...) nos fornece infinitos números primos?
5) Todo número par maior do que 2 pode ser obtido somando dois números primos?

O problema 1 refere-se à fórmula que Pierre de Fermat (1601-1665) escreveu em uma carta enviada a Marin Mersenne (1588-1648) em 1640, acreditando que se elevasse 2 à potência 2^N e ao resultado adicionasse 1, geraria sempre números primos. No entanto, em 1732, Leonhard Euler mostrou que à fórmula de Fermat falhava para N = 5. Euler também fez uma descoberta curiosa, observou que quando inseria todos os números de 0 a 39 na fórmula $n^2 + n + 41$, todos os números a serem gerados por essa fórmula eram primos. No entanto, se inserirmos 41, o número obtido será um múltiplo do número 41 e, além disso, a fórmula proposta por Euler falha quando inserimos o número 40.

O problema 2, apesar de ter um enunciado bastante simples, trata-se de mais um problema que continua em aberto sobre os números primos.

O problema 3 refere-se aos famosos primos gêmeos, cuja definição é a seguinte: dois números p e q são chamados de primos gêmeos quando a diferença entre eles tem sempre módulo 2, ou seja, considerando $p < q$, temos que $q = p + 2$. Apesar de serem conhecidos

primos gêmeos gigantes como, por exemplo, $65516468355.2^{333333} \pm 1$. Não se conseguiu provar até o momento, se existem infinitos pares de primos gêmeos, sendo essa mais uma conjectura em aberto sobre números primos.

Já o problema 4 trata-se da sequência de Fibonacci, nome dado e referência ao matemático Leonardo Fibonacci (1170-1250), também conhecido como Leonardo de Pisa, que usou em 1202 para descrever o crescimento de uma população de coelhos e que hoje tem aplicações em ciências da computação, na análise de mercados financeiros, na teoria dos jogos e também em algumas configurações biológicas.

Já o problema 5 é a famosa conjectura de Goldbach proposta pelo matemático alemão Christian Goldbach (1690-1764) a Leonard Euler, em 1742, que é um dos problemas mais antigos ainda em aberto em matemática.

No entanto, o problema mais importante sobre números primos foi proposto por Bernhard Riemann (1826-1866) e é conhecido como a hipótese de Riemann, (a hipótese de Riemann é um problema complexo de matemática avançada de auto grau de dificuldade) foi proposta por Riemann em um artigo de apenas oito páginas publicado em 1859 onde ele utilizava a *função zeta de Riemann* para investigar o padrão dos números primos. A hipótese de Riemann afirma que todos os zeros não-triviais da função zeta de Riemann pertencem a uma linha crítica. As palavras de David Hilbert (1862-1943) dadas em uma entrevista nos mostra a importância desse problema, Hilbert considerava a hipótese de Riemann o problema mais fundamental não só da matemática - mas em termos absolutos. Sendo esta parte do oitavo problema da lista proposta por Hilbert, o oitavo problema continha a hipótese de Riemann e também a conjectura de Goldbach, ambos ainda em aberto, da lista com os 23 problemas propostos por Hilbert numa palestra em 1900 na Universidade de Sorbonne, em Paris, na qual a hipótese de Riemann está também na lista dos problemas do milênio, problemas lançados pela Fundação Clay em 2000, lista esta contendo sete problemas com um belo prêmio de um milhão de dólares para resolução de cada um deles, sendo que até o momento apenas um deles, a *conjectura de Poincaré*, já foi resolvido. O autor desta façanha é o matemático russo Grigore Perelman, feito esse que lhe valeu uma medalha Fields e também o prêmio de um milhão de dólares. No entanto, Perelman rejeitou os dois. O fato de a hipótese de Riemann estar presente nessas duas listas e ainda não ter sido resolvido, mesmo depois de tantas investidas, só destaca o seu alto grau de importância.

Ainda falando sobre a hipótese de Riemann, sua importância é acentuada pelo fato que vários campos de estudo como, por exemplo, na Física, além de grandes consequências em

Teoria da Informação, para ser mais preciso, na segurança na internet. Daí, notamos o quanto a hipótese de Riemann tornou-se importante para humanidade.

O que vemos na educação básica é que mesmo com a sua beleza e toda a sua importância, o estudo dos Números Primos passa quase por despercebido, pois a maioria dos livros utilizados se detém apenas a sua definição e ao teorema fundamental da aritmética, não dando ênfase ao seu contexto histórico e também as suas aplicações práticas, como por exemplo, a criptografia RSA (criptografia mais utilizada para proteger nossas senhas de cartões de credito que utilizam como base números primos gigantes).

3.2. Teoremas e proposições

Definição:

Um número natural $p > 1$ e que tem apenas dois divisores distintos, 1 e o próprio p, é chamado de *número primo.* Caso esse número tenha mais de dois divisores será então chamado de número composto.

Da definição temos que 1 não é um número primo e também não é um número composto. Deduzimos também que o único número natural primo par é o 2.

Assim temos que os números naturais maiores que zero se dividem em três tipos:

I. O número 1;

II. Os números primos;

III. Os números compostos.

Assim, no conjunto dos números naturais, temos que a sequência dos primeiros números primos é: 2, 3, 5, 7, 11, 13, 17, 19,... e dos primeiros números compostos são 4, 6, 8, 9, 10, 12, 14, 15, 16, 18,... .

Antes das apresentações dos teoremas e proposições que virão a seguir, será apresentada um pouco da história daquele que, através de sua obra-prima "*Os Elementos"*, forneceu os pilares para o desenvolvimento de tantos ramos da Matemática: o grande *Euclides*.

Pouco se sabe sobre a vida de Euclides, sendo desconhecida a data, o local de nascimento e as circunstancias de sua morte. O que se sabe é que ele foi professor e, muito passivelmente, criador da Escola de Matemática de Alexandria.

Euclides é considerado um dos mais importantes matemáticos de todos os tempos, sendo chamado o "Pai da Geometria", muito disso devido a sua obra mais importante e revolucionária "*Os Elementos*". Mesmo tendo escrito outros trabalhos, nenhum foi tão importante e influente. Como encontrado em Eves:

> Embora Euclides fosse autor de pelo menos dez trabalhos (textos razoavelmente completos de cinco deles chegaram até nós), sua fama repousa principalmente sobre seus *Elementos*. Parece que esse trabalho notável imediata e completamente superou todos os *Elementos* precedentes; de fato, nenhum vestígio restou de esforços anteriores. Tão logo o trabalho apareceu, ganhou o mais alto respeito e, dos sucessores de Euclides até os tempos modernos, a mera citação do número de um livro e o de uma proposição de sua obra-prima é suficiente para identificar um teorema ou construção particular. Nenhum trabalho, exceto a Bíblia, foi tão largamente usado ou estudado e, provavelmente, nenhum exerceu influência maior no pensamento científico (EVES, p. 167, 2004).

Os "Elementos" de Euclides dominou o ensino da geometria por mais de dois mil anos, sendo que desde a sua primeira impressão, em 1482, já foram impressas mais de mil edições. Apesar de todo o reconhecimento com relação às contribuições dos *Elementos* no ensino da geometria, esta importante obra não cobre somente a geometria, mas também a aritmética e a álgebra.

Teorema 3.1.1: Todo número natural n maior do que 1 ou é primo ou é divisível por um número primo.

Demonstração: Para demonstrar este fato, usaremos a indução matemática.

Para $n = 2$ temos que o teorema é verdadeiro, pois 2 é um número primo.

Suponhamos que a hipótese seja verdadeira para todo n natural. Vamos agora verificar para $n + 1$. Se $n + 1$ é primo, então o teorema é verdadeiro, terminando assim a demonstração. Mas caso $n + 1$ não seja primo, ele pode ser escrito como produto de dois números a e b ambos naturais e com $1 < a < n + 1$ e $1 < b < n + 1$. Mas pela hipótese da indução, todo número menor que $n + 1$ satisfaz a condição do teorema. Assim, para os números a e b temos que ou algum deles é primo ou é divisível por um número primo, concluindo assim a demonstração.

□

Proposição 3.1.1: Dados dois números primos quaisquer p e q, temos que se $p|q$ então $p = q$.

Demonstração: Como q é primo, temos da definição que os únicos divisores de q são 1 e o próprio q e, da definição, de $p|q$ temos que existe um $k \in \mathbb{N}$ tal que $q = p \cdot k$, temos também que se p é primo então $p > 1$, resultando que $k = 1$, logo $q = p$ concluindo assim a demonstração.

□

Proposição 3.1.2: Seja $p \in \mathbb{N}$ um número primo, temos que se $p \nmid a$ então $(p, a) = 1$.

Demonstração: Temos que como p é um número natural primo, terá dois divisores que são o 1 e o próprio p. Temos também que existe um $d \in \mathbb{N}$ tal que $(p, a) = d$; da definição de máximo divisor comum temos que $d|a$ e $d|p$, mas como $d|p$, logo devemos ter $d = 1$ ou $d = p$. O último caso não pode acontecer, pois $p \nmid a$. Logo temos que $d = 1$, concluindo assim a demonstração.

□

A proposição abaixo é encontrada nos *Elementos de Euclides.*

Proposição 3.1.3: Sejam $a, b, p \in \mathbb{N}^*$, com p primo. Se $p|a.b$, então $p|a$ ou $p|b$.

Demonstração: Suponhamos que $p|a \cdot b$ e $p \nmid a$, logo de $p|a \cdot b$ temos que existe um $k \in \mathbb{N}$ tal que $a \cdot b = p \cdot k$, e como pela Proposição 2.1.5 que se $p \nmid a$ e $p|a \cdot b$ então $p|b$.

Para o caso de $p|a \cdot b$ e $p \nmid b$ o procedimento é análogo, logo de $p|a \cdot b$ existirá um $k \in \mathbb{N}$ tal que $a \cdot b = p \cdot k$, e pela Proposição 2.1.5 temos que se $p \nmid b$ então $p|a$, concluindo assim a demonstração.

□

Mostra-se indutivamente o seguinte Corolário:

Corolário: Seja p um número primo e $a_1, a_2, a_3, \ldots, a_n \in \mathbb{N}$, temos que se $p|a_1 \cdot a_2 \cdot a_3 \ldots a_n$ então para pelo menos um valor de $i = 1, 2, 3, \ldots, n$ teremos que $p|a_i$.

Proposição 3.1.4: Sejam p, q e r três números naturais primos. Temos que se $p|q \cdot r$ então $p = q$ ou $p = r$.

Demonstração: Suponha que $p|q.r$ e $p \neq q$, então existe um $k \in \mathrm{N}$ tal que $q \cdot r = p \cdot k$ e como $p \nmid q$. Logo existe um $m \in \mathrm{N}$ onde $m = p \cdot q$ é o menor múltiplo natural de p e q, mas temos também que $q \cdot r$ também é múltiplo de p, logo temos que $q \cdot r \geq p \cdot q$, resultando que $p \cdot q | q \cdot r$, e pela Proposição 2.1.4 resulta que $p|r$, mas como r é primo os seus únicos divisores são o 1 e o próprio r, e como p também é primo e divide r, conclui-se, pela proposição 3.1.1, que $p = q$.

Agora suponha que $p|q \cdot r$ e $p \nmid r$, procedendo de maneira análoga temos que irá existir um $k \in \mathrm{N}$ tal que $q \cdot r = p \cdot k$ e como $p \nmid r$ logo irá existir um $l \in \mathrm{N}$ que será o menor múltiplo natural de p e r, logo $l = p \cdot r$. Temos também que $q \cdot r$ também é um múltiplo natural de p, logo temos que $p \cdot r | q \cdot r$. Logo $p|q$ e consequentemente, pela Proposição 3.1.1, $p = q$, concluindo assim a demonstração.

□

Proposição 3.1.5. Sejam $p, p_1, p_2, p_3, ..., p_n,$ números naturais primos com $p_1 \neq p_2 \neq p_3 \neq ... \neq p_n$ temos que se $p | p_1 \cdot p_2 \cdot p_3 ... p_n$ então, para pelo menos um valor de $i = 1, 2, 3, ..., n$ teremos que $p = p_i$.

Demonstração: Pelo Corolário da Proposição 3.1.3 temos que $p|p_i$ para algum valor de i, mas como p_i é um número primo, terá apenas dois divisores que são o 1 e o próprio p_i. Mas como $p|p_i$ e p também é primo, logo temos que $p \neq 1$, logo $p = p_i$, concluindo assim a demonstração.

□

Teorema 3.1.2. O conjunto dos números primos é infinito.

Este teorema é, na verdade, uma das proposições, para ser mais exato, a Proposição 20, e impressiona a forma como é demonstrada nos *Elementos*. Como encontrado em Eves:

> A prova de Euclides da Proposição IX 20 (*o número de números primos é infinito*) é considerada universalmente pelos matemáticos como um modelo de elegância matemática. Ela emprega o método indireto, ou *reductio ad absurdum (...).* (EVES, p. 175, 2004).

Para demonstração desse teorema usaremos a redução ao absurdo.

Demonstração: Suponhamos que o conjunto P dos números primos seja finito e possua os seguintes elementos $2 \leq p_1 < p_2 < p_3 < ... < p_n$, onde p_n será o maior número primo. Precisamos agora mostra que existe um primo maior que p_n, para isso suponha agora um

número $q \in N$, onde $q = 1 + p_1 \cdot p_2 \cdot p_3 ... p_n$, logo temos que $q > p_i$ para $i = 1, 2, 3, ..., n$. como, do Teorema 3.1.1 temos que todo número maior que 1 ou é primo ou é composto. Temos agora duas possibilidades para q. Caso q seja composto, ele terá que ser divisível por algum primo p_i do conjunto $P = \{p_1, p_2, p_3, ..., p_n\}$, assim:

$$p_i | 1 + p_1 \cdot p_2 \cdot p_3 ... p_n$$

Mas como $p_i | p_1 \cdot p_2 \cdot p_3 ... p_n$ para $p_i | 1 + p_1 \cdot p_2 \cdot p_3 ... p_n$, pela proposição 2.1.6, ele terá que dividir 1, o que não é possível pois $p_i \geq 2$. Logo q é primo.

Concluímos assim que o conjunto dos números primos não possui maior elemento, ou seja, que é infinito.

□

Na demonstração do teorema fundamental da aritmética o Princípio de Indução usado não é o usual sendo também encontrada em HEFEZ.

Teorema Fundamental da Aritmética: Todo número natural n maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.

Nos *Elementos de Euclides*, umas das Proposições, a Proposição IX 14 é equivalente ao Teorema Fundamental da Aritmética, como encontrado em Eves p. 175, com o seguinte enunciado: "*todo inteiro maior que* 1 *pode se expressar como produto de primos de uma e, salvo quanto à ordem dos fatores, uma só maneira*".

Demonstração: usaremos o princípio da indução.

Para $n = 2$ o resultado é imediato.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale pra n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que $n_1 = p_1, ..., p_r$ e $n_2 = q_1, ..., q_s$. Portanto, $n = p_1 ... p_r \cdot q_1 ... q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha, agora, que $n = p_1, ..., p_r = q_1, ..., q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 ... q_s$, pelo corolário acima, temos que $p_1 = q_j$ para algum j, que, após reordenamento de $q_1, ..., q_s$, podemos supor que seja q_1. Portanto, $p_2 ... p_r = q_2 ... q_s$.

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

□

3.3. Métodos para calcular primos

O objetivo desta seção é mostrar alguns dos principais métodos de se verificar a primalidade de um determinado número, mostrando suas principais características e aplicações, adequando, sempre que possível, a uma linguagem mais acessível possível, visando facilitar o entendimento do leitor, sendo necessário para compreensão dos mesmos o domínio dos conceitos matemáticos básicos necessários para o Ensino Fundamental.

3.3.1. Método das divisões sucessivas

O funcionamento desse método é bem simples. Suponhamos que um determinado número inteiro $n > 1$ é primo, logo o que precisamos é verificar se n não é divisível por m números inteiros menores que n (neste caso a igualdade não se aplica pois tanto um primo quanto o composto é divisível por ele próprio), ou seja, basta verificar se n não é divisível por para todo m, com $1 < m < n$.

Como exemplo, iremos verificar se o número 97 é primo. De acordo com o algoritmo descrito acima, teríamos que verificar todos os inteiros m com $1 < m < 97$, o que levaria muito tempo.

No entanto, essa ideia pode ser simplificada se usarmos a seguinte proposição:

Proposição 3.3.1: Se n não é primo, então possui, necessariamente, um fator primo menor do que ou igual a $\sqrt{n}$.

Demonstração: Seja n composto, logo $n = a.b$, com $0 < a < n$ e $0 < b < n$. Sem perda de generalidade, consideremos $a \leq b$. Suponhamos que $a > \sqrt{n}$. Assim, $n = a.b$, mas temos também que $n = \sqrt{n}.\sqrt{n}$, resultando que $n = a.b > \sqrt{n}.\sqrt{n} = n$, ou seja, obtemos assim a desigualdade $n > n$ o que é obviamente um absurdo. Portanto, a única possibilidade possível é

que $a \leq \sqrt{n}$. Daí conclui-se que *n* possui um fator primo menor do que ou igual a $\sqrt{n}$, completando assim a demonstração.

□

A proposição acima nos diz que para verificarmos se um determinado número *n* é primo, é necessário apenas verificar se ele não é divisível por todos os números primos inferiores ou iguais a $\sqrt{n}$, reduzindo de forma significativa a quantidade de testes a serem feitos.

Exemplo 1: verifique se 97 é um número primo ou composto pelo método das divisões sucessivas.

Solução: Como $9 < \sqrt{97} < 10$ e 97 não é divisível por 2, 3, 5, 7, concluímos então que ele é um número primo.

Exemplo 2: verifique se 39 é um número primo ou composto.

Solução: Pelo método das divisões sucessivas iremos testar se 39 é divisível por 2, 3 e 5 que são os primos inferiores a $\sqrt{39}$, como 39 é divisível por 3 concluímos que trata-se de um número composto.

Nota-se que apesar desse algoritmo funcionar e ser de fácil compreensão, ele tem uma vulnerabilidade: torna-se pouco viável a sua utilização caso queiramos verificar a primalidade de números relativamente grandes, pois seria necessário efetuar um número muito elevado de verificações, o que consumiria muito tempo, inviabilizando o uso desse processo. Conclui-se que esse algoritmo é de grande valia caso o número testado seja relativamente pequeno.

3.3.2. Crivo de Eratóstenes

Nascido em Cirene, no sul do mediterrâneo, o grego Eratóstenes (276 – 194 a.C.) passou grande parte da sua vida em Atenas, mudando-se para Alexandria a convite de Ptolomeu III para ser tutor de seu filho e bibliotecário chefe da biblioteca da universidade local. Eratóstenes se destacava em todos os ramos do conhecimento de seu tempo como matemático, astrônomo, geógrafo, historiador, poeta e ainda atleta. Era conhecido por seus contemporâneos como Beta e, sobre essa forma como era chamado, foram criadas algumas hipóteses, como em Eves,

> Era também conhecido como Beta e a respeito dessa alcunha aventaram-se algumas hipóteses. Alguns acreditam que, devido ao seu saber amplo e brilhante, era alçado à condição de segundo Platão. Uma explicação menos abonadora propõe que, não obstante fosse ele talentoso em muitos campos, nunca conseguiu ser o primeiro de seu tempo em campo nenhum. (EVES, p. 197, 2004).

Alguns historiadores defendem ainda que Eratóstenes era chamado assim por causa dos números de certos gabinetes ou salas de leitura a qual ele estivesse associado.

No campo da matemática, fez contribuições significativas, dentre elas se destacou por ter calculado a medida da circunferência da terra e também por ter desenvolvido um dispositivo conhecido como crivo de Eratóstenes, que calculava todos os números primos até certo número dado.

O seu método era o seguinte: escreve-se a sucessão dos números inteiros até o número desejado, começando do 1, em seguida suprime o 1, como o 2 é primo, agora elimina da lista todos os múltiplos do 2, o primeiro número que sobra é o 3 que é primo, elimina da lista todos os múltiplos do 3, o primeiro que sobra é o 5 repetindo-se o processo até o número desejado. Essa foi a maneira através da qual ele construiu sua tabela. Esse processo ficou conhecido mais tarde como *crivo de Eratóstenes.*

Como exemplo, vamos calcular todos os primos até 50.

1º passo: suprimimos o 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

2º passo: o 2 é primo, logo eliminaremos todos os múltiplos do 2 exceto o 2.

	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~~

3º passo: o primeiro número que sobra é o 3, que é primo. Agora eliminaremos todos os múltiplos dos 3 maiores que 3.

	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~~

4º passo: o próximo número da lista que sobra é o 5, que é primo. Eliminaremos todos os múltiplos dos 5 maiores que o 5.

	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~~

O próximo inteiro da lista é o 7. Assim, eliminaremos todos os múltiplos do 7 com exceção do próprio 7.

	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~~

Faremos o mesmo processo com mesmo processo com o 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47. Os que sobrarem na lista serão os primos procurados.

Apesar da forma descrita acima ser bastante eficiente, ela repete muitos passos que poderiam ser retirados. Assim, podemos refinar o crivo de Eratóstenes com os seguintes procedimentos: sendo x o número dado, calculamos primeiro a $\sqrt{x}$, pois, pela proposição 3.2.1, temos que se x é composto ele possui um fator primo menor que ou igual a $\sqrt{x}$, assim é

suficiente testar com os primos começando com o 2 até a $\sqrt{x}$, descartando os múltiplos desses primos.

O procedimento descrito acima é bem simples, primeiro retiramos todos os pares da lista com exceção de 2. Quando descartamos todos os múltiplos de um determinado primo P_i o primeiro inteiro que permanece também será primo - vamos chamá-lo de P_{i+1}. Também não precisamos nos preocupar em efetuar o produto dos primos com os números pares, pois sabemos que o produto de um inteiro por um par vai resultar em um par que já retiramos da lista anteriormente. Note também que se torna desnecessário nos preocuparmos com os ímpares menores que $(P_{i+1})^2$, pois os números compostos que foram formados e que são menores que tais números já foram retirados da lista, ou seja, é suficiente começar cada etapa pegando os múltiplos impares de P_{i+1} maiores que ou iguais a P_{i+1}.

Como exemplo, iremos calcular os primos até o número 100.

Temos que $\sqrt{100}$ é 10. Nosso teste se restringe aos primos menores que 10. Retiramos todos os pares da lista com exceção do número 2. O próximo da lista é o 3, que é primo, retiramos da lista todos os múltiplos impares do 3 a partir do 3^2. O próximo inteiro da lista que permanece é o 5 que também é primo, daí retiramos todos os múltiplos impares do 5 a partir do 5^2. O próximo da lista que ainda permanece é o 7, retiramos os impares da lista a partir do 7^2, os números que restam são todos primos. Assim, os números primos menores que 100 são: 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.

3.3.3. Pequeno Teorema de Fermat.

Nascido em Beaumont de Lamagne, cidade que se encontra nas proximidades de Toulouse, França, Pierre de Fermat (1601 – 1665) é considerado o maior matemático francês do século XVII. Teve grande importância no desenvolvimento da matemática na época principalmente no desenvolvimento da moderna teoria dos números, deixando uma enorme quantidade de acervo, que ajudou, de forma considerável, o desenvolvimento de tal ramo da matemática.

Fermat deixou uma vasta quantidade de conjecturas, por meio delas um grande número de matemáticos se deteve a tentar prova-las. Entre eles, podemos citar o grande matemático Leonhard Euler. A mais famosa de suas conjecturas é o chamado Último Teorema de Fermat,

que foi provado por Andrew Wiles, que conseguiu este fato no final do século XX, onde este é o problema matemático com o maior número de publicações de sua demonstração de maneira incorreta.

Com relação ao nosso objeto de estudo nesta seção, o Pequeno Teorema de Fermat teve sua primeira demonstração publicada em 1736 por Leonhard Euler cujo enunciado é o seguinte:

Dado um número p primo, tem-se que $a^p - a$ é divisível por p para todo $a \in \mathrm{N}$.

Demonstração: Para verificar o resultado, iremos usar o Princípio da Indução Finita.

Para $a = 1$ o resultado é valido, pois $1^p - 1 = 0$ e $p|0$.

Suponha que seja válido para todo número natural $a > 1$, iremos verificar se é valido para $a + 1$.

Logo, desenvolvendo a expressão, usando o binômio de Newton, temos:

$(a + 1)^p - (a + 1) = a^p + p \cdot a^{p-1} + ... + p \cdot a + 1^p - (a + 1) = a^p - a + p \cdot (a^{p-1} + ... + a) + 1 - 1 = a^p - a + p \cdot (a^{p-1} + ... + a)$.

Mas, pela hipótese da Indução, temos que $p| a^p - a$ e temos também que $p| p.(a^{p-1} + ... + a)$, pela proposição 2.1.6 $p|a^p - a + p.(a^{p-1} + ... + a)$ temos que o teorema é valido para $a + 1$, completando assim a demonstração.

□

Exemplo 1. Usando o Pequeno Teorema de Fermat, verifique se o número 63 é primo ou composto.

Solução: Temos que 2^6 deixa resto 1 quando dividido por 63. Logo, pela proposição 3.1.5, $2^{60} = (2^6)^{10}$ deixa resto $1^{10} = 1$ quando dividido por 63. Temos também que 2^3 deixa resto 8 quando dividido por 63, pela proposição 3.1.4, $2^{60} \cdot 2^3$ deixa resto $1 \cdot 8 = 8$ quando dividido por 63. Logo, pelo teste de Fermat, concluímos que 63 é um número composto.

Exemplo 2. Usando o Pequeno Teorema de Fermat, verifique se o número 341 é primo ou composto.

Solução: Usando o mesmo procedimento do exemplo anterior, temos que 2^{10} deixa resto 1 quando dividido por 341. Logo $(2^{10})^{34}$ deixa resto igual a $1^{34} = 1$ quando dividido por

341. Temos também que 2^1 deixa resto 2 quando dividido por 341. Assim $2^{341} = 2^{340}.2^1$ deixa resto igual a 1·2 quando dividido por 341. Logo, pelo teste de Fermat, não podemos afirmar se ele é primo ou composto. Mas 341 = 31·11, logo é um número composto.

Por muito tempo, mesmo antes de Cristo, achava-se que se 2^p deixasse resto 2 quando dividido por *p*, então *p* deveria ser um número primo. Hoje sabemos que esse teste não é suficiente para garantir a primalidade de um número.

Uma maneira equivalente de se apresentar o Pequeno Teorema de Fermat é a seguinte.

Seja *p* um número primo e *a* um número natural não divisível por *p*, logo temos que:

$p|a^{p-1} - 1$.

Demonstração: Pelo Pequeno Teorema de Fermat $p|a^p - a$, logo $p|a(a^{p-1} - 1)$, como $p \nmid a$ pela proposição 2.1.5 temos que $p|a^{p-1} - 1$, completando assim a demonstração.

□

Apesar de ser de fácil aplicação o Pequeno Teorema de Fermat, é útil para verificar se um determinado número não é primo, pois qualquer número que falhe no teste seguramente não será primo. No entanto, se um determinado número passar no teste, não se pode afirmar com toda a certeza se ele será primo ou composto, pois existem números que sempre passam no referido teste. Esses números que passam sempre pelo teste de Fermat são chamados os números de Carmichael, números assim conhecidos em referencia a quem estudou esses números. No entanto quem os descobriu foi Alwin Reinhold Korselt (1864-1947). Fazendo parte também do grupo dos pseudoprimos, mesmo não sendo os únicos. São chamados assim por se comportarem de maneira parecida com os números primos. Os números de Carmichael são infinitos, fato este provado em 1994 pelos matemáticos Willian Alford, Andrew Ganville e Carl Pomerance. Apesar de serem infinitos, só existem 2163 números de Carmichael menores que 25000.000.000, 255 são menores que 100.000.000 e apenas 16 deles são menores que 100.000; são eles os números 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745,63973 e 75361.

Mesmo sabendo que se um determinado número passar no teste de Fermat não será necessariamente primo, as chances de ser um número primo é muito grande. O grande gênio matemático húngaro Paul Erdos (1913-1996) estimou, embora não tivesse uma prova conclusiva para este fato, que se um determinado número menor que 101^{50} passasse no teste

de Fermat uma única vez, as chances de não ser primo seria 10^{-43}. Ou seja, de posse de uma lista dos números de Carmichael, o teste de Fermat em pelo menos duas bases diferentes é quase que suficiente para verificar se um determinado número relativamente pequeno é primo ou composto.

Como exemplo, iremos novamente verificar se 341 é composto.

Como na base dois, o teste foi inconclusivo. Testaremos agora na base três. Logo, 3^6 deixa resto 47 quando dividido por 341, 3^{12} deixa resto 163. Continuando o processo, veremos que 3^{341} deixa resto 168 e não 3, logo conclui-se que ele é composto.

Existem outros testes para verificar se um determinado número é primo ou composto. Dentre eles, podemos citar o teste de *Miller- Rabin*, que tem como base o Pequeno Teorema de Fermat com uma pequena modificação que o torna mais eficaz, mas ainda existe uma chance pequena de erro; e também o teste de primalidade AKS, que se trata de um algoritmo que executa em tempo polinomial o teste de primalidade que também usa como base o Pequeno Teorema de Fermat.

Nota-se o quanto o Pequeno Teorema de Fermat é de fato de grande importância no passeio pelo universo tão maravilhoso, que é a busca pelos infinitos números primos desconhecidos.

4. MODELOS DE SEQUÊNCIAS DIDÁTICAS

Neste capítulo são oferecidas duas propostas didáticas de abordagens do estudo dos números primos. Uma está direcionada para o sexto ano do Ensino Fundamental, seção um deste trabalho, e a outra direcionada para o nono ano da mesma etapa de ensino, correspondendo a seção dois. Na seção três deste capítulo são oferecidos alguns jogos envolvendo números primos, que poderão ser usados a fim de tornar atrativo o estudo destes números, mudando assim a rotina das aulas, onde o professor pode escolher quais dos jogos ele poderá utilizar, levando-se em conta a realidade de sua sala de aula.

4.1. Proposta de introdução 6º ano

Observe a seguinte sequência de números naturais:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

O número 1 possui apenas um divisor que é ele mesmo; os divisores do número 2 são 1 e 2; os divisores do número 3 são 1 e 3; os divisores do número 4 são 1, 2 e 4; os divisores de 5 são 1 e 5, os divisores de 6 são 1, 2, 3 e 6; os divisores de 7 são 1 e 7; os divisores de 8 são 1, 2, 4 e 8; os divisores de 9 são 1, 3 e 9 e os divisores de 10 são 1, 2, 5 e 10.

O que se observa com este fato é que alguns desses números têm uma característica em comum: possuir apenas dois divisores, que são 1 e ele próprio. Esses números especiais que possuem apenas dois divisores são chamados "*Números Primos*".

Número Primo é todo número natural maior do que 1 que possui exatamente dois divisores que são o 1 e ele próprio.

Logo, da sequência acima, podemos afirmar que os números 2, 3, 5 e 7 são primos. Já os números que possuem mais de dois divisores distintos são chamados de números compostos. Notamos também, a partir da definição, que o número 1 não é um número primo e também não é um número composto.

Assim, temos que os números naturais maiores que zero se dividem em três grupos:

I. O número 1;

II. Os números primos;

III. Os números compostos.

Exercícios

1) Qual o menor número natural Primo?

2) Liste os dez primeiros números naturais primos?

3) Lucas levou um pacote de balas para os seus amigos e observou o seguinte:

i) se as dividisse por 4, sobraria uma bala;

ii) se as dividisse por 7, também sobraria uma bala;

iii) se as dividisse por 3, sobrariam duas balas.

Quantas balas Lucas levou, sabendo que o número de balas corresponde a um número primo inferior a 30?

4) Existe algum número primo que também é composto?

5) Existe algum número natural par maior do 2 que é primo?

6) O zero é um número primo?

7) Existe algum número natural maior do que 5, terminado em 5, que é um número primo?

8) Verifique que todos os números pares maiores do que 2 e menores que 20 podem ser escritos como a soma de dois números primos.

9) A soma de dois números primos é 30. Sabendo que a diferença entre esses dois números é 4, quais são esses dois números?

4.1.1. Métodos para verificar se um determinado número é primo ou composto

Há muito tempo atrás os gregos já se perguntavam como se pode saber se um determinado número é primo ou composto. Mesmo depois de tanto tempo não se descobriu nenhum algoritmo capaz de verificar através de um teste simples se um determinado número é

um primo. Vejamos agora alguns métodos de se verificar a primalidade de um determinado número.

Crivo de Eratóstenes.

O grego Eratóstenes (276 – 194 a.C.) ficou muito conhecido por ser o primeiro a calcular, com certo grau de precisão, a circunferência da terra. Eratóstenes se destacava não só em Matemática, mas em vários campos do conhecimento de sua época. Foi também criador do método que calcula todos os primos até um número pré-determinado, método esse conhecido como *Crivo de Eratóstenes.*

Vejamos como funciona este processo:

Como exemplo, iremos calcular todos os números primos menores que 50.

✓ Primeiro construímos uma tabela com todos os naturais menores que ou iguais a 50 e retiramos o 1, pois sabemos que ele não é primo.

	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

✓ O primeiro número da lista que sobra é primo, depois retiramos todos os múltiplos do dois, ou seja, todos os pares.

	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~~

✓ O próximo da lista, no caso o 3, é primo. Agora retiraremos todos os múltiplos ímpares do 3 a partir do 3^2.

	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~~

- ✓ Logo o número 5 também será primo. Agora retiraremos todos os múltiplos ímpares do 5 a partir do 5^2.

	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~~

- ✓ O 7, que é o próximo da lista, será primo. Logo iremos retirar todo os múltiplos ímpares do 7 a partir do 7^2.

	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~~

Terminando assim o processo, pois o maior número a ser checado corresponde, no máximo à raiz quadrada do maior valor arredondado para baixo. Logo, como nesse caso, o maior valor é 50, o maior número primo que precisamos testar é o 7. Assim os números que restaram na tabela acima são os números primos menores que 50.

Método das divisões sucessivas

O funcionamento desse método é bastante simples, precisando seguir os seguintes passos:

Para verificar se um determinado número é primo, teremos que verificar se esse número não é divisível por nenhum primo menor que raiz quadrada deste número. Neste caso, a

igualdade não se aplica, pois, se ele possuir raiz exata, será um número composto. Caso ele não seja divisível por nenhum dos primos, ele será um número primo.

Como exemplo, iremos verificar se 53 é primo.

Para isso, teremos de verificar se 53 não é divisível por 2, 3, 5 e 7, que são os números primos menores que a raiz quadrada de 53. Como 53 é ímpar, logo não será divisível por 2, 53 deixa resto 2 quando dividido por 3, deixa resto 3 quando dividido por 5 e deixa resto 4 quando divido por 7. Logo concluímos que 53 é um número primo.

Exercícios:

1) Usando a tabela abaixo, verifique se 67 é primo usando o Crivo de Eratóstenes.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70

2) Verifique se 73 é primo usando o método das divisões sucessivas.

3) Quantos são os números primos compreendidos entre 1 e 100?

4) Dos números 37, 43, 47, 49, 51, 53, 55 e 57, quais deles são primos?

5) Marque a alternativa correta

a) 7 e 11 são ambos números primos;

b) 7 e 11 tem dois divisores em comum;

c) 7 é composto e 11 é primo;

d) 7 é primo e 11 é composto.

Decomposição de um número em fatores primos

Sabe-se que todo número natural pode ser decomposto em fatores primos. Vejamos a decomposição em fatores primos dos seguintes números:

60 = 2.2.3.5

15 = 3.5

39 = 3·13

Quando decompomos um determinado número em fatores primos, estamos usando o *Teorema Fundamental da Aritmética*, cujo enunciado é o seguinte.

"*Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos*".

Vejamos agora alguns processos de decompor um número composto em fatores primos.

Processo das divisões sucessivas

O funcionamento deste processo é bem simples, vejamos o exemplo.

Vamos decompor 210 em fatores primos.

- Primeiro fazemos a divisão do número 210 pelo menor número primo possível, no caso o 2, logo 210/2 = 105.
- Prosseguimos o processo novamente efetuando a divisão pelo menor primo possível, no caso o 3, logo 105/3 = 35.
- Continuamos o processo até encontrarmos o 1 como quociente. Assim 35/5 = 7, 7/'7 = 1. Logo a decomposição do número 210 em fatores primos é 2·3·5·7.

Processo das fatorações sucessivas

Veja, como exemplo, a fatoração do número 30 utilizando o processo das fatorações sucessivas.

30 = 2·15, como 2 é primo iremos fazer a fatoração do 15, onde 30 = 2·15 = 2·3·5, como 3 e 5 são também números primos, concluímos assim que a decomposição do número 30 em fatores primos é 30 = 2·3·5.

Exercícios:

1) Quais são os fatores primos de 7000?

2) O número 18018 é divisível por 231? Se for, qual é o resultado da divisão?

3) Dentre os números abaixo, existe um que é divisível por 2, 3, 5, 7, 11. Qual é esse número?

a) 1111

b) 1155

c) 2110

d) 2310

4) A fatoração do número 300 em fatores primos é:

a) $3 \cdot 2 \cdot 2 \cdot 5 \cdot 5$

b) $3 \cdot 10 \cdot 10$

c) $3 \cdot 100$

d) $1 \cdot 300$

5) Determine o número natural cuja decomposição em fatores primos é:

a) $2 \cdot 3 \cdot 5 \cdot 7$

b) $5 \cdot 7 \cdot 11$

c) $2^2 \cdot 3 \cdot 5^2$

d) $2^0 \cdot 3^3 \cdot 5$

6) Um professor possui um número x de balas e pretende dividi-las com todos os 35 alunos de sua sala aula. Sabendo que a quantidade de balas que ele possui é divisível por 5 e 7 é possível que ele distribua todas as suas balas de maneira que todos os alunos recebam a mesma quantidade?

7) Analisando o número 109 responda:

a) Quantos e quais são os seus divisores?

b) Pode-se concluir que 109 é um número primo?

8) Enuncie o Teorema Fundamental da Aritmética?

9) Dê a decomposição em fatores primos dos seguintes números usando o método das divisões sucessivas.

a) 42;

b) 47;

c) 63;

d) 77.

10) Dê a decomposição em fatores primos dos seguintes números usando o método das fatorações sucessivas.

a) 27;

b) 51;

c) 75;

d) 88.

4.2. Proposta de introdução 9º ano

Definição:

Um número natural p > 1 e que só tem dois divisores distintos, 1 e o próprio p, é chamado de *número primo.* Caso tenha mais de dois divisores é chamado de composto.

Da definição podemos deduzir que 1 não é número primo, e também que o único número natural par que é primo é o 2. Logo os números 2, 3, 5, 7,11, 13, 17, 19 são todos primos. Já os números 4, 6, 8, 9, 10, 12, 14, 15, 16, 18 e 20 são todos compostos.

Assim, podemos classificar os números naturais maiores que zero em três grupos:

I. O número 1;

II. Os números primos;

III. Os números compostos.

Métodos para calcular primos

Saber identificar de uma forma simples se um número é primo ou composto sempre foi uma obsessão dos matemáticos, obsessão esta que já perdura por mais de dois milênios. Mesmo com todo o desenvolvimento que a matemática alcançou, não foi possível descobrir esse teste, pelo menos não de forma tão simples.

Com relação aos métodos a serem utilizados para verificar a primalidade de um número, destacamos aqueles que serão o objeto de estudo desta seção, que são eles: O crivo de Eratóstenes, o método das divisões sucessivas e o Pequeno Teorema de Fermat.

Relembraremos o funcionamento do crivo de Eratóstenes.

Primeiro, deve-se criar uma tabela com todos os números a partir do 1 até o valor limite. Em seguida, calcular a raiz quadrada do valor limite, fazendo os testes com todos os números primos menores que a raiz quadrada calculada, procedendo da seguinte maneira:

- O 1 não é primo, logo deve ser riscado da lista, o próximo da lista que sobra é o 2 que é um número primo;
- Em seguida, risca todos os pares maiores que o 2, o próximo número da lista que sobra é o 3, que é primo;
- Agora se deve retirar da lista os múltiplos ímpares do número 3 a partir do 3^2, o próximo da lista que é o 5, é primo. O procedimento deverá prosseguir até o maior primo inferior à raiz quadrada do valor limite.

Já para o caso do método das divisões sucessivas, deve-se testar com todos os primos menores que a raiz quadrada do valor limite. Caso o número a ser testado falhe para algum dos primos, concluímos tratar-se então de um número composto.

Pequeno Teorema de Fermat

Pierre de Fermat (1601 – 1665) é considerado o maior matemático francês de seu tempo, deixando um vasto acervo de contribuições em vários campos da Matemática, inclusive sobre os números primos. Dentre a suas contribuições, destacamos Pequeno Teorema de Fermat, que será nosso objeto de estudo, cuja demonstração se encontra no capítulo três deste trabalho.

"Dado um número p primo, tem-se que $a^p - a$ é divisível por p para todo $a \in \mathrm{N}$."

Que pode ser escrito de maneira equivalente da seguinte forma:

"Seja p um número primo e a um número natural não divisível por p logo temos que $p|a^{p-1} - 1$."

Vejamos alguns exemplos:

Exemplo 1: $3|2^3 - 2$, pois $2^3 - 2 = 8 - 2 = 6$ e $3|6$;

Exemplo 2: $5|4^5 - 4$, pois $4^5 - 4 = 1024 - 4 = 1020$ e $5|1020$.

Exemplo 3: $5|2^4 - 1$, pois $2^4 - 1 = 16 - 1 = 15$ e $5|15$;

Exemplo 4: $7|3^6 - 1$, pois $3^6 - 1 = 729 - 1 = 728$ e $7|728$.

Exemplo 5. Usando o Pequeno Teorema de Fermat, verifique se o número 341 é primo ou composto.

Para resolvermos este exemplo usaremos a Proposição 3.1.5, cuja demonstração se encontra no capítulo 3 deste trabalho, com o seguinte enunciado:

Se a divisão euclidiana de m por a deixa resto b com $a, b, m \in \mathrm{N}$ e $b < a$ então m divido por a^n deixa resto b^n.

Solução: Pela proposição acima temos que 2^{10} deixa resto 1 quando dividido por 341, logo $2^{340} = (2^{10})^{34}$ deixa resto igual a $1^{34} = 1$ quando dividido por 341, temos também que 2^1 deixa resto 2 quando dividido por 341. Assim $2^{341} = 2^{340}.2^1$ deixa resto igual á 1.2 quando dividido por 341. Logo, pelo teste de Fermat, não podemos afirmar se ele é primo ou composto. Mas 341 = 31.11, logo é um número composto.

Observação: O teste de Fermat é muito útil para verificar se um determinado número é composto, pois, se um determinado número não passar uma única vez no teste já é suficiente para afirmar que ele não é primo. No entanto, se ele passar no teste, nada se pode concluir, pois existem alguns números que passam pelo teste de Fermat em todas as bases. Esses números são conhecidos como *números de Carmichael*, sendo que o menor deles é 561, existindo apenas 16 deles menores que 100.000, apesar de existir tão pouco desses números no intervalo apresentado anteriormente, pois eles são infinitos.

No entanto, o grande matemático húngaro Paul Erdos (1913 – 1996) estimou, mesmo sem uma prova irrefutável, que se um número menor do que 101^{50} tivesse passado no teste de Fermat uma única vez, as chances de ser um número primo eram muito altas, sendo da ordem de 10^{-43}. Logo, de posse de uma lista contendo os *números de Carmichael* até o intervalo desejado e fazer o teste de Fermat com pelo menos duas bases diferentes é quase suficiente para verificar se o número a ser testado é primo ou composto.

No capítulo três desse trabalho encontra-se a lista dos 16 primeiros *números de Carmichael* citados anteriormente.

Primos gêmeos

Sejam p e q dois números primos e, sem perda de generalidade, considere $p < q$, serão chamados de primos gêmeos se a diferença entre eles sempre for módulo dois, ou seja, $p = q + 2$.

(3, 5); (5, 7); (11, 13); (17, 19) são os pares de primos gêmeos menores do que 20.

Ainda não se pode afirmar se existem infinitos pares de primos gêmeos, onde a conjectura dos primos gêmeos é mais um problema que continua em aberto sobre os números primos.

Exercícios:

1) (Banco de questões OBMEP - 2008) A soma é 100 – A soma de 3 números é 100, dois são primos e um é a soma dos outros dois.

a) Qual é o maior dos 3 números?

b) Dê um exemplo desses 3 números.

c) quantas soluções existem para esse problema?

2) (Banco de questões OBMEP - 2008) Palíndromos – O ano de 2002 é *palíndromo* porque é o mesmo quando lido da direita para a esquerda.

a) Qual será o próximo palíndromo depois de 2002?

b) O último ano palíndromo, 1991, era ímpar. Qual será o próximo ano palíndromo ímpar?

c) O último ano palíndromo primo ocorreu há mais de 1000 anos, em 929. Quando ocorrerá o próximo ano palíndromo primo?

3) Usando a tabela abaixo, verifique se 113 é primo usando o Crivo de Eratóstenes.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84

85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	102	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120

4) Usando a tabela abaixo responda:

a) Calcule todos os números primos menores que 200 usando o Crivo de Eratóstenes?

b) Quantos e quais são os pares de primos gêmeos menores que 200?

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	82	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

5) Verifique se 197 é primo usando o método das divisões sucessivas.

6) Sabendo que os números 7 e 11 são ambos primos, $7^2 + 11^2$ também será um número primo?

7) Seja p e q dois números primos ímpares, $p^2 + q^2$ também será um número primo?

8) Sabendo que 79 é um número primo, qual o resto da divisão de 2^{79} por 7?

9) Verifique se o número 511 é primo ou composto usando o Pequeno Teorema de Fermat.

10) Qual o resto da divisão de 2^{46} por 47?

11) Qual o resto da divisão de 5^{37} por 3?

12) Dados os números 1, 27, 53, 71, 83, 85, 89, 91 e 97. Quais deles são primos?

13) Um determinado número deixa resto 1 quando dividido por 2, deixa resto 1 quando dividido por 3, 4 quando dividido por 5, 2 quando dividido por 7.

a) Sabendo que este número é inferior a 100, podemos afirmar que ele é primo? Justifique.

b) Qual o número procurado?

c) Qual o primeiro número maior que 100 com as características descritas acima?

Decomposição de um número natural em fatores primos

Sabe-se, há muito tempo, que um determinado número maior do que 1 ou é primo ou pode ser formado como um produto de fatores primos, no qual destacamos o *Teorema Fundamental da Aritmética*, cuja definição é a seguinte:

"*Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos*"

Vejamos alguns exemplos da decomposição em fatores primos:

Exemplo 1: decomponha os números 60 e 95 em fatores primos

$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$

$95 = 5 \cdot 19$.

Exemplo 2: Verifique se o número 945 é divisível por 63.

Solução:

Decompondo os números dados em fatores primos temos $945 = 3^3 \cdot 5 \cdot 7$ e $63 = 3^2 \cdot 7$, logo temos que ele é divisível e o resultado da divisão é $3 \cdot 5 = 15$.

Exercícios

1) Marque a alternativa correta:

a) 7 e 9 são ambos números primos;

b) 7 e 9 tem dois divisores em comum;

c) 7 e 9 são ambos compostos;

d) 7 é primo e 9 é composto.

2) Dentre os números abaixo existe um que é divisível por 2, 3, 5, 7, 11. Qual é esse número?

a) 1111

b) 1155

c) 2110

d) 2310

3) A fatoração completa do número 5000 é:

a) $5^3 \cdot 2^4$

b) $5^4 \cdot 2^4$

c) $5^4 \cdot 2^3$

d) $5^3 \cdot 2^3$

4) O número 180180 é divisível por 2310? Se for qual é o resultado da divisão?

5) O número 91 é primo? Justifique.

6) (Banco de questões OBMEP – 2015 ADAPTADA). João possui mais que 30 e menos que 100 chocolates. Se ele organizar os chocolates em linha de 7, sobrará um. Caso ele organize em linhas de 10, sobrarão 2.

a) Podemos afirmar que ele possui um número primo de chocolates? Justifique.

b) Quantos chocolates ele possui?

c) Este problema possui solução caso João tivesse uma quantidade inferior a 30 chocolates? Justifique.

7) Usando a decomposição em números primos, simplifique até que se tornem irredutíveis as seguintes frações:

a) 725/75;

b) 123/63;

c) 1280/165;

d) 3132/612.

e) 3510/105

8) Usando a decomposição em fatores primos, calcule a raiz quadrada dos seguintes números:

a) 1764;

b) 1225;

c) 900;

d) 5929.

9) Usando a decomposição em fatores primos, calcule a raiz cúbica dos seguintes números:

a) 42875;

b) 216;

c) 1728;

d) 9261.

4.3. Jogos e atividades

Os jogos e as atividades matemáticas, quando usados corretamente, são um recurso pedagógico de grande importância no ensino-aprendizagem, fazendo com que, a partir dos desafios oferecidos, nossos alunos desenvolvam, além de outros aspectos, a concentração, a criatividade e a habilidade para resolver problemas, permitindo que eles se sintam envolvidos e estimulados, retirando o bloqueio existente em alguns discentes no que diz respeito a aprender Matemática, melhorando assim a relação com essa importante área de estudo.

Nesta seção são oferecidos alguns jogos e atividades, envolvendo números primos, que o professor poderá usar em suas aulas.

4.3.1. Formando retângulos

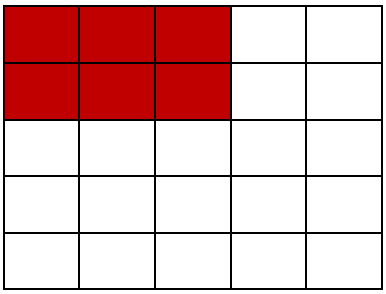
O objetivo deste jogo é formar retângulos com ambas as dimensões maiores que uma unidade.

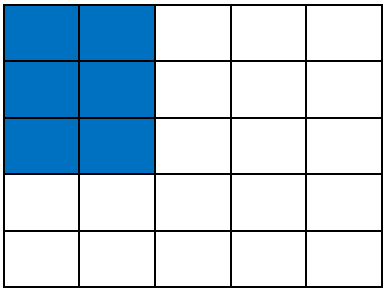
Material necessário: Papel quadriculado, grãos de feijão ou milho.

Normas do jogo:

O professor sorteia alguns números que representam a área de retângulos e as equipes tentam formar estes retângulos, com o comprimento e largura maiores do que uma unidade.

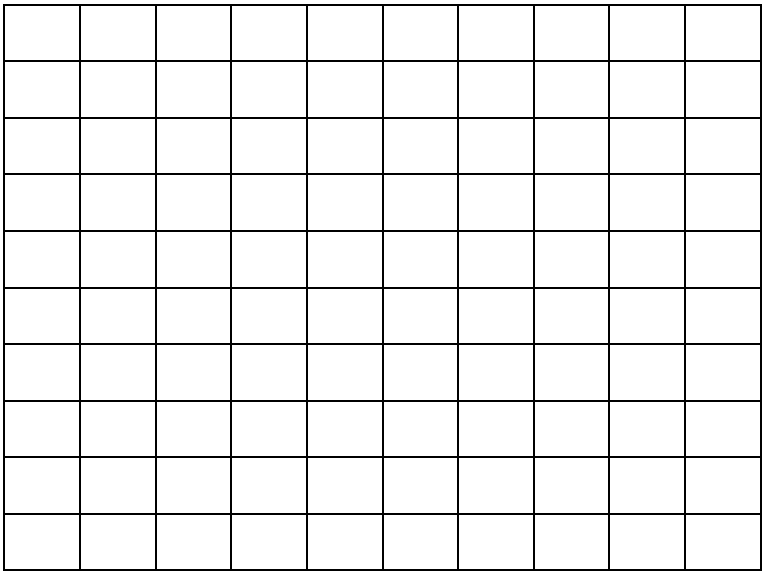
Exemplo: Caso o número a ser sorteado seja 6, logo teremos os seguintes casos:

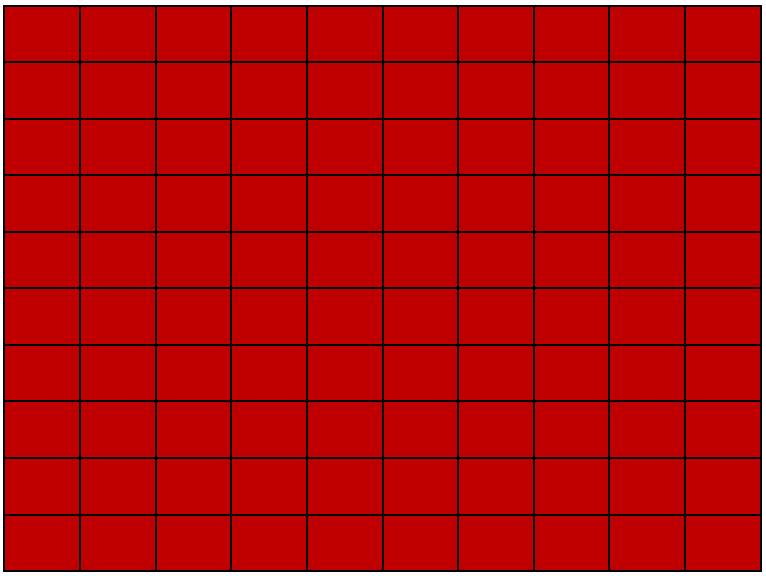




Observações:

- Cabe ao professor levantar a seguinte questão: por que alguns números não formam retângulos usando a regra dada acima?
- Caso não haja uma resposta satisfatória, cabe ao professor informar que aqueles números que não formam retângulos usando a regra dada acima são números primos.
- Não necessariamente o material a ser utilizado deve ser grãos de feijão ou milho, eles podem ser substituídos, caso o professor ache conveniente, por outro material, como por exemplo, como o que foi utilizado no exemplo acima, por papel quadriculado colorido recortado.





4.3.2. Descobrindo a senha.

O objetivo deste jogo é fazer com a equipe consiga abrir um documento contendo uma mensagem salva em um computador ou tablet protegida por uma senha.

Normas do jogo:

Primeiro, o professor cria algumas mensagens e as salva na área de trabalho com uma senha diferente para cada mensagem, informando que a equipe tem apenas uma tentativa para cada documento, sendo dada como pista o número n onde $n = p \times q$, com p e q ambos números primos, onde a equipe tentará decompor o número n descobrindo assim a senha que será os números p e q escritos da seguinte maneira: no campo “senha” digita pq.

Exemplo 1: Suponha que o documento a ser aberto tenha como pista o número 187. Logo usando a decomposição em fatores primos do número 187, temos que 187 = 11x17. Assim, no campo senha, deverá ser digitado 1117ou 1711 tendo assim acesso ao arquivo.

Exemplo 2: Suponha que o documento a ser aberto tenha 210 como pista. Usando a decomposição em fatores primos, temos que 210 = 2x3x5x7. Assim no campo senha deverá ser digitado 2357 ou 7532 abrindo o arquivo.

Observações:

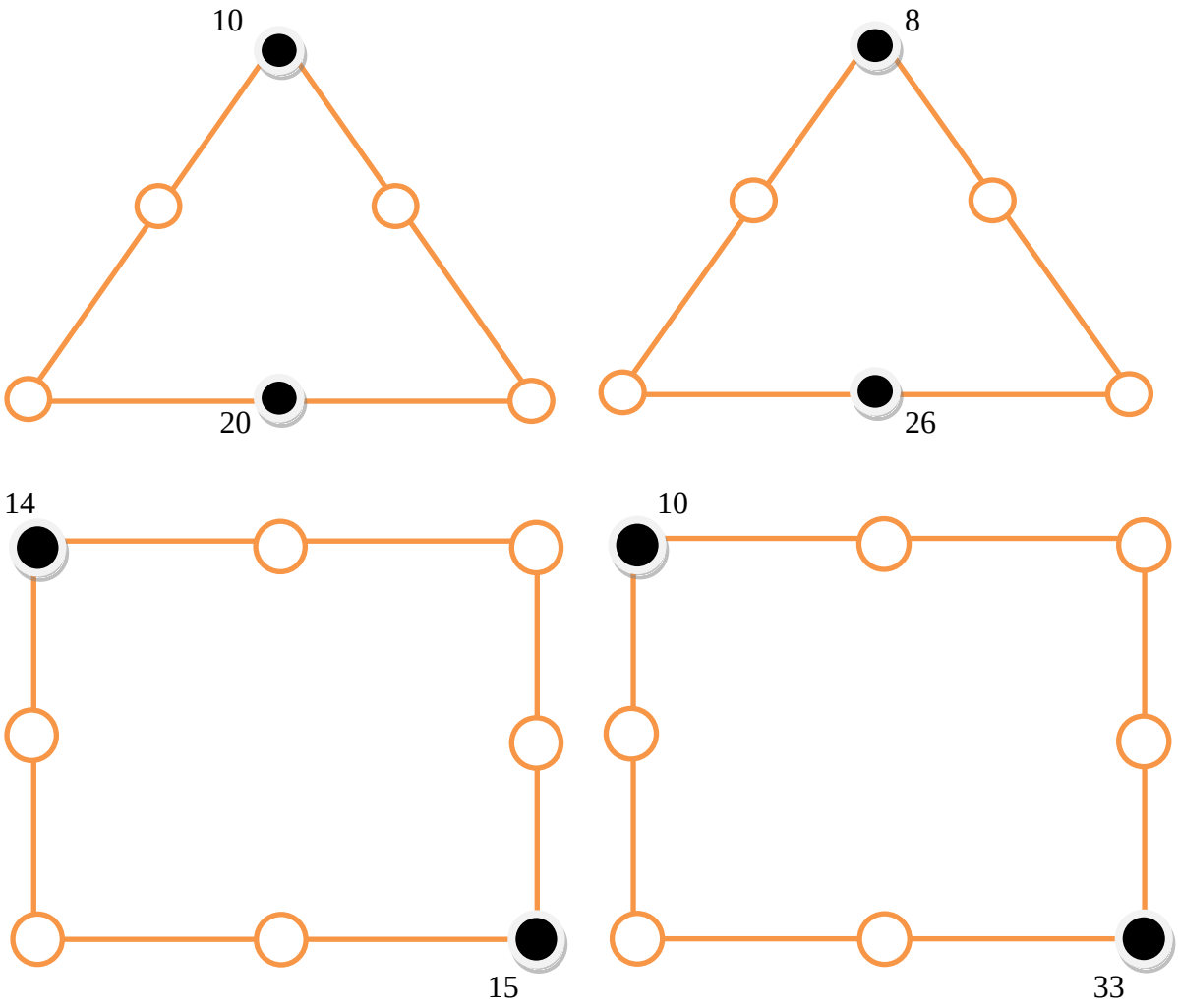
- Cabe ao professor informar se os números p e q vão ser escritos na forma crescente ou decrescente;
- É interessante que as senhas estejam em ordem crescente de dificuldade;

- Ganha o jogo a equipe que conseguir decifrar o maior número de senhas, abrindo assim o maior número de mensagens.
- Cabe ao professor definir a quantidade de participantes por equipe, sendo que o ideal seria três participantes em cada grupo.

4.3.3. Preencha os espaços nos triângulos e retângulos abaixo usando apenas números primos

Normas:

Você deve preencher os espaços que faltam nos triângulos e retângulos abaixo usando as operações adição, subtração, multiplicação e divisão, usando apenas os números primos.



Observações:

- Não necessariamente você deverá usar todas as operações em uma mesma figura;
- Não pode haver números repetidos em uma mesma figura;
- Cada espaço que falta pode apenas ser preenchido com números primos.

4.3.4. Crisson

Este jogo é uma adaptação do jogo Crisson encontrado na Revista do Professor de Matemática nº 76, cuja autoria pertence aos professores Edílson da Silva Campos e Crisângela Avila Nunes.

Vejamos como funciona o jogo:

Nas linhas (horizontais), cada número dentro de uma célula que for precedido por duas outras células preenchidas será a soma desses dois números.

Nas colunas (verticais) o processo é semelhante, só que usando a multiplicação, ou seja, cada número dentro de uma célula que for precedido por duas outras células preenchidas será a soma desses dois números.

Na prática teremos o seguinte: da esquerda para a direita teremos a adição, da direita para a esquerda, subtração; de cima para baixo, multiplicação, de baixo para cima divisão.

Vejamos o exemplo:

■			12	■
6	■	4	■	
			11	
30	■		■	19
■			270	■

■	10	2	12	■
6	■	4	■	1
5	3	8	11	19
30	■	32	■	19
■	14	256	270	■

Preencha os espaços em branco e depois liste os números primos que aparecem nos seguintes exemplos:

■			24	■
8	■		■	
		10		
56	■		■	253
■	37		237	■

■			12	■
4	■		■	
		6		
20	■		■	143
■	23			■

Observações:

- Como pré-requisito é necessário o domínio das quatro operações, além de reconhecer quando um determinado número é primo;
- Caso essa atividade venha a ser trabalhada em grupo, é interessante que seja executada, no máximo, com quatro pessoas;
- É interessante que sejam relatadas por cada grupo as estratégias de resolução que foram usadas.
- Ao final do jogo o professor pode pedir para que os grupos relatem quais dos números utilizados são primos e quais são compostos.

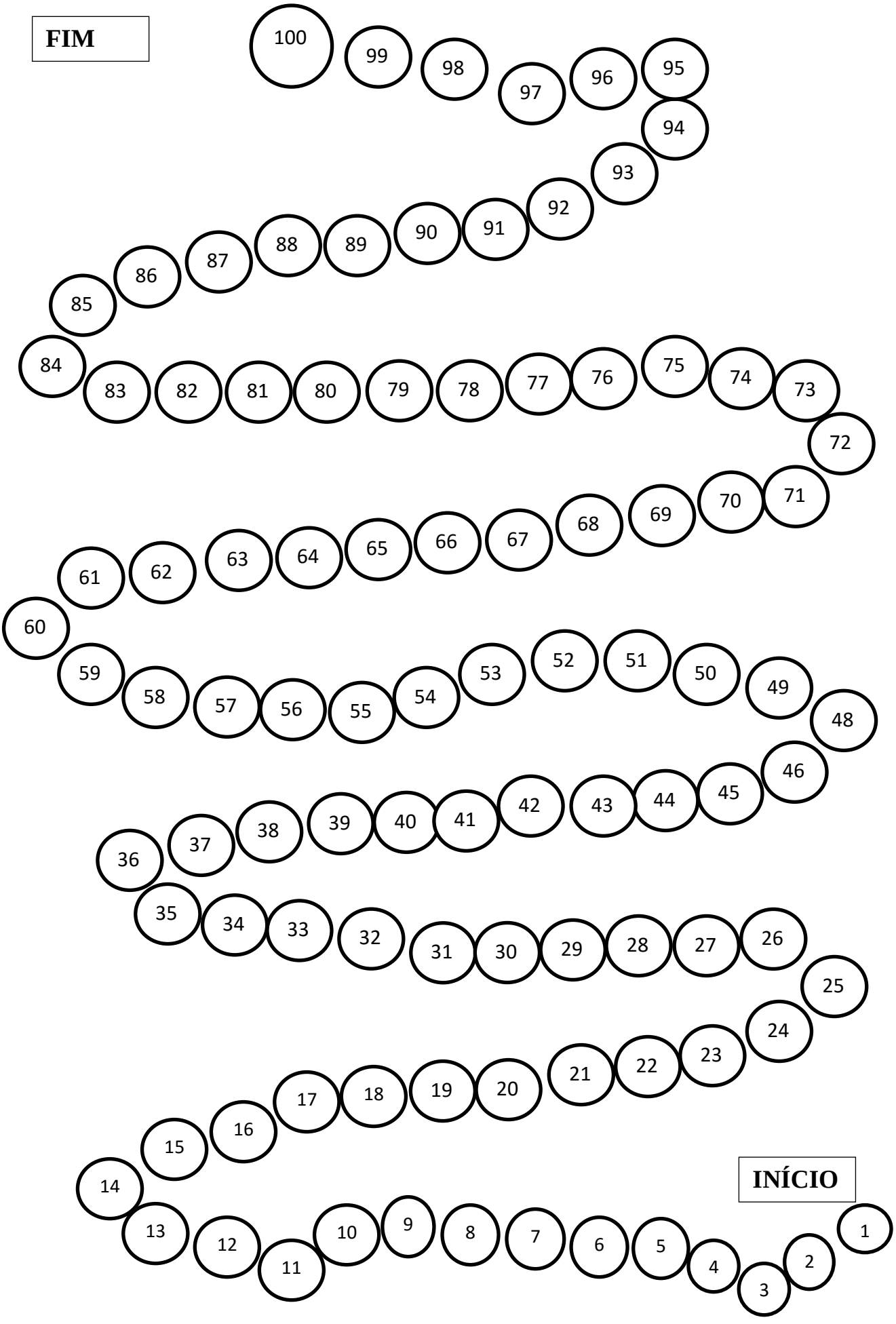
4.3.5. Completando o percurso

O objetivo do jogo é completar o percurso usando para isso os números primos, fazendo com que o aluno distinga os números primos dos compostos na sequência dada.

Normas do jogo:

Joga-se o dado uma vez. O valor que sair na jogada será a quantidade máxima de casas que o jogador poderá percorrer, lembrando que ele deverá escolher um número primo. Caso o número escolhido não seja primo, voltará para o início da última jogada. Cada jogador terá direito a uma única jogada por rodada. Ganha o jogo aquele que primeiro completar o percurso.

Observação: Cabe aos jogadores verificar se o número em questão é primo ou composto. O professor apenas irá verificar se a informação dada é verídica ou não, fazendo sempre a intervenção quando for necessário.


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

4.3.6. Bingo

O objetivo deste jogo é fazer com que os alunos diferenciem os números primos e os números compostos, decompondo os últimos em fatores primos.

Normas do jogo:

Divide-se a sala de aula em grupos, de três pessoas, coloca-se em uma urna uma sequência de números e começa o sorteio, com um intervalo de tempo de um minuto por sorteio. Os grupos devem identificar quais dos números sorteados são primos ou compostos, decompondo os compostos em fatores primos. Ganha o jogo a equipe que obtiver a maior quantidade de acertos.

Observações: Caso o professor ache conveniente, poderá alterar tanto a quantidade de componentes como também o intervalo de tempo entre os sorteios.

4.3.7. Amarelinha dos números primos

Este jogo é encontrado no livro “Os mistérios dos números” p. 47.

Normas do jogo:

O primeiro jogador pega uma ficha e a coloca sobre um número primo que esteja, no máximo, a cinco passos da casa 1. O segundo jogador pega a ficha e a move para um primo maior que esteja a no máximo cinco casas adiante de onde o primeiro jogador a colocou. O primeiro jogador, em seguida, move a ficha para um primo ainda maior que esteja, no máximo, cinco casas adiante. O perdedor é o primeiro jogador incapaz de mover a ficha segundo as regras.

As regras são: (1) a ficha não pode ser movida mais de cinco casas adiante; (2) ela deve ser movida sempre até um número primo; (3) e não pode ser movida para trás nem ficar onde está.

Vejamos um exemplo de como funciona este jogo:

Jogador 1 

Jogador 2 

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

Vemos então, que neste exemplo, o jogador 2 ganhou a partida pois o próximo primo é o 29, que não é possível de ser alcançado pelas regras descritas acima. Convém ressaltar que o jogo foi decidido bem antes do número 23, onde o jogador que colocar a ficha no 5, usando estas regras, ganhará sempre a partida.

Observações:

- Antes de iniciar a partida seria interessante que o professor pedisse a cada participante que calculasse todos os primos até o intervalo desejado.
- Pedir a cada participante vencedor que descreva a estratégia usada. Caso a resposta não seja satisfatória, o professor pode relatar a estratégia descrita acima.
- O professor pode propor este jogo permitindo que os jogadores movam no máximo seis ou sete casas, pedindo que os alunos expliquem qual estratégia deve usar para sempre sair vencedor.

Seguem abaixo as fichas e o tabuleiro que podem ser usados para este jogo.

Jogador 1 

Jogador 2 

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

4.3.8. Forme os números naturais usando apenas números primos

Este jogo é uma adaptação de um problema em particular, cujo enunciado é o seguinte: “Todo número par maior do que 2 pode ser escrito como a soma de dois números primos”, sendo conhecido como a conjectura de Goldbach proposta pelo matemático alemão Christian Goldbach a Leonhard Euler, em 1742, que é um dos problemas mais antigos ainda em aberto em matemática. O segundo critério apresentado é conhecido como a versão “fraca” da conjectura de Goldbach.

Normas:

O professor coloca em uma urna uma série de números naturais maiores que o número 3 e sorteia os números estabelecendo um determinado intervalo de tempo para que as equipes os formem usando apenas os números primos e a adição obedecendo aos seguintes critérios:

1) Caso o número sorteado seja par maior que 2 ou o número 5, poderá ser usado apenas a soma de dois números primos;

2) Caso o número sorteado seja ímpar e maior do que 5, ele irá usar a soma de três números primos.

Observações: (1) Cabe ao professor determinar o intervalo de tempo entre cada sorteio levando sempre em conta o grau de instrução da turma e também a dificuldade do número sorteado; (2) é interessante que o professor peça aos alunos que calculem todos os primos até um intervalo suficiente para os números a serem sorteados.

4.3.9. Balões com números

Regras:

Divide a sala em grupos e coloca os balões contendo números primos e compostos em seu interior. Depois de escolhido o balão, cada equipe irá enchê-lo até estourar, após estourá-lo a equipe deverá recolher os números que estavam em seu interior, separando os primos e os compostos, fazendo a decomposição em fatores primos do último.

Observações:

- As quantidades de números existentes em cada balão deverão ser as mesmas;
- Pode haver repetições de alguns números em balões diferentes;
- Ganha o jogo a equipe que tiver a maior quantidade de acertos;
- Se houver empate, a equipe vencedora será aquela que primeiro terminar a tarefa;
- Cabe ao professor estipular a quantidade de números em cada balão e também o grau de dificuldade, levando sempre em conta o grau desenvolvimento da turma a ser trabalhada.

4.3.10. Jogo dominó com números primos e compostos

O objetivo deste jogo é fazer com que o aluno reconheça um número primo, e também, que saiba decompor um número composto em fatores primos.

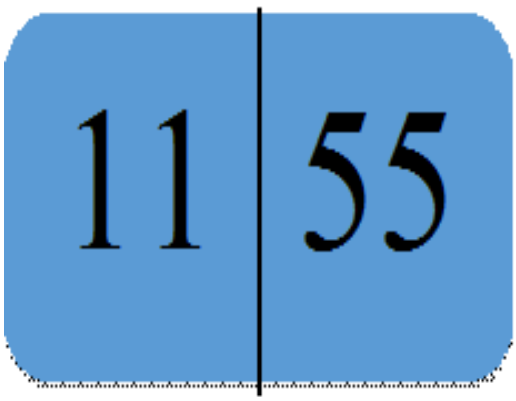
Cada peça do dominó é composta por um número primo de um lado e, um número composto do outro lado.

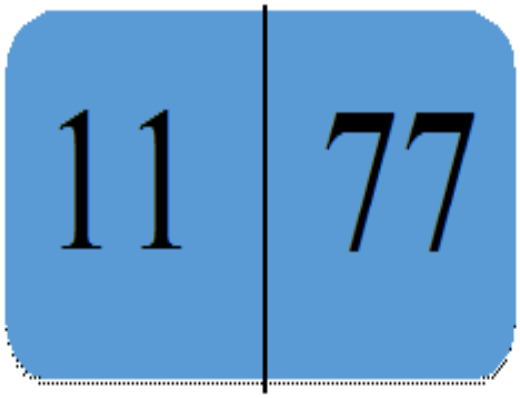
O funcionamento deste Jogo é o seguinte:

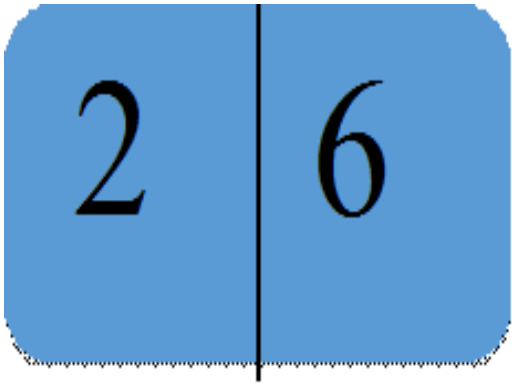
Digamos que você comece o jogo com uma peça que tenha de um lado 2 e, do outro, 21, seu oponente terá que inserir uma peça que seja um múltiplo do 2, que deve ser colocado junto ao 2, ou uma peça que tenha o número 3 ou o 7, que deve ser colocado junto ao 21. Veja o exemplo:

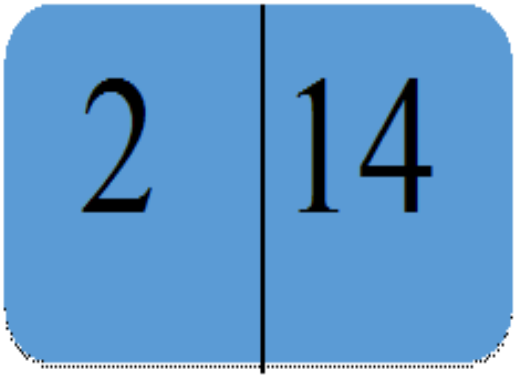
2	21
3	33

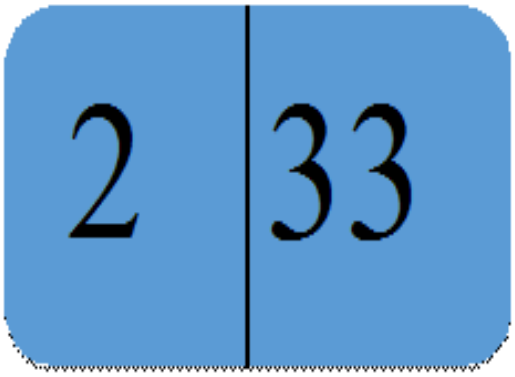
Para continuar o jogo acima, o próximo a jogar teria que ter uma peça com um número múltiplo do dois para inserir do lado esquerdo, ou ter uma peça com um dos lados com os números 3 ou 11, para inserir do lado direito. Ganhando a partida o primeiro a usar todas as peças com as quais iniciou o jogo. Segue abaixo o modelo das peças que você pode recortar e colar em uma superfície mais resistente, como por exemplo, papelão, e usar para jogar esse jogo.

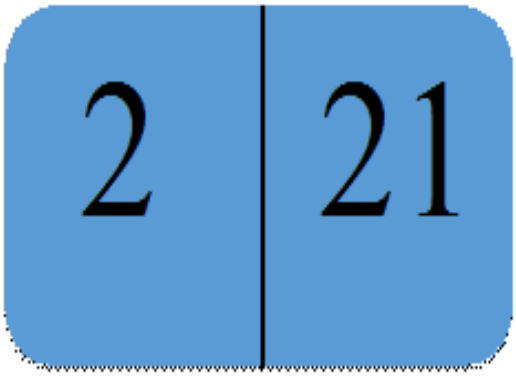


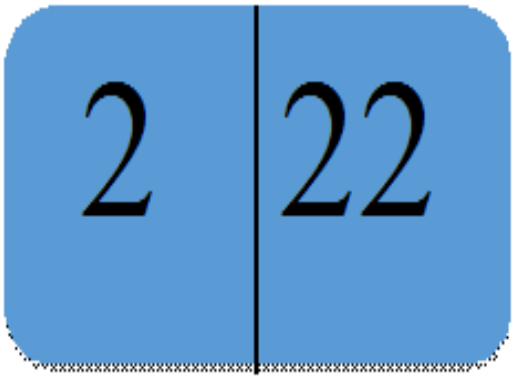


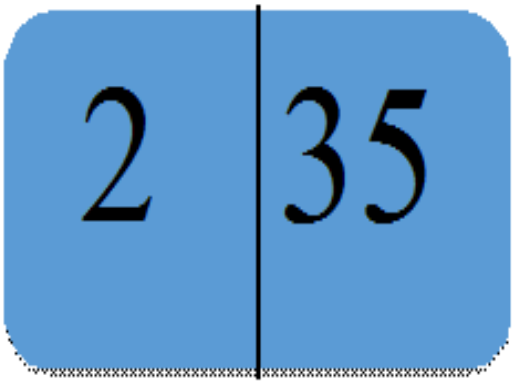

2
6

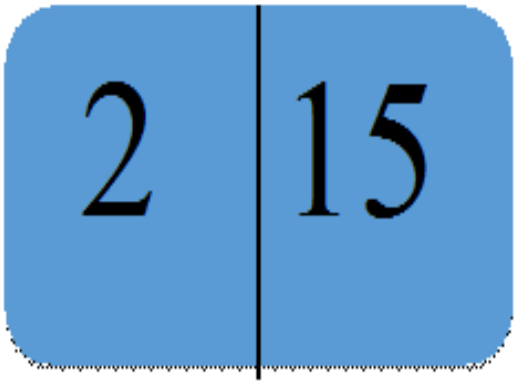

2
14

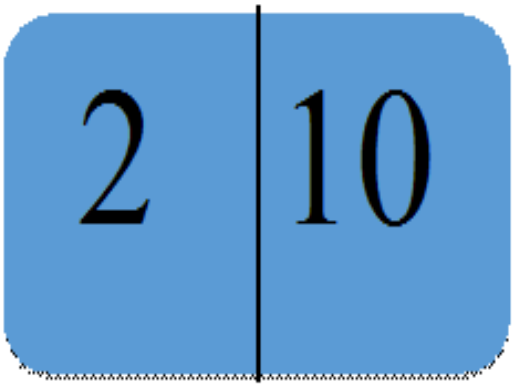

2
33

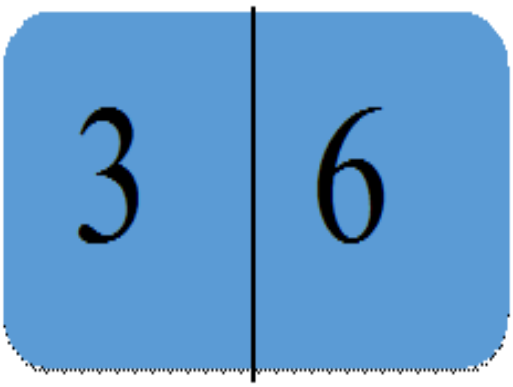

2
21

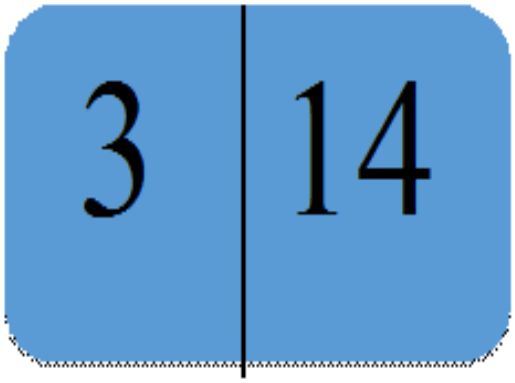

2
22

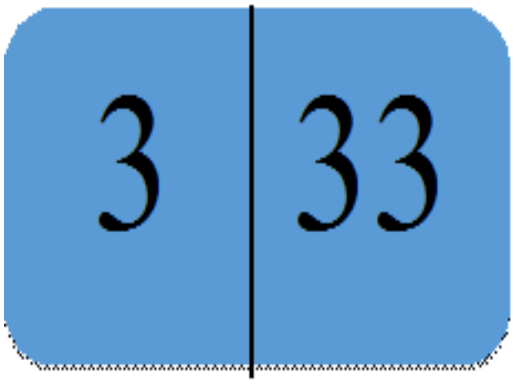

2
35

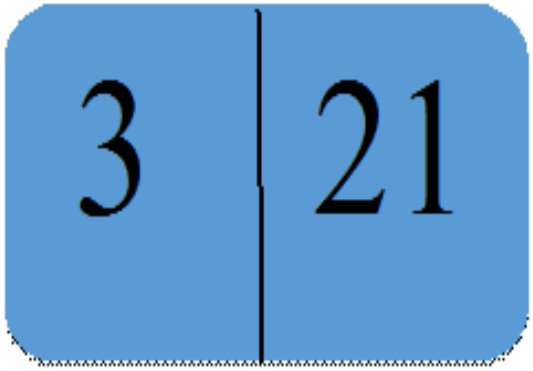

2
15

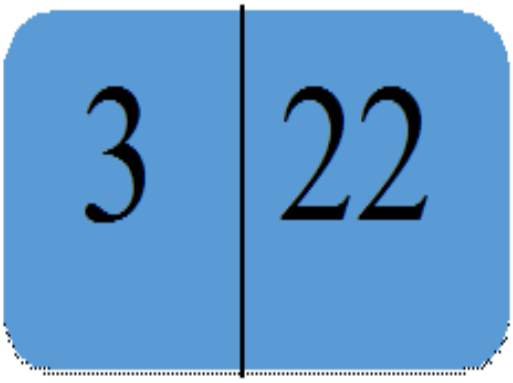

2
10

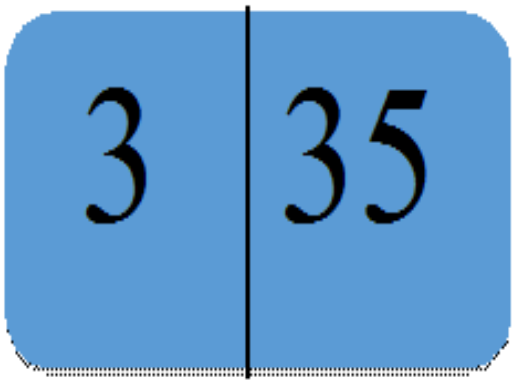

3
6

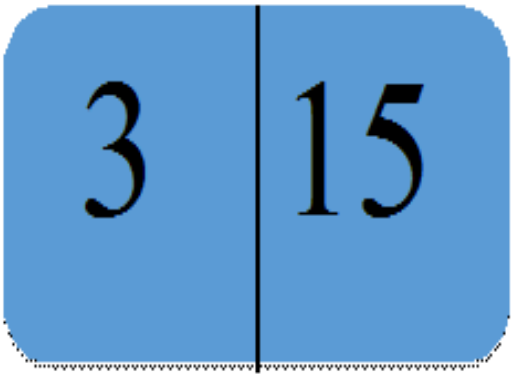

3
14

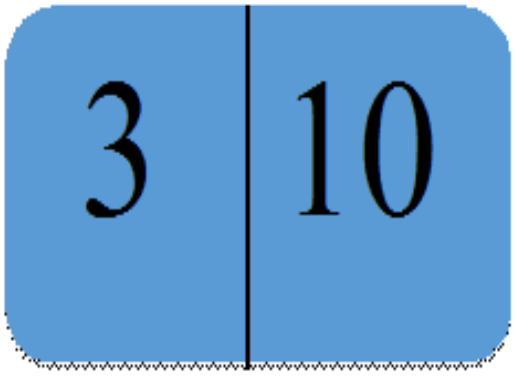

3
33

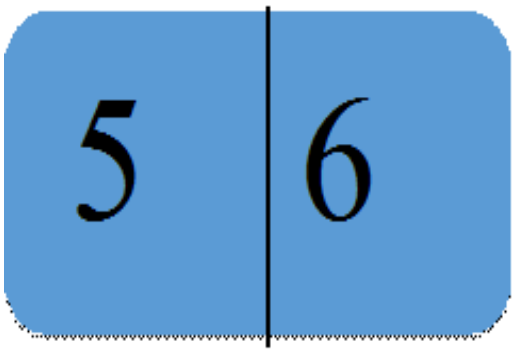

3
21

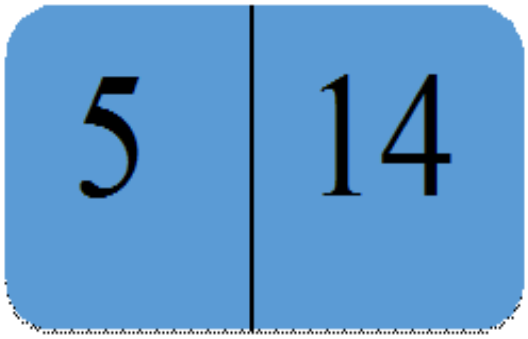

3
22

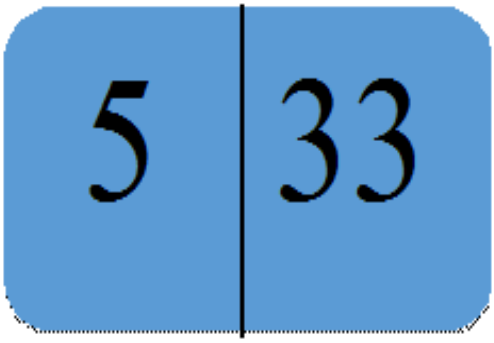

3
35

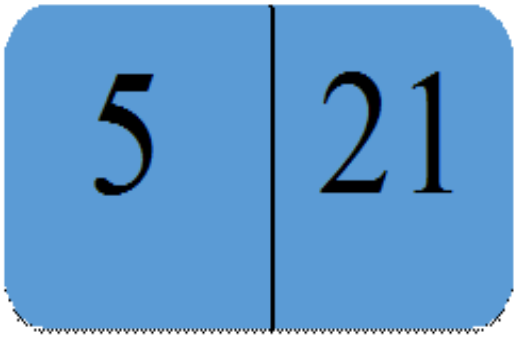

3
15

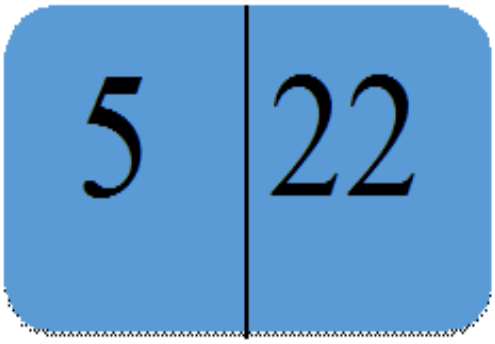

3
10

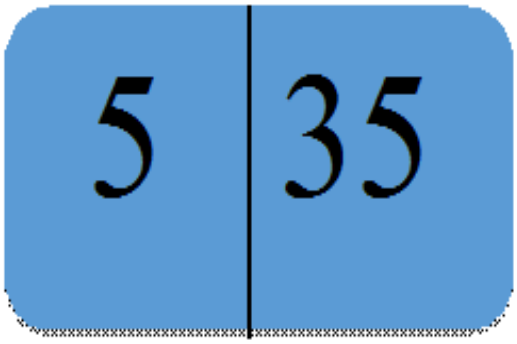

5
6

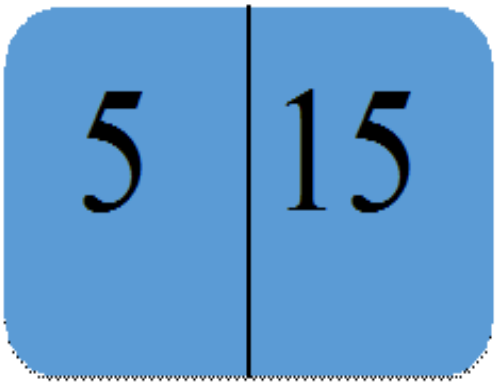

5
14

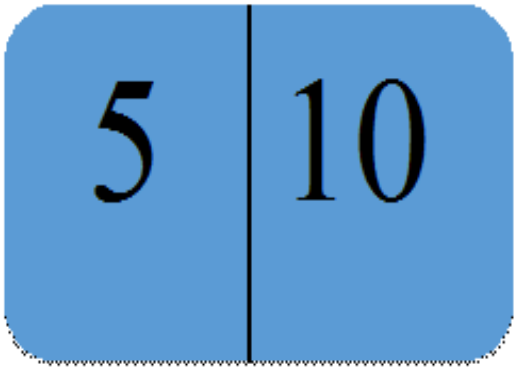

5
33

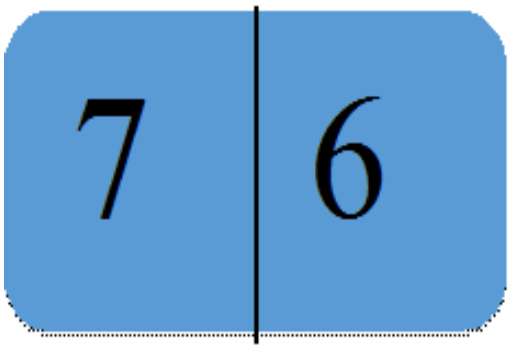

5
21

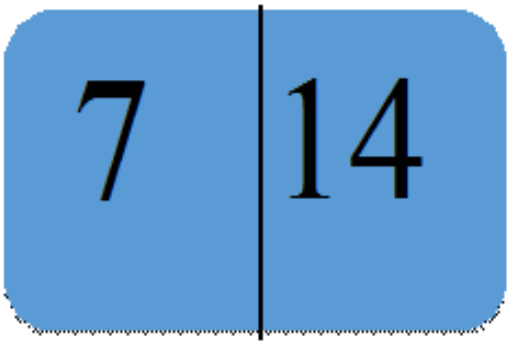

5
22

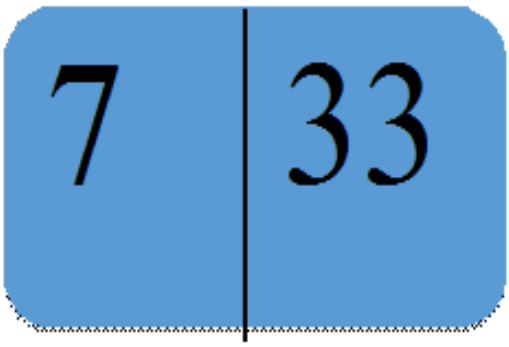

5
35

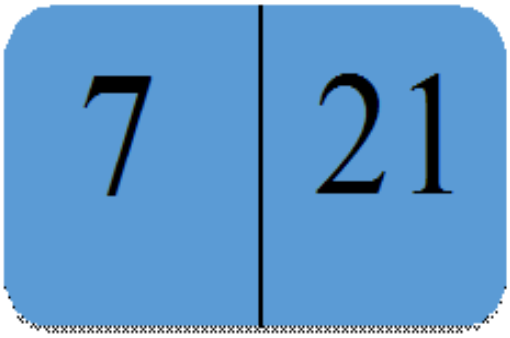

5
15

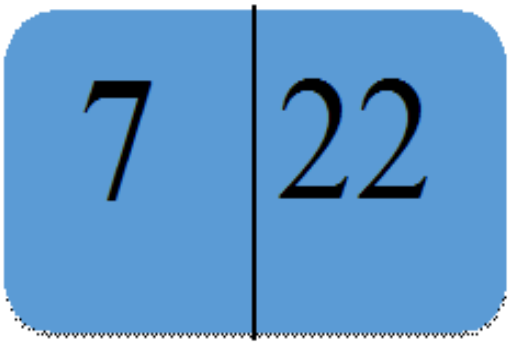

5
10

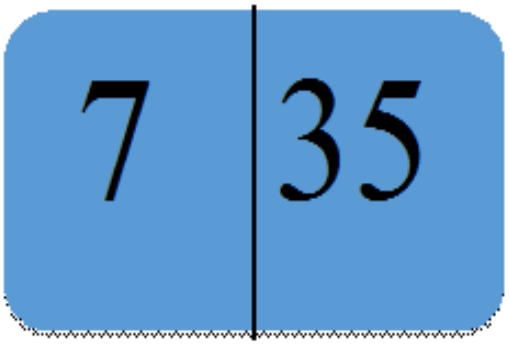

7
6

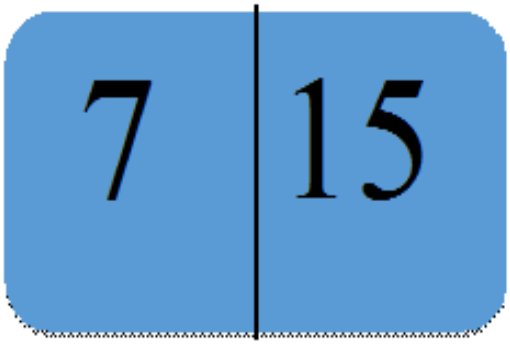

7
14

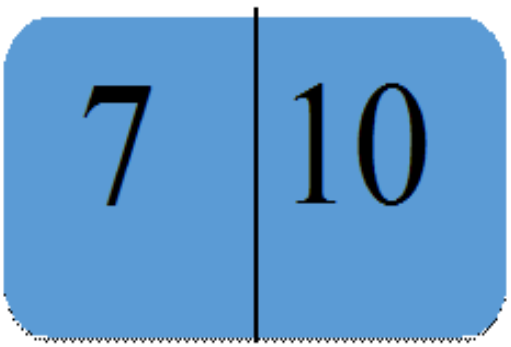

7
33

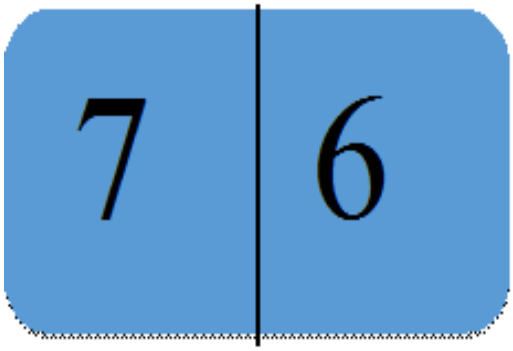

7
21

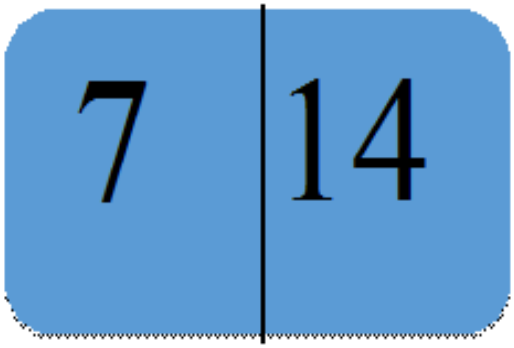

7
22

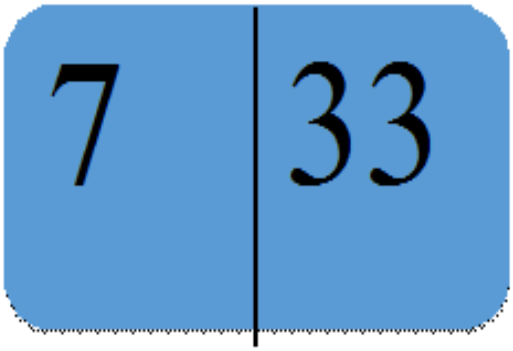

7
35

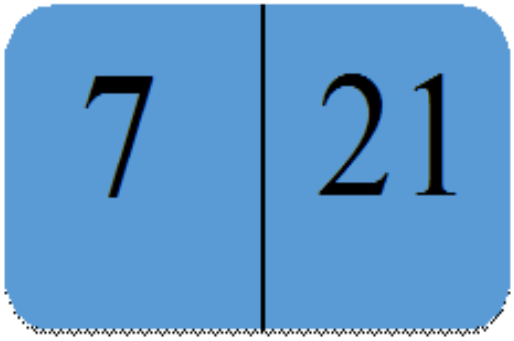

7
15

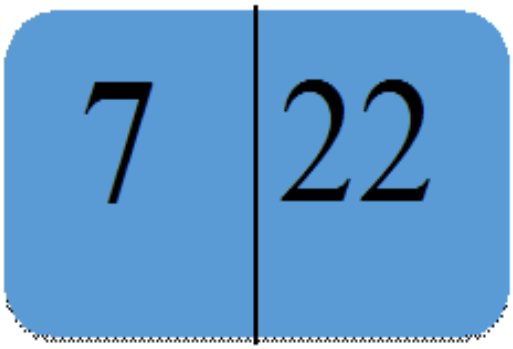

7
10

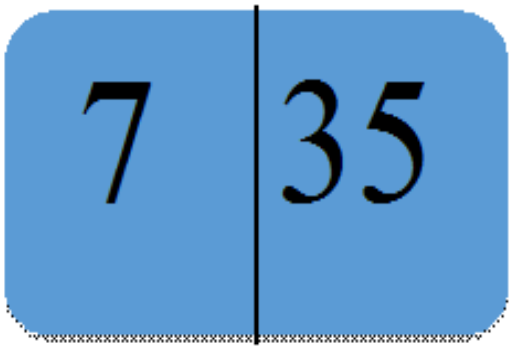

7
6

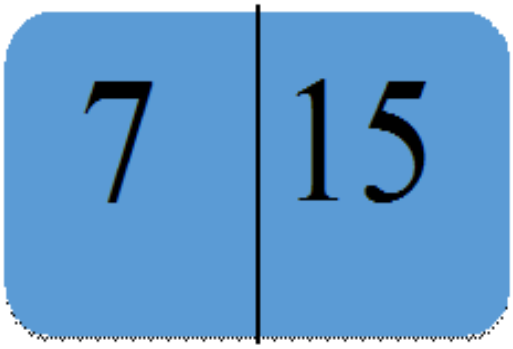

7
14

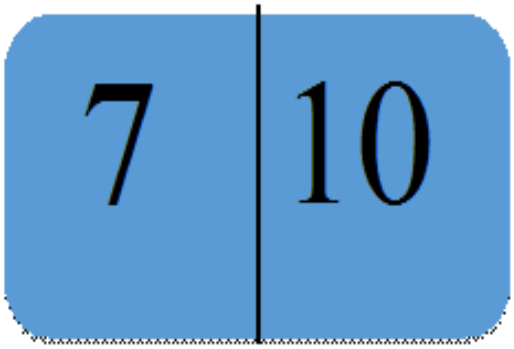

7
33

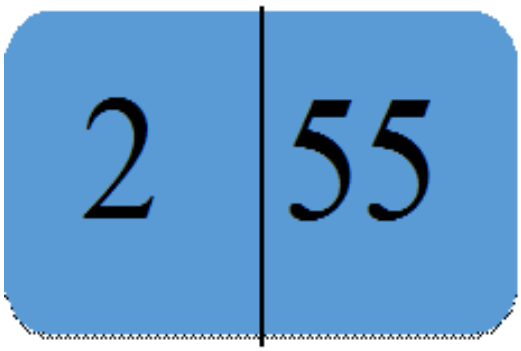

7
21

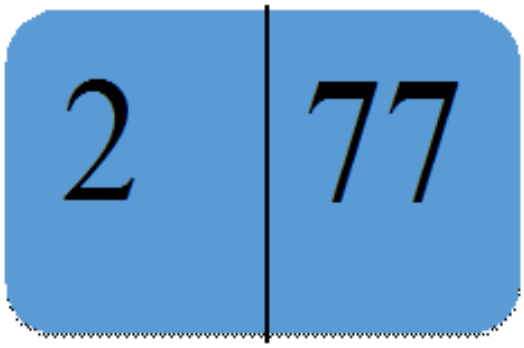

7
22

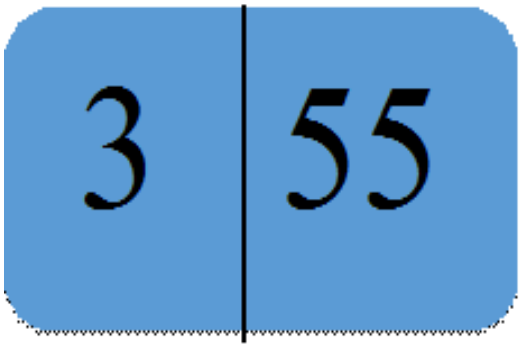

7
35

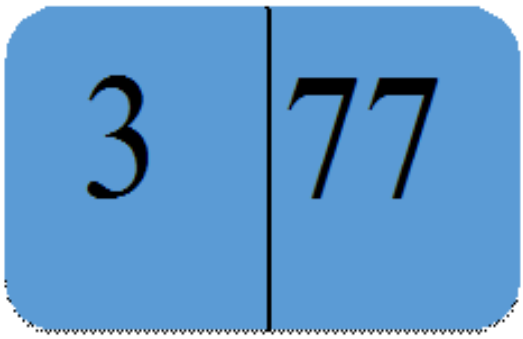

7
15

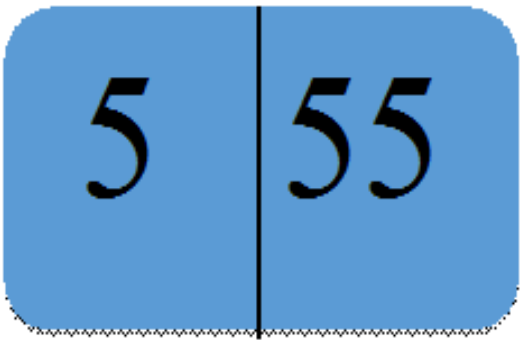

7
10

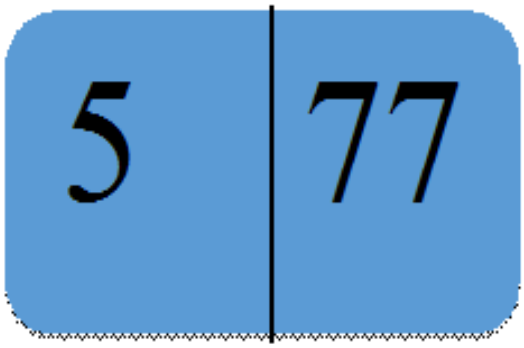

2
55

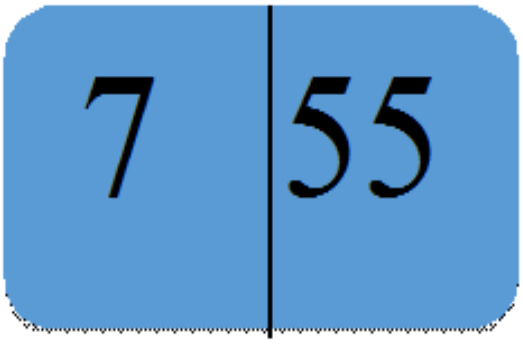

2
77

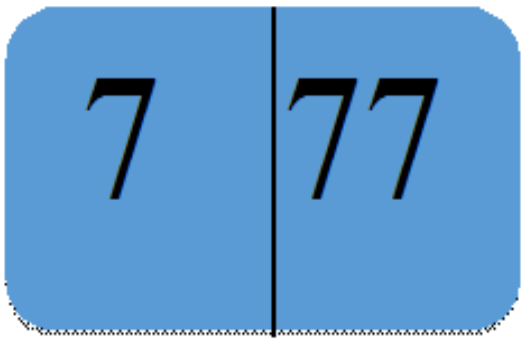

3
55


3
77


5
55


5
77


7
55


7
77

4.3.11. Descubra a senha e resolva o enigma.

A criptografia já era usada há muito tempo no Egito antigo, principalmente, para assuntos ligados a guerra, onde se precisava passar uma mensagem que, caso caísse nas mãos inimigas, estes não tivessem como descobrir o seu significado. Em um passado mais recente, a criptografia, foi amplamente utilizada na segunda guerra mundial, onde, através da Máquina Enigma, os comandantes nazistas passavam mensagem para os seus comandados, que se caso essa mensagem caísse na mão dos aliados, estes não teriam como saber o seu real significado, fazendo com que suas estratégias não fossem descobertas e, como consequência, provocando muitas baixas no exército que lutava contra o nazismo. O matemático inglês Alan Mathison Turing foi o responsável por criar uma Máquina, chamada de O Colossus, capaz de descobrir a criptografia usada pela Máquina Enigma, permitindo assim que milhares, ou talvez milhões, de vidas fossem salvas. Sem essa Máquina criada por Turing é possível que a guerra tivesse sido vencida pelos nazistas, onde, provavelmente, o mundo com o qual estamos tão acostumados seria totalmente diferente. A Máquina criada por Turing é precursora dos computadores atuais, por esse fato Turing é conhecido como o "Pai dos Computadores". Caso tenha interesse em obter maiores informações sobre como funcionava a Enigma, segue o link do vídeo sobre a Demonstração da Máquina Enigma – Museu da UFRGS. https://www.youtube.com/watch?v=VMJeDLv2suw

Imagine que você encontre a mensagem descrita abaixo e precise decifrá-la, tendo apenas uma oportunidade para este fato, sendo lhe fornecido apenas uma pista.

Observações:

- É necessário ter o domínio do Pequeno Teorema de Fermat para essa atividade;
- Para aplicação dessa atividade foram necessárias quatro aulas, sendo que duas foram utilizadas para explicar as noções básicas do Pequeno Teorema de Fermat;
- Cada espaço em branco na tabela corresponde o espaço entre as palavras;
- A segunda linha da tabela corresponde às letras da mensagem criptografada e a primeira linha corresponde as letras na mensagem original.

Exemplo: Decifre a seguinte mensagem:

MAXOUH JVHBXHDGQ ABHXJMAXN

Onde a dica é a seguinte:

Dica: O número que corresponde à chave correta é o resto da divisão de 5^{88} por 89.

CHAVE 1

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
	.	O	Q	X	L	R	T	U	S	P	J	E	V	M	Z	A	H	D	G	I	F	C	B	N

CHAVE 2

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
O	.	X	S	L	C	R	T	U	Q	Z	J	E	V	M	N	H	A	F	G	I	D		B	P

CHAVE 3

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
Z	V	R	N	G	U	A	Q	P	L		E	B	T	D	S	F	H	M	J	I	.	X	C	O

CHAVE 4

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
T	E	O	Q	.	M	R	A	U	H	P	J	G	V	L	C	D	I	X		B	F	S	N	Z

Solução: Pelo Pequeno Teorema de Fermat temos que 5^{88} quando dividido por 89 deixa resto 1. Assim a chave correta será a chave 1. Como a primeira linha da chave corresponde as letras da mensagem original e a segunda linha corresponde as letras da mensagem criptografada, temos que:

M = P, A = R, X = E; trocando todas as letras, obtemos que a mensagem original é:

PRECISAMOS ESTUDAR SEMPRE.

2: Decifre a seguinte mensagem:

APNOT ZUXI RAPNT.UOBAPNCB UAPF

Dica: O número que corresponde à chave correta é o resto da divisão de 3^{103} por 103.

CHAVE 1

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
	.	O	Q	X	L	R	T	U	S	P	J	E	V	M	Z	A	H	D	G	I	F	C	B	N

CHAVE 2

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
O	.	X	S	L	C	R	T	U	Q	Z	J	E	V	M	N	H	A	F	G	I	D		B	P

CHAVE 3

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
X	H	R	J	O	M	Z	Q		V	G	U	T	A	C	E	B	P	I	.	S	L	D	N	F

CHAVE 4

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
T	E	O	Q	.	M	R	A	U	H	P	J	G	V	L	C	D	I	X		B	F	S	N	Z

3: Decifre a seguinte mensagem:

SUO PQLISUOZAQSUOU.OA CA AXSUE

Dica: O número que corresponde à chave correta é o resto da divisão de 2^{138} por 47.

CHAVE 1

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
.	F	G	H	L	C	J	N	A	R	T	Q		S	Z	D	I	U	X	P	V	M	B	O	E

CHAVE 2

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
X	H	R	J	O	M	Z	Q		V	G	U	T	A	C	E	B	P	I	.	S	L	D	N	F

CHAVE 3

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
T	E	O	Q	.	M	R	A	U	H	P	J	G	V	L	C	D	I	X		B	F	S	N	Z

CHAVE 4

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z		.
	.	O	Q	X	L	R	T	U	S	P	J	E	V	M	Z	A	H	D	G	I	F	C	B	N

CONSIDERAÇÕES

O estudo dos números primos, conhecendo sua conceituação e seus principais aspectos históricos só tende a dar maior ênfase a sua importância na construção do conhecimento matemático, mostrando não só as suas aplicações no restante da vida escolar do corpo discente, mas também sua importância no desenvolvimento da sociedade atual, tirando aquela falsa impressão de pouca importância deixada tanto pelos livros didáticos como também pelos PCNs de matemática.

Ficou esclarecido que comumente os livros didáticos não costumam fazer uma abordagem dos números primos aliado a seus principais aspectos históricos, além do que, não oferecem uma quantidade suficiente de exercícios e, os que são oferecidos não são, pelo menos a maior parte deles, tão desafiadores, deixando a impressão de não ter tanta importância para o bom desenvolvimento do restante da vida escolar dos discentes. Essa forma de abordagem, muito possivelmente está atrelada a laços históricos. Mas também há de se ressaltar que os próprios PCNs de Matemática não estabelece uma maneira sistematizada de como este conteúdo deverá ser trabalhado, deixando esta responsabilidade não mão do currículo a ser adotado por cada unidade de ensino, o que gera outro problema, pois, quase sempre o currículo a ser adotado é baseado no livro didático. Daí nota-se que é necessário um complemento, pois grande parte dos alunos chegam ao Ensino Médio sem o conhecimento das noções básicas dos números primos fazendo com que não tenham um bom desenvolvimento nessa importante área de estudo.

O resultado do questionário aplicado só corrobora a necessidade de uma abordagem mais completa e atrativa. Contudo, os livros didáticos que são usados comumente no Ensino Fundamental, não oferecem uma abordagem priorizando a ênfase tanto a sua conceituação como também a seus principais aspectos históricos.

Entretanto, há de se ressaltar, a escassez de material acessível destinado ao Ensino Fundamental, principalmente quando se trata de jogos e atividades interessantes, onde, como dito anteriormente, não foi encontrado em nenhum dos livros didáticos analisados. Embora os jogos envolvendo números primos também não sejam tão fáceis de encontrar em outras fontes, dificultando ainda mais a inserção do estudo dos números primos de maneira mais atrativa e desafiadora.

Os jogos e atividades encontrados no trabalho foram todos aplicados em sala de aula e o resultado foi bem interessante, pois os alunos envolvidos nas atividades mostraram estar entusiasmados em tentar resolver as atividades propostas e, como consequência, fazendo com que eles tenham um melhor conhecimento das noções básicas do referido conteúdo resultando em uma melhora considerável no que diz respeito a aprender matemática.

Independentemente da estratégia que irá ser utilizada na inserção do estudo dos números primos na educação básica, há de ressaltar a importância do professor, pois o professor é a principal peça no processo de ensino-aprendizagem, estimulando o aluno a pensar e questionar, fazendo assim que eles tenham suas próprias opiniões e, consequentemente, melhorando o seu aprendizado.

REFERÊNCIAS

AABOE, Asger. **Episódios da história antiga da matemática.** Aaboe Asger; tradução: João Bosco Pitombeira. Rio de Janeiro: SBM, 2013.

BONJORNO, José Roberto. BONJORNO, Regina Azenha. OLIVARES, Ayrton. **Matemática: fazendo a diferença.** 5ª série. 1. Ed. São Paulo: FTD, 2006.

BRASIL. Ministério da Educação. Secretaria de Educação Fundamental. **PCN Ensino Fundamental**: Matemática. Brasília: MEC, SEF, 1998. Disponível em: <http//http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf >. Acesso: 27 dez. 2014

CAMPOS, Edílson da Silva. NUNES, Crisângela Avila. **Crisson, uma atividade para sala de aula**. RPM nº 76. Ano 29. Rio de Janeiro, 2011.

CAVALCANTE, Luiz G.. SOSSO, Juliana. VIEIRA, Fábio. POLI, Ednéia.**Para saber Matemática.** 5ª série. 2. Ed. São Paulo: Saraiva, 2006.

CENTURIÓN, Marília. JAKUBOVIC, José. **Matemática teoria e contexto.** 6º ano**.** 1. Ed. São Paulo: Saraiva, 2012.

DANTE, Luiz Roberto. **Projeto Teláris: matemática.** 6º ano**.** 1. Ed. São Paulo: Ática, 2012.

DEWDNEY, A. K. **20.000 Léguas Matemáticas: Um passeio pelo misterioso mundo dos números.** A. K. Dewdney; tradução: Vera Ribeiro; revisão: Vitor Tinoco. Rio de Janeiro: Zahar, 2000.

EVES, Howard. **Introdução à história da matemática**. Howard Eves; tradução: Hygino H. Domingues. Campinas – SP: Editora da Unicamp, 2004.

HEFEZ, Abramo. **Elementos de aritmética.** 2. Ed. Rio de Janeiro: SBM, 2011.

IEZZI, Gelson. DOLCE, Osvaldo. ANTONIO, Machado. **Matemática e realidade.** 5ª série. 5. ed. São Paulo: Atual, 2005.

IFRAH, Georges. **Os números: História de uma grande invenção**. Georges Ifrah; tradução: Stella Maria de Freitas Senra. 11. ed. São Paulo: Globo, 2005.

LANDAU, Edmund Georg Hermann (1877 – 1938). **Teoria Elementar dos Números.** Edmund Georg Hermann Landau; tradução: Paulo Henrique Viana de Barros; revisão: Lázaro Coutinho. Rio de Janeiro: Ciência Moderna, 2002.

MAZZIEIRO, Alceu dos Santos. **Descobrindo e aplicando a Matemática.** 6º ano**.** 1. Ed. Belo Horizonte: Dimensão, 2012.

MOREIRA, Carlos Gustavo Tamm de Araújo. MARTÍNEZ, Fabio Enrique Brochero. SALDANHA, Nicolao Corção. **Tópicos de Teoria dos Números.** Rio de Janeiro: SBM, 2012.

RIBENBOIM, Paulo. **Números primos, amigos que causam problemas.** Paulo Ribenboim, - Rio de Janeiro: SBM, 2015.

ROQUE, Tatiana. **História da matemática: uma visão crítica desfazendo mitos e lendas**. Rio Janeiro: Zahar, 2012.

SAUTOY, Marcus du. **A música dos números primos: a história de um problema não resolvido na matemática.** Marcus du Sautoy; tradução: Diego Alfaro. Rio de Janeiro: Jorge Zahar, 2007.

_____. **Os mistérios dos números: os grandes enigmas da matemática (que até hoje ninguém foi capaz de resolver).** Marcus du Sautoy; tradução: George Schlesinger. Rio de Janeiro: Jorge Zahar, 2013.

SHOKRANIAN, Salahoddin. **Uma Breve História da Teoria dos Números no Século Vinte.** Rio de Janeiro: Ciência Moderna, 2010.

_____. **Uma Introdução à Teoria dos Números.** Rio de Janeiro: Ciência Moderna, 2008.

STEWART, Ian. **Mania de matemática: diversão e jogos de lógica e matemática.** Ian Stewart; tradução: Maria Luiza X. de A Borges. Rio de Janeiro: Jorge Zahar, 2005.

_____. **Os maiores problemas matemáticos de todos os tempos**. Ian Stewart; tradução: George Schlesinger. 1. Ed. Rio de Janeiro: Jorge Zahar, 2014.

ANEXOS

Como sugestões para leitura de livros, apresentam-se os seguintes:

"Os mistérios dos números" e "A música dos números primos" de Marcus Du Sautoy. No primeiro é feita uma abordagem interessante e de fácil leitura sobre enigmas matemáticos que ainda não foram resolvidos. Já o segundo fala da história dos números primos, passando por todos que ofereceram contribuições importantes até os dias de hoje. Apesar deste último ser um livro que aborda um tema específico, é bem interessante a sua leitura. Em "os maiores problemas matemáticos de todos os tempos", de Ian Stewart, o autor aborda os grandes problemas matemáticos de forma sutil e interessante. Em "20.000 Léguas Matemáticas", de A. K. Dewdney, o autor nos leva a uma viagem interessante pelo mundo misterioso dos números. Livro de fácil leitura com linguagem simples e bem interessante.

Os livros citados acima são escritos de uma forma que para gostar de sua leitura não necessariamente precisa gostar de matemática.

Com relação à história da matemática, podemos citar os seguintes: "Episódios da história antiga da matemática", cujo autor é Asger Aaboe, "Uma breve história da teoria dos números no século vinte", cujo autor é Salahoddin Shokranian e "História da matemática uma visão crítica, desfazendo mitos e lendas", escrito por Tatiana Roque.

Dentre os filmes, podemos citar o *jogo da imitação*, que trata da história de um matemático, Alan Turing, que decifrou o código de guerra alemão, o "Enigma". Alan Turing inventou a máquina que precedeu os computadores modernos, no entanto, além do fato citado acima, do qual trata o filme, Turing tinha uma outra esperança: inventar uma máquina capaz de derrubar o oitavo problema da lista dos 23 de Hilbert: a Hipótese de Riemann. Outro filme que podemos citar é *Uma mente brilhante*, filme este que relata a vida de do grande matemático John Forbes Nash, que relata seus avanços na matemática e sua luta contra a esquizofrenia. Nash ganhou o prêmio Nobel da economia em 1994 e também foi outro grande matemático a tentar decifrar sem muito sucesso a Hipótese de Riemann. Em *Contato*, filme adaptado do romance contato escrito por Carl Sagam, uma cientista capta um sinal e percebe que se trata de uma série de pulsos que, depois de convertê-los, observa que são todos números primos.

Independentemente de qual estratégia nós, professores, iremos usar, o que precisamos mesmo é mostrar para os nossos alunos o quão importante são os *números primos*, não só pela sequência dos conteúdos na qual torna necessário o domínio de suas propriedades básicas, mas também porque eles são de suma importância para nossas vidas.

Tabela contendo todos os números primos Até o número 2000.

2	101	211	307	401	503	601	701	809	907
3	103	223	311	409	509	607	709	811	911
5	107	227	313	419	521	613	719	821	919
7	109	229	317	421	523	617	727	823	929
11	113	233	331	431	541	619	733	827	937
13	127	239	337	433	547	631	739	829	941
17	131	241	347	439	557	641	743	839	947
19	137	251	349	443	563	643	751	853	953
23	139	257	353	449	569	647	757	857	967
29	149	263	359	457	571	653	761	859	961
31	151	269	367	461	577	659	769	863	977
37	157	271	373	463	587	661	773	877	983
41	163	277	379	467	593	673	787	881	991
43	167	281	383	479	599	677	797	883	997
47	173	283	389	487		683		887	
53	179	293	397	491		691			
59	181			499					
61	191								
67	193								
71	197								
73	199								
79									
83									
89									
97									

1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
1069	1193	1283		1481	1597	1669	1789	1889	1997
1087		1289		1483		1693			1999
1091		1291		1487		1697			
1093		1297		1489		1699			
1097				1493					
				1499					