UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

MÁRCIO DOMINICALI RIGOTI

NÚMEROS PRIMOS: OS ÁTOMOS DOS NÚMEROS.

DISSERTAÇÃO

CURITIBA

2015

MÁRCIO DOMINICALI RIGOTI

NÚMEROS PRIMOS: OS ÁTOMOS DOS NÚMEROS.

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de “Mestre”.

Orientador: João Luis Gonçalves, Dr.

CURITIBA

2015

Dados Internacionais de Catalogação na Publicação

R572n 2015

Rigoti, Márcio Dominicali
Números primos : os átomos dos números / Márcio Dominicali Rigoti.-- 2015.
48 f.: il.; 30 cm

Texto em português, com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional, Curitiba, 2014.
Bibliografia: f. 48.

1. Números primos. 2. Teoria dos números. 3. Demonstração automática de teoremas. 4. Números naturais. 5. Matemática (Ensino fundamental) - Estudo e ensino. 6. Prática de ensino. 7. Matemática - Dissertações. I. Gonçalves, João Luis, orient. II. Universidade Tecnológica Federal do Paraná - Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD 22 -- 510

Biblioteca Central da UTFPR, Câmpus Curitiba

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba

Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Título da Dissertação No. 023

"Números Primos: Os Átomos dos Números"

por

Márcio Dominicali Rigoti

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de Mestre em Matemática, pelo Programa de Mestrado em Matemática em Rede Nacional - PROFMAT - da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba, às 14h30 do dia 12 de dezembro de 2014. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

_____
Prof. João Luis Gonçalves, Dr.
(Presidente - UTFPR/Curitiba)

_____
Prof. Rodrigo Silva Lima, Dr.
(UNIFEI)

_____
Profa. Denise de Siqueira, Dra.
(UTFPR/Curitiba)

Visto da coordenação:

_____
Prof. Ronie Peterson Dario, Dr.
(Coordenador do PROFMAT/UTFPR)

"A Folha de Aprovação assinada encontra-se na Coordenação do PROFMAT/UTFPR"

À minha esposa Caroline Berger Rigoti, sem seu apoio e incentivo este trabalho não seria possível.

AGRADECIMENTOS

- A todos meus familiares em especial meus pais e irmãos que sempre me incentivaram.
- Ao meu grande amigo Marlon Mühlbauer pelo companheirismo nas horas de viagens e estudos.
- A todos os professores do PROFMAT por terem compartilhado seus conhecimentos.
- Ao meu orientador Dr. João Luis Gonçalves, por ter aceitado me orientar e pela sua dedicação.
- Ao Sindicato dos Trabalhadores Municipais de São Bento do Sul, pelo apoio prestado.
- À Prefeitura Municipal de São Bento do Sul, em especial a secretária de educação Alcione Teresinha Hinke, pelo incentivo à melhoria na educação.
- À Márcia Regina Innocente diretora da Escola Básica Municipal Rodolfo Berti, que colaborou na implementação deste trabalho em sala de aula.
- À Sociedade Brasileira de Matemática que na busca da melhoria do ensino de Matemática na Educação Básica viabilizou a implementação do PROFMAT.
- À CAPES pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior e pelo incentivo financeiro.

RESUMO

RIGOTI, Márcio Dominicali. NÚMEROS PRIMOS: OS ÁTOMOS DOS NÚMEROS.. 48 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Este trabalho apresenta um estudo sobre os Números Primos que passa por resultados básicos, como a infinitude dos números primos e o Teorema Fundamental da Aritmética, e resultados mais sofisticados, como o Teorema de Wilson e a consequente função geradora de primos. Além dos resultados teóricos apresenta-se uma interpretação geométrica para os números primos. Essa interpretação é aplicada na ilustração de alguns dos resultados relacionados a primos abordados no ensino básico. Atividades envolvendo a interpretação geométrica apresentada são sugeridas no capítulo final.

Palavras-chave: Números primos, Função geradora de primos, Interpretação geométrica dos primos

ABSTRACT

RIGOTI, Márcio Dominicali. PRIME NUMBERS: NUMBER'S ATOMS. 48 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

This work presents a study about Prime Numbers, since basic results, like the prime number's infinity and the Arithmetic Fundamental Theorem, to more sophisticated results, as Wilson's Theorem and it's consequent Prime generating function. Further the theoretical results we present a prime's geometric interpretation. This interpretation is applied to illustrate some results related to primes, which appears in basic education. Activities about this geometric interpretation are suggested in the final chapter.

Keywords: Prime numbers, Prime generating function, Prime number's geometric interpretation.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Durante o estudo de matemática nos deparamos com o fascinante conceito de número primo, conceito este que atualmente é ensinado no 6º ano do ensino fundamental juntamente com os conteúdos relacionados a múltiplos e divisores de um número natural.

Em livros didáticos como (IEZZI, 1991) e (RIBEIRO, 2009) encontram-se poucas referências históricas do estudo de números primos. Apenas algumas referências a métodos para produção de listas de primos, como o Crivo de Erátostenes. As abordagens muitas vezes ficam restritas a métodos para cálculo de Máximo Divisor Comum e de Mínimo Múltiplo Comum, não dando a devida importância que esse assunto tem na Teoria dos Números.

Resultados importantes como o da infinitude dos números primos e o Teorema Fundamental da Aritmética são apresentados como propriedades e não como teoremas. Esta forma de abordagem superficial contribui para que os alunos concluam a educação básica sem reconhecer a força e a beleza da matemática, e o seu papel de fornecer modelos abstratos para situações concretas.

Apresentar as teorias de uma maneira completamente axiomática, não convém à educação básica, mas apresentar definições e propriedades importantes de forma correta, e quando possível provar e demonstrar as afirmações, fará com que os estudantes reconheçam a importância do método matemático para as demais ciências. Segundo (LIMA, 2006)

> "Provar o óbvio transmite a falsa impressão de que a matemática é inútil. Por outro lado, usar argumentos elegantes para demonstrar resultados inesperados é uma maneira de exibir sua força e beleza. As demonstrações, quando bem apresentadas, contribuem para desenvolver o raciocínio, o espirito crítico, a maturidade e ajudam a entender o encadeamento lógico das proposições matemáticas."

Um dos objetivos deste trabalho é apresentar definições e resultados importantes relacionados a números primos bem como suas demonstrações, com a finalidade de colaborar para a prática docente de profissionais da educação básica. Visto que muitos destes resultados e demonstrações são desconhecidos por alunos e por profissionais da educação.

Num segundo momento será abordada a construção de uma função capaz de gerar números primos. Esta função geradora de primos é pouco conhecida, foi proposta por Ross Honsberger (HONSBERGER, 1976) e é capaz de gerar todos os números primos. Além disso, esta função é sobrejetora sobre o conjunto dos primos, ou seja, gera apenas números primos.

No capítulo seguinte será proposto uma forma geométrica de interpretação dos números naturais que permite uma visualização simples de várias propriedades e demonstrações referentes a números primos, como a da infinitude dos números primos, o Teorema Fundamental da Aritmética e o Crivo de Eratóstenes. O objetivo destas ilustrações é oferecer uma alternativa para facilitar a compreensão destes assuntos para alunos da educação básica.

No último capítulo será apresentado sugestões de atividades envolvendo a interpretação geométrica de números naturais e demais assuntos estudados neste trabalho e aplicáveis em diferentes níveis da educação básica.

2 NÚMEROS PRIMOS

No dia a dia o ser humano lida com números a todo momento. Os números transmitem diversas informações: a idade, a hora de acordar, o quanto pode-se comprar com o respectivo salário, o endereço de uma residência. Estes números estão associados a diferentes idéias como tamanho, peso, valor, tempo e posição.

Ao procurar a definição de número no dicionário (FERREIRA, 1988), encontra-se:

> "s.m. Relação entre qualquer quantidade e outra tomada como termo de comparação e que se chama unidade. Reunião de várias unidades, ou frações de unidade. Algarismo ou algarismos que indicam o lugar que uma coisa ocupa numa série. Coleção de coisas; quantidade. Exemplar de uma obra periódica (jornal, revista etc.). Cada uma das cenas dos espetáculos de circo, de teatro de variedades. Gramática Propriedade que têm as palavras de representar, por meio de certas formas ou flexões, a ideia de unidade ou pluralidade: algumas línguas têm, além do singular e do plural, o número dual. Matemática Número abstrato, número considerado em si mesmo, feita abstração da espécie de unidade que representa. Número algébrico, número marcado por um sinal (+ ou -). Número aritmético, número que serve para medir uma grandeza, independente de sua orientação. Número concreto, número que convém a uma coleção de objetos que se podem contar. Número decimal, número composto com a ajuda de submúltiplos decimais da unidade, com a parte decimal separada da parte inteira por uma vírgula. Número incomensurável ou irracional, número que não tem medida comum com a unidade. Número ordinal, número inteiro que indica o lugar ocupado pelos objetos de um conjunto, quando estão dispostos em determinada ordem. Número primo, número inteiro que só é divisível por si mesmo e pela unidade, como 3, 5, 7, 11 etc. Números primos entre si, números que só têm como divisores comuns a unidade: 18 e 35 são números primos entre si.

Verifica-se dentre vários significados que o primeiro refere-se a uma comparação entre duas grandezas, uma delas utilizada como unidade. Esta comparação é a ideia de contagem. Utilizando a comparação o ser humano, no decorrer de sua evolução, reconheceu padrões existentes em seu cotidiano e criou símbolos sonoros e escritos para expressar esses padrões. Por exemplo, pescar um peixe era diferente de pescar dois, que por sua vez era diferente de pescar vários. Assim percebe-se que a criação do conceito de número está associada com a necessidade do ser humano contar e registrar quantidades, e se desenvolveu antes da escrita sendo impossível datar exatamente quando e onde aconteceu. Existem artefatos arqueológicos tais como o Osso Lebombo, Figura 1, que mostram a necessidade da contagem e registro de quantidades.

Figura 1: Osso Lebombo, artefato matemático datado de 35 mil anos A.C..
Fonte: http://cnncba.blogspot.com.br/ , acessado em 28/05/2014.

Para contar e representar grandes quantidades foram criados sofisticados sistemas de numeração, alguns são estudados no ensino fundamental como os sistemas de numeração Romano e Egípcio, apresentado na Figura 2.

Figura 2: Símbolos do sistema de numeração egípcio.
Fonte: http://revistaescola.abril.com.br/, acesso em 28/05/2014

Com a evolução do comércio e da ciência surgiram novas necessidades, além da contagem, e novos números foram criados. Um aluno que concluiu a educação básica no Brasil teve contato com diferentes tipos de números organizados em conjuntos, o conjunto dos números naturais , dos inteiros, dos irracionais , dos reais e dos complexos.

Neste trabalho será utilizado principalmente o conjunto dos números naturais para as definições e demonstrações, e o representaremos por $\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$.

Dentro de $\mathbb{N}$ existem números com diferentes propriedades relativas a quantidade de

divisores, para verificá-las precisa-se compreender o conceito de divisibilidade a seguir.

Definição 2.1 (Divisibilidade)**.** *Dados dois números naturais a e b, com* $a \neq 0$ *diz-se que:*

O número a divide o número b se, e somente se, existir $k \in \mathbb{N}$ *de modo que* $b = k \cdot a$*, dizemos que a é divisor ou fator de b, e que, b é múltiplo de a.*

***Notação**:* $a \mid b \iff \exists \quad k \in \mathbb{N}$ *tal que* $b = k \cdot a$.

O número a não divide o número b se, e somente se, não existe $k \in \mathbb{N}$ *de modo que* $b = k \cdot a$.

***Notação**:* $a \nmid b \iff \nexists \quad k \in \mathbb{N}$ *tal que* $b = k \cdot a$.

Desta forma os números naturais maiores que 1 podem ser separados em dois grupos, números primos e números compostos (não primos), definidos a seguir:

Definição 2.2. *Número Primo é todo número natural maior que* 1 *e divisível apenas por* 1 *e ele mesmo.*

Exemplo 2.3. *O número* 7 *é primo pois é divisível apenas por* 1 *e* 7.

Definição 2.4. *Número composto é todo número natural maior que* 1 *que possui divisores naturais diferentes de* 1 *e ele mesmo, podendo ser escrito como o produto de dois naturais ambos diferentes de* 1.

Exemplo 2.5. *O número* 6 *é composto pois é divisível por* $1, 2, 3$ *e* 6.

Entre os significados da palavra número, vistos anteriormente em (FERREIRA, 1988), aparece a seguinte definição de número primo:

> "Número primo, número inteiro que só é divisível por si mesmo e pela unidade, como 3, 5, 7, 11 etc."

Segundo a mesma, o número 1 seria número primo, pois é divisível por ele mesmo e pela unidade, o que está errado. Além disso, os números primos devem ser números naturais e não inteiros. Deve-se considerar que um dicionário, não é um livro que expressa o rigor matemático, mas em sala de aula a definição deve ser rigorosa.

Os números primos são conhecidos pelos gregos desde a Escola Pitagórica. Para os gregos o número 1 era supremo, pois a partir da unidade pode-se formar qualquer outra quantidade (natural), com a operação de adição. Mas logo percebeu-se que também era possível

formar outras quantidades utilizando a operação de multiplicação com números diferentes de 1. Mas alguns números não podiam ser obtidos através da multiplicação.

Considerando então a propriedade de um número natural poder ou não ser escrito como uma multiplicação de números diferentes de 1, os números ficam classificados em três grupos, a unidade, os incompostos e os compostos . Sendo os incompostos os que não podem ser representados por uma multiplicação de dois fatores maiores que a unidade e os compostos os que podem. Segundo (BOYER, 1996) foi Fibonacci que primeiro utilizou a nomenclatura números primos no lugar de incompostos.

Euclides em sua obra *Os Elementos*, traduzida e reeditada em (BICUDO, 2009), foi o primeiro a demonstrar que os números primos são infinitos. Em sua demonstração Euclides utiliza um conceito de que um número composto pode ser escrito de maneira única, exceto pela ordem, como o produto de fatores primos. Esse conceito é tão importante que, posteriormente, foi chamado de *Teorema Fundamental da Aritmética*.

A demonstração da infinitude dos números primos foi feita por Euclides, na proposição 20 do livro 9 da obra *Os Elementos*. Essa foi a primeira demonstração por redução ao absurdo de que se tem conhecimento, e é considerada por muitos matemáticos como a mais bela da matemática.

> "*Os números primos são mais numerosos do que toda quantidade que tenha sido proposta de números primos.*
>
> *Sejam os números primos que tenham sido propostos A,B,C; digo que os números primos sejam mais numerosos que os A,B,C. Fique, pois, tomado o menor medido pelos A,B,C e seja o DE, fique acrescida a unidade DF ao DE. Então, o EF ou é primo ou não. Primeiramente, seja primo; portanto, os números primos A,B,C, EF achados são mais numerosos que os A,B,C.*
>
> *Mas, então, não seja primo o EF; portanto, é medido por algum número primo. Seja medido pelo primo G; digo que G não é o mesmo que algum dos A,B,C. Pois se possível, seja. Mas os A,B,C medem o DE; portanto, o G também medirá o DE. E também mede EF; e o G, sendo um número, medirá a unidade DF restante; oque é absurdo. Portanto, o G não é o mesmo que algum dos A,B,C. E foi suposto primo. Portanto, os números achados, A,B,C, G são mais numerosos do que a quantidade que tenha sido proposta dos A,B,C; oque era preciso provar.*
> *(Euclides, por volta de 400 A.C.).* "

Esta demonstração utiliza termos linguísticos pouco habituais atualmente. Segue uma adaptação desta demonstração com uma linguagem mais atual, apresentada em (BOYER, 1996).

Teorema 2.6. *Existem infinitos números primos.*

Demonstração. Suponha que exista somente um número finito r de primos, a saber $p_1, p_2, p_3, \ldots, p_r$. Considerando agora o número $N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r + 1$. Se N for primo, então tem-se uma

contradição, já que foi suposto existir somente r números primos e N evidentemente não é um deles. Se N não for primo, então existe um número primo p que divide N. Mas esse número primo p não pode ser nenhum dos números p_i $(i = 1,2,3, \ldots, r)$, pois se fosse, dividiria o produto $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$, e portanto dividiria o número 1, assim existe p primo com $p \neq p_i$ $(i = 1,2,3, \ldots, r)$. Em ambos os casos, conclui-se a existência de mais números primos do que a quantidade suposta inicialmente. Logo, a suposição de que existe um número finito de números primos é falsa. □

Note que um número da forma $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r + 1$, com p_i o i-ésimo primo, não é necessariamente primo. Por exemplo, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ não é primo, pois $30031 = 59 \cdot 509$.

Teorema 2.7 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único, exceto pela ordem dos fatores, como um produto de números primos.*

Demonstração. O teorema faz duas afirmações, que a decomposição de um número natural maior do que 1 em fatores primos existe, e que é única, exceto pela ordem. Precisa-se provar, a existência e a unicidade.

Existência: Seja n um número natural, tal que $n > 1$, se n for primo, ele é a sua própria decomposição, a qual, portanto existe. Suponhamos n composto. Tomemos $p_1 > 1$ o menor divisor natural de n. Temos que p_1 é primo, pois caso contrário, existiria p natural $(1 < p < < p_1)$, com $p \mid p_1$, e portanto $p \mid n$, contradizendo a escolha de p_1. Assim podemos escrever $n = p_1 \cdot n_1$.

Se n_1 for primo, novamente a prova estará completa. Se n_1 é composto, tomemos p_2 como o menor fator de n_1. Pelo mesmo argumento, temos que p_2 é primo e portanto $n = p_1 \cdot p_2 \cdot n_2$.

Se repetirmos esse procedimento obteremos uma sequência decrescente de números naturais $n_1, n_2, n_3, \ldots, n_r$ $(r \in \mathbb{N})$, todos maiores que 1. Pelo *Princípio da Boa Ordenação*, este processo não pode ser repetido indefinidamente. Neste momento teremos uma sequência $p_1, p_2, p_3, \ldots, p_k$, com $k \in \mathbb{N}$, de números primos não necessariamente distintos. Se tivermos l primos distintos, sem perda de generalidade, podemos renomeá-los como $p_1, p_2, p_3, \ldots, p_l$. Logo n terá a forma $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_l^{\alpha_l}$, que é a decomposição de n em fatores primos.

Unicidade: A unicidade é mostrada usando indução sobre n. Para $n = 2$, a afirmação é verdadeiramente trivial. Assumimos que ela se verifica para todos os naturais maiores do que 1 e

menores do que n. Vamos provar que ela também é válida para n.

Se n é primo, não há o que provar. Suponhamos n composto e que n possua duas decomposições:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_t \text{ com } s \text{ e } t \in \mathbb{N}.$$

Onde os p_i $(i = 1,2,\ldots,s)$ e os q_j $(j = 1,2,\ldots,t)$ são primos. Temos que provar que $s = t$ e que cada p_i é igual a algum q_j. Podemos escrever:

$$p_2 \cdot \ldots \cdot p_s = \frac{q_1 \cdot q_2 \cdot \ldots \cdot q_t}{p_1}.$$

Como $p_2 \cdot \ldots \cdot p_s$ é um número natural, então $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_t$, o que implica que p_1 divide algum dos fatores q_1 , q_2 , ... , q_t. Sem perder a generalidade, podemos supor que $p_1 \mid q_1$. Assim pela Definição 2.2, $p_1 = q_1$. Logo:

$$1 < p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_t < n.$$

Pela hipótese de indução as duas decomposições são idênticas, isto é, $s = t$ e, exceto pela ordem, as decomposições $p_2 \cdot \ldots \cdot p_s$ e $q_2 \cdot \ldots \cdot q_t$ são iguais. □

Este resultado, aparentemente simples, confere aos números primos o papel de blocos construtores dos números naturais, mediante o uso da multiplicação. Por esse motivo alguns os consideram os "átomos dos números". O Teorema 2.7 fornece uma excelente ferramenta para interpretar os números naturais, fazendo-se fundamental para entender-se novos conceitos, como o de Máximo Divisor Comum, Mínimo Múltiplo Comum e números primos entre si, entre outros.

Definição 2.8 (Máximo Divisor Comum)**.** *Dados dois números naturais $a \neq 0$ e $b \neq 0$, a cada número podemos associar um conjunto de divisores, D_a e D_b. O Máximo Divisor Comum de a e b, denotado por $mdc(a,b)$, será o maior elemento da intersecção $D_a \cap D_b$.*

Note que $D_a \cap D_b$ não é vazia, pois 1 pertence a ambos. E além disso, $D_a \cap D_b$ é finita, pois os maiores elementos de D_a e D_b são respectivamente a e b. Assim a definição de Máximo Divisor Comum está bem posta.

Exemplo 2.9. *Para determinar o Máximo Divisor Comum, entre* 48 *e* 30*, será utilizado o teorema 2.7, assim escreve-se:*

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$ *e* $30 = 2 \cdot 3 \cdot 5$*, o Máximo Divisor Comum é o produto dos fatores comuns, assim* $mdc(48,30) = 2 \cdot 3 = 6$.

Definição 2.10 (Mínimo Múltiplo Comum)**.** *Dados dois números naturais a e b maiores que* 1*, a cada um desses números pode-se associar um conjunto infinito de seus respectivos múltiplos,*

M_a e M_b. O Mínimo Múltiplo Comum entre a e b é o menor valor não nulo de $M_a \cap M_b$, e será denotado por $mmc(a,b)$.

Note que sempre existe o $mmc(a,b)$ pois $a \cdot b$ pertence a $M_a \cap M_b$.

Exemplo 2.11. *Sejam os números* 15 *e* 12*, tem-se que os respectivos conjuntos de múltiplos são* $M_{15} = \{0, 15, 30, 45, 60, 75, \ldots\}$ *e* $M_{12} = \{0, 12, 24, 36, 48, 60, 72, \ldots\}$.

A intersecção $M_{15} \cap M_{12} = \{0, 60, \ldots\}$*, então* $mmc(15,12) = 60$.

Note que o Teorema 2.7 facilita o cálculo e a compreensão do MMC e do MDC. Como no Exemplo 2.11, observando os fatores de a e b, fica fácil formar um número que contenha todos os fatores que aparecem nas decomposições de a e b. O produto de todos esses fatores é o $mmc(a,b)$.

Exemplo 2.12. *Para determinar o Mínimo Múltiplo Comum entre* 12,15 *e* 8*, escrevemos:*

$12 = 2 \cdot 2 \cdot 3$*,* $15 = 3 \cdot 5$ *e* $8 = 2 \cdot 2 \cdot 2$*, assim o Mínimo Múltiplo Comum deverá conter o mínimo possível para que todos esses fatores estejam inseridos, assim* $mmc(12,15,8) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 120$.

Os Exemplos 2.9 e 2.12 ilustram dois assuntos estudados no 6^o ano do ensino fundamental, na forma como os mesmos são apresentados aos alunos, porém com a sutil presença da utilização do Teorema 2.7. Atividades com essa abordagem não visam apenas fazer o aluno decorar mais um teorema, mas sim a reflexão do assunto e suas diferentes aplicações, estimulando o pensamento crítico e a construção de ideias com base em um raciocínio. O que concorda com um dos objetivos da escola que é formar cidadãos críticos e participativos, como afirma (FREIRE, 1980),

> *... o educador ou educadora crítica, exigente, coerente, no exercício de sua reflexão sobre a prática educativa ou no exercício da própria prática, sempre a entendem em sua totalidade. Não centra a prática educativa, por exemplo, nem no educando, nem no educador, nem no conteúdo, nem nos métodos, mas a compreende nas relações de seus vários componentes, no uso coerente por parte do educador ou da educadora dos materiais, dos métodos, das técnicas.*

2.1 RESULTADOS E DEFINIÇÕES IMPORTANTES SOBRE NÚMEROS PRIMOS

Muitos assuntos estudados durante a educação básica utilizam conceitos envolvendo números primos e divisibilidade. Como por exemplo o Algoritmo de Euclides.

Definição 2.13 (Algoritmo de Euclides)**.** *Dados dois números inteiros a e b, com* $a > 0$*, tem-se que existem inteiros q e r,* $0 \leq r < a$*, tais que* $b = q \cdot a + r$.

Exemplo 2.14. $33 = 14 \cdot 2 + 5$.

Este algoritmo pode ser estendido, se tornando um importante método de cálculo do máximo divisor comum, e também para determinar se dois números são primos entre si.

Definição 2.15 (Algoritmo de Euclides Estendido)**.** *Sejam a e b inteiros positivos e* $c = mdc(a,b)$*, existem m e* $n \in \mathbb{Z}$ *tais que:*

$$am + bn = c.$$

Exemplo 2.16. *Sejam* $a = 4$*,* $b = 6$ *e* $c = mdc(4,6) = 2$*, então existem m e n tais que:*

$$4 \cdot m + 6 \cdot n = 2.$$

De fato se $m = 2$ *e* $n = 1$ *tem-se que:*

$$4 \cdot 2 + 6 \cdot 1 = 2.$$

Definição 2.17 (Números primos entre si)**.** *Dados dois números* $a \neq 0$ *e* $b \neq 0$*, estes serão chamados primos entre si quando o máximo divisor comum é* 1*, ou seja* $mdc(a,b) = 1$.

Exemplo 2.18. *Oa números* 15 *e* 28 *são primos entre si, pois,* $mdc(15,28) = 1$.

Outro resultado apresentado por Euclides (BICUDO, 2009), relacionado com números primos é o Lema de Euclides.

Proposição 2.19 (Lema de Euclides)**.** *Sejam* $a, b, p \in \mathbb{N}$ *com p primo. Se* $p \mid a \cdot b$*, então* $p \mid a$ *ou* $p \mid b$.

Demonstração. É suficiente provar que se $p \mid a \cdot b$ e $p \nmid a$ então $p \mid b$. Suponha que p não divide a, assim mdc(a,p)=1. Pelo Algoritmo de Euclides estendido, existem $m, n \in \mathbb{Z}$ tais que

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

e

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

Como $p \mid a.b$ e $p \mid p$, então $p \mid b$. □

Exemplo 2.20. *Sejam* $a = 6$*,* $b = 8$ *e* $p = 3$*, tem-se que* $p \mid 48$ *e* $p \mid 6$.

Este resultado é essencial para compreensão de assuntos como simplificação de frações.

A utilização do Teorema Fundamental da Aritmética como uma estratégia de cálculo no cotidiano do aluno, requer que o mesmo seja capaz de produzir listas simples de números primos. E uma maneira eficiente de gerar estas lista é utilizar o Crivo de Eratóstenes.

Proposição 2.21 (Crivo de Eratóstenes)**.** *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração. Suponha, por absurdo, que n não seja divisível por nenhum primo p, com $p^2 \leq n$. Seja q o menor primo que divide n, então $n = q \cdot k$ e $q < k$. Dai $q^2 = q \cdot q \leq q \cdot k = n \Rightarrow q^2 \leq n$, o que é absurdo, pois por hipótese n não é divisível por qualquer primo q tal que $q^2 \leq n$. Logo n é primo.

□

Resultados mais complexos, relacionados a números primos, são estudados apenas em Teoria dos Números. Como por exemplo o Pequeno Teorema de Fermat. A demonstração deste teorema, a ser apresentada neste trabalho, requer um resultado prévio.

Proposição 2.22. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. Se $i = 1$, tem-se que $\binom{p}{1} = p$ e $p \mid p$. Tome então $1 < i < p$. Como $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p.(p-1)\cdot\ldots\cdot(p+1-i)}{i!}$. Tem-se que $i! \mid p \cdot (p-1) \cdot \ldots \cdot (p+1-i)$. Mas, o Máximo Divisor Comum entre $i!$ e p é 1; assim $i! \mid (p-1) \cdot \ldots \cdot (p+1-i)$.

Logo, $\binom{p}{i} = p \cdot n$, onde $n = \frac{(p-1)\cdot\ldots\cdot(p+1-i)}{i!}$ e $p \mid \binom{p}{i}$. □

Exemplo 2.23. *Seja $p = 5$, tem-se que $\binom{5}{1} = 5$, $\binom{5}{2} = 10$, $\binom{5}{3} = 10$ e $\binom{5}{4} = 5$, são todos divisíveis por 5.*

Teorema 2.24 (Pequeno Teorema de Fermat)**.** *Dado um número primo p, tem-se que p divide o número $a^p - a$. Para todo $a \in \mathbb{N}$.*

Demonstração. Será utilizado o princípio da indução sobre a. Para $a = 1$ tem-se $a^p - a = 0$, assim $p \mid 0$, o que é verdade.

Suponha que o resultado é válido para algum $a > 1$ e será provado que vale para $a + 1$. Tem-se que:

$$(a+1)^p - (a+1) = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \ldots + \binom{p}{p-1} a + 1 - (a+1) =$$

$$a^p - a + \binom{p}{i} a^{p-1} + \binom{p}{2} a^{p-2} + \binom{p}{p-1} a$$

Pela hipótese de indução, $p \mid a^p - a$ e pela Proposição 2.22 $p \mid \binom{p}{i}$, $0 < i < p-1$, e segue que $p \mid (a+1)^p - (a+1)$. □

Exemplo 2.25. *Seja $p = 5$ e $a = 2$, tem-se que $2^5 - 2 = 30$ e $5 \mid 30$.*

Dentre os trabalhos de Fermat, destaca-se também os números de Fertat.

Definição 2.26. *Todo número da forma $F_n = 2^{2^n} + 1$, com $n \in \mathbb{N}$ é chamado número de Fermat.*

Fermat conjecturou que estes números eram primos, em uma carta enviada a Marin Mersene (BOYER, 1996). De fato, os números de Fermat quando n assume os valores $0, 1, 2, 3, 4$, são primos.

Exemplo 2.27. $F_0 = 2^{2^0} + 1 = 2 + 1 = 3.$

$F_1 = 2^{2^1} + 1 = 4 + 1 = 5.$

$F_2 = 2^{2^2} + 1 = 16 + 1 = 17.$

$F_3 = 2^{2^3} + 1 = 256 + 1 = 257.$

$F_4 = 2^{2^4} + 1 = 65536 + 1 = 65537.$

Posteriormente Euler mostrou que quando $n = 5$, F_5 é um número composto.

Exemplo 2.28. $F_5 = 2^{2^5} + 1 = 4294967296 + 1 = 4294967297 = 641 \cdot 6700417.$

Outro resultado relacionado a produção de números primos são os Números de Mersene. O nome é uma homenagem a Marin Mersene que se dedicou ao estudo destes números e suas propriedades.

Definição 2.29. *Todo número da forma $M_q = 2^q - 1$ sendo q um número primo é chamado número de Mersene.*

Muitos Números de Mersene são primos, estes são conhecidos como Primos de Mersene.

Um fato interessante é a possibilidade de se obter uma sequência de k números compostos. Estas sequências de números compostos são chamadas de Desertos de Primos.

Proposição 2.30. *Seja $k \in N$ com $k > 0$, a sequência de números consecutivos $(k+1)!+2, (k+1)!+3, (k+1)!+4, \ldots, (k+1)!+k, (k+1)!+(k+1)$, contém k números compostos.*

Demonstração. Basta observar que $2 \mid (k+1)!+2$, $3 \mid (k+1)!+3$,$4 \mid (k+1)!+4$,...,$(k+1) \mid (k+1)!+(k+1)$. □

Vale ressaltar que este resultado não contradiz infinitude dos números primos.

3 UMA FÓRMULA PARA PRIMOS

Euclides provou que existem infinitos números primos, ou seja, existem primos maiores do que todos os já conhecidos. A demanda por primos cada vez maiores deve-se principalmente às aplicações em criptografia e segurança na internet.

O maior número primo conhecido atualmente é $2^{57885161} - 1$ que é um primo de Mersene conforme Definição 2.29. Esse primo foi descoberto por Curtis Cooper , da Universidade Central do Missouri em Warrensburg e tem 17 milhões de dígitos.

O gráfico da Figura 3, mostra a evolução do maior número primo conhecido de 1950 a 2014.

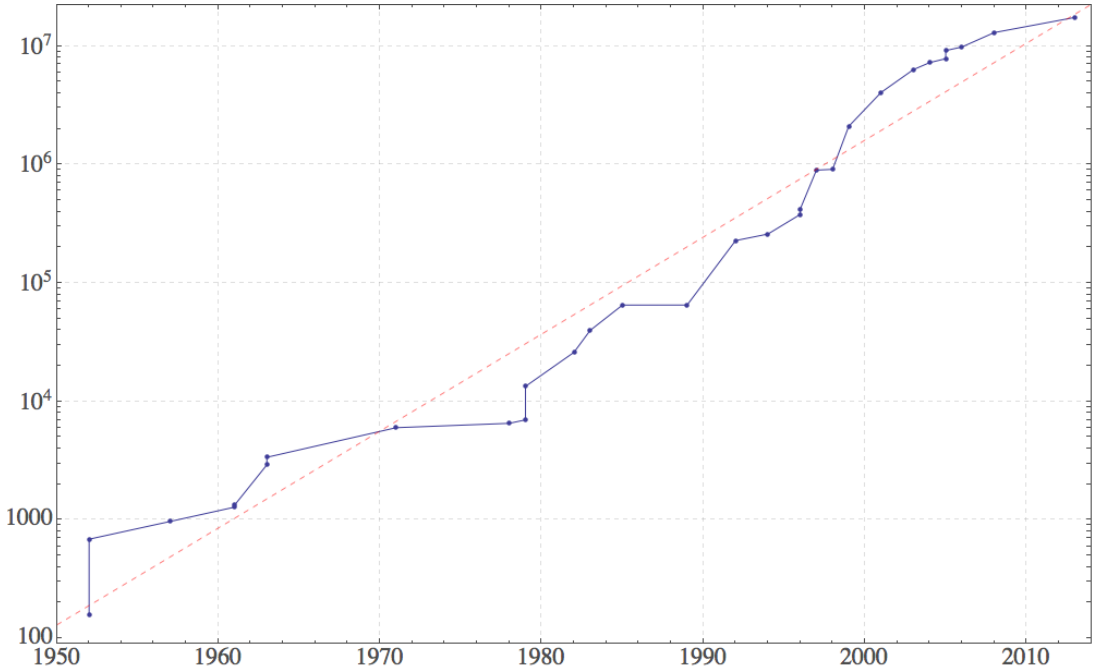


Figura 3: O maior primo por ano até 2014.

O teste de primalidade de números grandes só é viável com o uso de programas específicos, por exemplo os testes de Lucas-Lehmer (BRUCE, 1993), de Solovay-Strassen (SOLOVAY; STRASSEN, 1977) e de Miller-Rabin (RABIN, 1980) e mesmo assim demanda um esforço computacional muito grande. Em um artigo publicado na Revista do Professor de ma-

temática (TERADA, 2001), afirma que para fatorar um número com 100 dígitos, um computador demoraria aproximadamente 74 anos.

A organização *Electronic Frontier Foundation*, oferece prêmios por números primos recordes, US$ 150 mil e US$ 250 mil a quem descobrir os primeiros números primos com 100 milhões e 1 bilhão de dígitos, respectivamente.

Uma fórmula para geração de números primos foi procurada por matemáticos durante muito tempo. Por exemplo, em 1772, Euler destacou que a função quadrática $f(x) = x^2 + x + 41$, fornece números primos para os 40 primeiros naturais, $0, 1, 2, \ldots, 39$. Como o gráfico desta função é uma parábola de concavidade voltada para cima com vértice em $x = -\frac{1}{2}$, seu gráfico é simétrico em relação ao ponto $\left(-\frac{1}{2}, 0\right)$, assim estendendo o domínio para os valores inteiros equidistantes de $\left(-\frac{1}{2}, 0\right)$, tem-se uma sequência de 80 números inteiros consecutivos, $-40, -39, \ldots, 38, 39$, tais que $f(x)$ são números primos. Este trinômio apresentado por Euler possui outras propriedades interessantes, como, por exemplo $f(x)$ é um quadrado perfeito apenas para $f(40) = f(-41) = 41^2$ e $f(x)$, $x \in \mathbb{Z}$ não é divisível por nenhum inteiro entre 1 e 41.

A fórmula de Euler além de não gerar unicamente números primos, por exemplo $f(40) = 1681 = 41 \times 41$, também não gera números primos menores que 41, visto que sua imagem é $y \geq 40,75$.

W. H. Mills (MILLS, 1947) mostrou que existe um número real k tal que $\left[k^{3^n}\right]$ é um número primo para $n = 1, 2, 3, \ldots$, onde $[z]$ denota o maior inteiro não superior a z. Mills mostrou a existência de k mas o seu valor é desconhecido.

Logo seria necessário apenas se descobrir um valor para esta número real k. Mas posteriormente E. M. Wright (WRIGHT, 1954) provou que existem infinitas possibilidades para k para o resultado de W. H. Mills.

Outra função capaz de gerar todos primos foi apresentada em 1963, B. M. Bredihin (BREDIHIN, 1963). Bredihin provou que $f(x,y) = x^2 + y^2 + 1$ assume valores primos para infinitos pares (x,y). No entanto $f(x,y) = x^2 + y^2 + 1$ não gera apenas valores primos.

Ross Honsberger (HONSBERGER, 1976) apresentou uma função sobrejetora capaz de produzir todos os números primos, e que produz apenas números primos. O resultado tem como base o Teorema de Wilson.

O Teorema de Wilson foi provado por Lagrange aproximadamente 100 anos após Leibniz ressaltar sua importância. A conjectura desse teorema foi atribuída a Sir John Wilson, por

Edward Waring em 1770.

Este teorema é um resultado surpreendente, pois dá uma condição necessária e suficiente para um número ser primo, e assim, teoricamente, tem-se uma maneira de distinguir os números primos. A demonstração a ser apresentada requer o conceito de congruência e alguns outros resultados.

Definição 3.1 (Equação Diofantina Linear com duas incógnitas)**.** *Chama-se Equação Diofantina Linear com duas incógnitas, as equações na forma, $ax+by=c$, com a, b, c, x e $y \in \mathbb{Z}$, $a \neq$ ou $b \neq 0$.*

Proposição 3.2. *Uma equação diofantina linear $ax+by=c$, com a, b, c, x e $y \in \mathbb{Z}$, $a \neq$ ou $b \neq 0$, admite solução, se e somente se, $d = mdc(a,b) \mid c$.*

Demonstração. ($\Rightarrow$) Seja o par de inteiros (x_0, y_0) uma solução da equação, então vale a igualdade:

$$ax_0 + by_0 = c.$$

Como $d \mid a$ e $d \mid b$, então $d \mid c$.

($\Leftarrow$) Como $d = mdc(a,b)$, pelo Algoritmo de Euclides estendido, existem inteiros x_0 e y_0 tais que:

$$ax_0 + by_0 = c.$$

Por hipótese que $d \mid c$ segue que $c = dt$, para algum $t \in \mathbb{Z}$. Assim,

$$c = dt = (ax_0 + by_0) = a(x_0 t) + b(y_0 t),$$

o que mostra que o par $(x_0 t, y_0 t)$ é solução da equação considerada. □

Proposição 3.3. *Seja o par de inteiros (x_0, y_0) uma solução particular da equação diofantina $ax+by=c$ com a, b e $c \in \mathbb{Z}$, $a \neq 0$ ou $b \neq 0$. Então essa equação admite infinitas soluções (x,y) na forma $x = x_0 + \frac{b}{d}t$ e $y = y_o - \frac{a}{d}t$ com $t \in \mathbb{Z}$.*

Demonstração. Sejam (x,y) soluções da equação $ax+by=c$, então: $ax+by=c=ax_0+by_0$ o que equivale a $a(x-x_0) = b(y_0-y)$.

Supondo $a = dr$ e $b = ds$, tem-se que $r(x-x_0) = s(y_0-y)$ onde $mdc(r,s) = 1$. Como $r \mid s(y_0-y)$, então $(y_0-y) = rt$ para algum $t \in \mathbb{Z}$.

Portanto $y = y_0 - rt = y_0 - \frac{a}{d}t$.

De modo análogo tem-se $r(x-x_0) = srt$ para algum $t \in \mathbb{Z}$.

E portanto $x = x_0 + st = x_0 + \frac{b}{d}$.

Assim para todo $t \in \mathbb{Z}$ o par $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ é solução da equação diofantina dada. □

Definição 3.4 (Congruência)**.** *Sejam a e b inteiros e $m \in \mathbb{N}$, $m \neq 0$. Diz-se que a é congruente a b módulo m se m divide a diferença $a - b$.*

Em outros termos, a é congruente a b se existe um inteiro k tal que: $a - b = k \cdot m$.

Exemplo 3.5. *Sejam $a = 7$, $b = 12$ e $m = 5$. Diz-se que $7 \equiv 12 (mod\ 5)$, pois $12 - 7 = 5$ e $5 \mid 5$.*

Definição 3.6 (Congruências lineares)**.** *Chama-se congruência linear toda congruência da forma,*

$$a \cdot x \equiv b (mod\ m)$$

onde a, b e x são inteiros e m é um inteiro positivo.

Todo inteiro x_0 tal que $a \cdot x_0 \equiv b (mod\ m)$ é uma solução dessa congruência linear.

Exemplo 3.7. *A congruência linear $3 \cdot x \equiv 1 (mod\ 5)$, tem como solução $x = 2$, como pode ser verificado, $3 \cdot 2 = 6 \equiv 1 (mod\ 5)$.*

Teorema 3.8. *Se $d \mid b$, sendo $d = mdc(a,m)$, então a congruência linear $a \cdot x \equiv b\,(mod\ m)$ tem precisamente d soluções mutuamente incongruentes módulo m.*

Demonstração. Pelo algoritmo da divisão euclidiana a congruência $a \cdot x \equiv b\,(mod\ m)$ é equivalente a equação diofantina linear $a \cdot x - m \cdot y = b$, que tem solução se e somente se $mdc(a,m) = d$. Como $d \mid b$, o par de inteiros x_0, y_0 é uma solução particular da equação $a \cdot x - m \cdot y = b$, então todas as outras soluções desta equação são dadas pelas fórmulas: $x = x_0 + \frac{m}{d}\ t$, $y = y_0 + \frac{a}{d}\ t$, onde t é um inteiro arbitrário.

Dentre os infinitos inteiros dados pela primeira das fórmulas consideremos somente os d números que resultam de $t = 0, 1, 2, \ldots, d-1$. Assim temos os números:

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d}, \ldots,\ x_0 + (d-1)\,\frac{m}{d},$$

vamos mostrar que esses valores são incongruentes módulo m.

Considere dois valores para t, t_1 e t_2 com $0 \leq t_1 < t_2 \leq d-1$. Se dois valores dentre $x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d}, \ldots$ e $x_0 + (d-1)\,\frac{m}{d}$ fossem congruentes, teríamos:

$$\left(\frac{m}{d}\right) t_1 \equiv \left(\frac{m}{d}\right) t_2\,(mod\ m) \Rightarrow t_1 \equiv t_2\,(mod\ m) \Rightarrow t_1 - t_2 \equiv 0\,(mod\ m)\,.$$

E isto é impossível, porque $0 < t_2 - t_1 < d - 1$.

Assim todos os valores x_0, $x_0 + \frac{m}{d}$, $x_0 + \frac{2m}{d}, \ldots, x_0 + (d-1)\left(\frac{m}{d}\right)$, são incongruentes módulo m.

Quando $t > d - 1$, tem-se pelo algoritmo da divisão euclidiana que:

$t = d \cdot q + r$, onde $0 \leq r \leq d - 1$.

Assim existem exatamente d soluções incongruentes módulo m para a congruência $a \cdot x \equiv b \,(mod\, m)$. □

Corolário 3.9. *Se $mdc(a,m) = 1$, então a congruência $a \cdot x \equiv b \,(mod\, m)$ tem uma única solução módulo m.*

Definição 3.10. *Seja a um número inteiro, chama-se inverso de a módulo m um inteiro a_0 tal que $a \cdot a_0 \equiv 1 \,(mod\ m)$*

Teorema 3.11. *Se $mdc(a,m) = 1$, então a tem um único inverso módulo m.*

Demonstração. Com efeito, se $mdc(a,m) = 1$, então a congruência linear

$$a \cdot a_0 \equiv 1 \,(mod\ m)$$

tem uma única solução a_0, que é o único inverso do inteiro a módulo m. □

Teorema 3.12 (Teorema de Wilson)**.** *Um número p é primo se, e somente se,*

$$(p-1)! \equiv (p-1) mod\, p.$$

Demonstração. ($\Rightarrow$) Será demonstrado por redução ao absurdo. Primeiramente relembre duas propriedades relativas a divisão.

Sejam $a \neq 0, b \neq 0, c \in \mathbb{Z}$:

Se $a \mid b$, e $b \mid c$, então $a \mid c$.

Se $a \neq 1$ e $a \mid b$, então $a \nmid (b+1)$.

Suponha, por absurdo, que para algum p composto $(p-1)! \equiv (p-1)\, mod\, p$. Então tem-se que $p \mid (p-1)! + 1$.

Sendo p um número composto, então pelo Teorema 2.7, pode ser decomposto em fatores primos menores que p, tome q um dos fatores de p, de modo que $q \mid (p-1)!$.

Por outro lado, pela transitividade, $p \mid (p-1)!+1 \Rightarrow q \mid (p-1)!+1$. Assim tem-se que $q \mid (p-1)!$ e $q \nmid (p-1)!+1$, o que é absurdo. Portanto p é primo.

($\Leftarrow$) Deve-se mostrar que se p é primo então $p \mid (p-1)!+1$.

O resultado é válido para $p = 2$, pois:

$$(2-1)!+1 = 1!+1 = 2 \text{ e } 2 \mid 2.$$

Então se $p > 2$, p é ímpar.

Considere os números $1, 2, 3, \ldots, p-1$, tem-se que $p-1$ é uma quantidade par.

Seja a algum inteiro dentre $1, 2, 3, \ldots, p-1$, então conforme a Definição 3.11 a congruência linear:

$a \cdot a_0 \equiv 1\,(mod\ m)$, admite uma única solução pois $mdc(a, p) = 1$.

Tem-se que $a = a_0$ apenas para $a = 1$ e $a = p-1$, pois:

$aa_0 \equiv 1(mod\,p) \Rightarrow a^2 \equiv 1(mod\,p) \Rightarrow a^2 - 1 \equiv 0(mod\,p) \Rightarrow (a-1)(a+1) \equiv 0(mod\,p)$.

Assim

$$(a-1) \equiv 0(mod\,p) \Rightarrow a = 1$$

ou

$$(a+1) \equiv 0(mod\,p) \Rightarrow a = p-1.$$

Omitindo os valores 1 e $p-1$ dentre $1, 2, 3, \ldots, p-1$, tem-se $\dfrac{p-3}{2}$ pares congruentes a 1 módulo p.

Desta forma pode-se agrupar os fatores do produto $2 \times 3 \times 4 \times \ldots \times (p-2)$ de modo que:

$2 \times 3 \times 4 \times \ldots \times (p-2) \equiv 1(mod\ p)$.

Portanto : $(p-1)! \equiv 1 \times 2 \times 3 \times \ldots (p-2) \times (p-1) \equiv p-1(mod\ p) \Rightarrow p \mid (p-1)!+1$.

□

Utilizando o Teorema de Wilson, a proposição a seguir apresenta uma função de domínio $\mathbb{N} \times \mathbb{N}^*$ e contra-domínio o conjunto dos números primos, que é sobrejetora. Ou seja, esta função além de gerar apenas números primos, gera todos os números primos.

Proposição 3.13 (Fórmula para gerar números primos)**.** *Sejam $x, y \in \mathbb{N}$, $y \neq 0$, e P o conjunto formado por todos os números primos. A função $f : \mathbb{N} \times \mathbb{N}^* \to P$ definida por $f(x,y) =$*

$\frac{y-1}{2}[|a^2-1|-(a^2-1)]+2$, *com* $a = x(y+1)-(y!+1)$ *é sobrejetora.*

Demonstração. Deve-se provar duas afirmações, que $f(x,y)$ é sempre um número primo e que f fornece todos os números primos.

Como o número a é inteiro, tem-se que, a^2 também é inteiro.

Assim tem-se dois casos para a: $a^2 \geq 1$ ou $a^2 = 0$.

Se $a^2 \geq 1$, $|a^2-1| = a^2-1$ e $f(x,y) = 0+2 = 2$.

Se $a^2 = 0$, $f(x,y) = \frac{y-1}{2} \times 2+2 = y+1$.

Substituindo $a = 0$ em $a = x(y+1)-(y!+1)$, tem-se que $x(y+1) = (y!+1)$, como x, y e $y!+1$, são todos naturais, $y+1 \mid y!+1$, e pelo Teorema de Wilson, $y+1$ é primo. Portanto $f(x,y)$ é sempre um número primo.

Novamente utilizando o Teorema de Wilson, tem-se que se p é primo, $p \mid (p-1)!+1$, e o quociente $\frac{(p-1)!+1}{p}$ é um número natural, assim pode-se calcular $f\left(\frac{(p-1)!+1}{p}, p-1\right)$.

Calculando o valor de a tem-se:

$a = \frac{(p-1)!+1}{p} \times (p-1+1)-[(p-1)!+1] = 0$.

Segue então que, $f\left(\frac{(p-1)!+1}{p}, p-1\right) = p-1+1 = p$.

Esta igualdade prova que para todo número primo, é sempre possível associar um par (x,y) tal que $f(x,y) = p$. □

O resultado embora surpreendente, em nada contribui para explicar a distribuição dos números primos, pois existe uma predileção pelo número 2, visto que $f(x,y) = 2$ sempre que $a^2 \geq 1$.

Enquanto que para fornecer os demais primos deve-se calcular: $f\left(\frac{(p-1)!+1}{p}, p-1\right)$, com p primo.

Note que quando p assume um valor grande, $\frac{(p-1)!+1}{p}$ assume um valor maior ainda.

Como por exemplo para gerar o número primo 13, deve-se calcular:

$f(36846277, 12) = 13$

Essa grande diferença entre p e $\frac{(p-1)!+1}{p}$, torna inviável a aplicação desta função para obtenção de números primos muito grandes.

4 UMA INTERPRETAÇÃO GEOMÉTRICA DE NÚMEROS NATURAIS

Um número natural n, $n > 0$, pode ser representado como um muro, de blocos bidimensionais, com lados denominados neste trabalho, altura h e comprimento l, tais que $n = h \cdot l$, com $h, l \in \mathbb{N}$.

Para isto é necessário admitir a unidade como um bloco quadrado fundamental de lados $1 \cdot 1$.

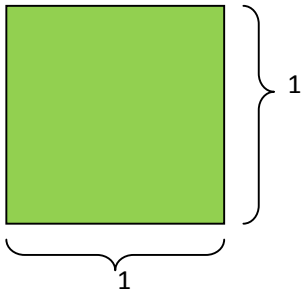
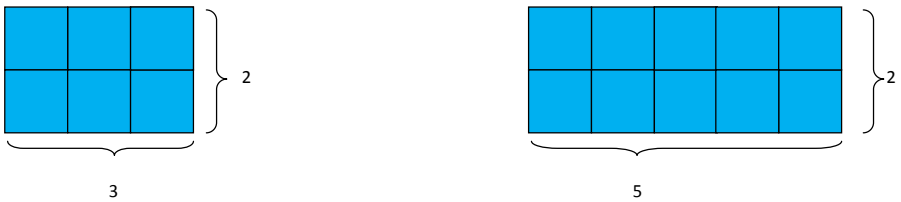


Figura 4: Bloco de unidade.

Os números 6 e 10 por exemplo, podem ser representados da seguinte forma:



(a) 6 (b) 10

Figura 5: Exemplo de representação geométrica dos números 6 e 10.

Esta interpretação geométrica fornece uma caracterização interessante para os números primos e compostos.

Propriedade 4.1. *Na representação geométrica acima, um número primo p, somente pode ser representado como um bloco com p unidades alinhadas.*

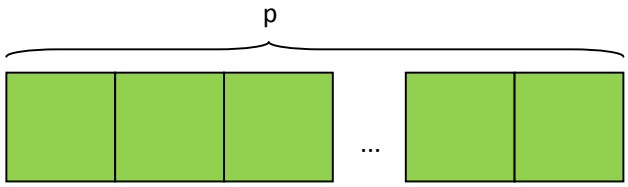


Figura 6: Representação de um número primo p.

Propriedade 4.2. *Na representação geométrica acima, um número n composto sempre pode ser representado como um bloco com lados medindo h e l, tais que* $n = h \cdot l$ *com* $h,l \in \mathbb{N}$ *e* $h,l > 1$.

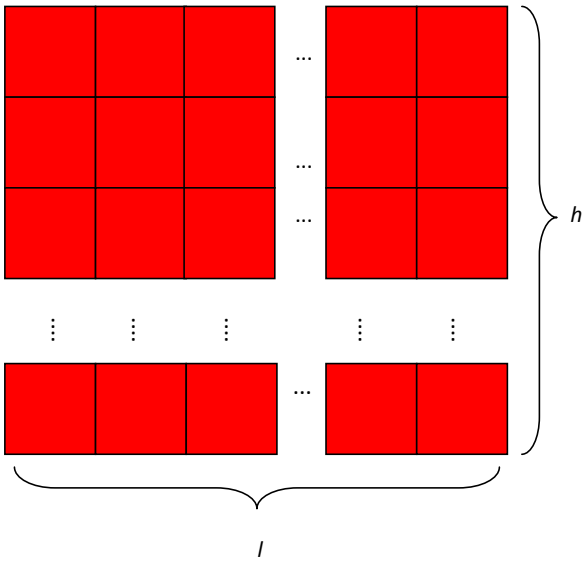


Figura 7: Representação de um número composto $n = h \cdot l$**.**

Note que enquanto um número primo admite uma única representação, um número composto tem pelo menos duas representações, $n = n \cdot 1 = h \cdot l$, como na figura 8.

Cada divisor de um número composto corresponde a uma medida de um dos possíveis lados. Com isso a divisibilidade também pode ser representada geometricamente.

Propriedade 4.3 (Representação geométrica de divisibilidade)**.** *Um bloco numérico* $n > 0$ *é divisível por* $h > 0$*, se e somente se, h for a medida de um lado de uma representação geométrica de n.*

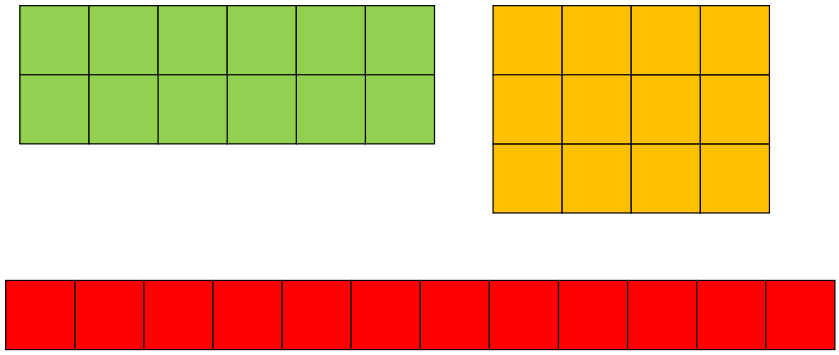


Figura 8: Representações do número 12**.**

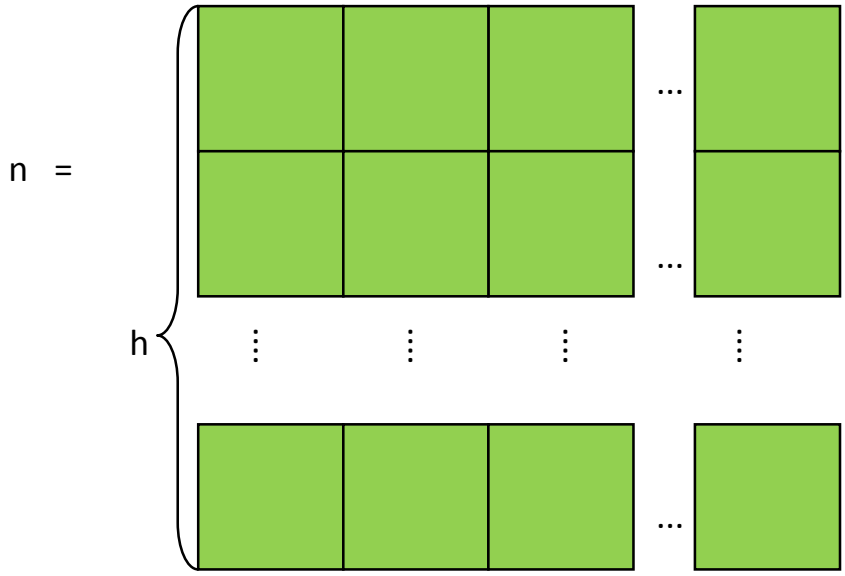


Figura 9: Representação de $h \mid n$**.**

Exemplo 4.4. *Na Figura 10 está representado que* $2 \mid 10$*.*

Exemplo 4.5. *Na Figura 11 está representado que* $2 \nmid 11$*.*

Exemplo 4.6. *Para determinar todos os divisores de* 15*, considera-se todas as representações geométricas de* 15*.*

Os divisores possíveis são 1*,* 3*,* 5 *e* 15*.*

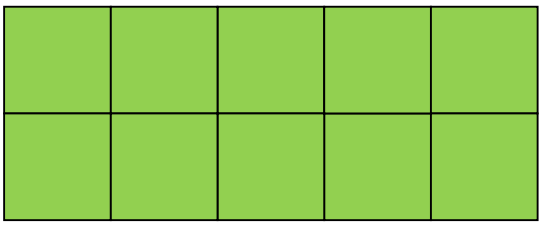


Figura 10: 10 **representado como bloco de altura** 2**.**

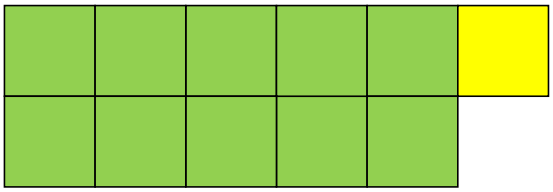


Figura 11: 11 **não pode ser representado como bloco de altura** 2**.**

Figura 12: Representações geométricas do número 15**.**

A visualização dos números naturais como blocos auxilia o aluno, mesmo no ensino fundamental, a compreender as demonstrações de resultados como a infinitude dos números primos, Teorema 2.6 e do Teorema Fundamental da Aritmética 2.7.

Ilustração da demonstração da infinitude dos números primos, Teorema 2.6. Suponha que p seja o maior número primo, então existe uma quantidade finita de primos.

Considere o número n, igual 1 mais o produto de todos os números primos, Figura 13.

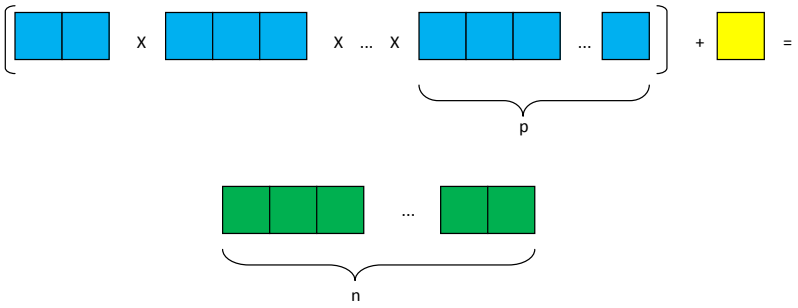


Figura 13: Representação de n.

Tem-se que n é primo ou composto.

Se n é primo, tem-se uma contradição com a hipótese de p ser o maior primo, pois $n > p$.

Se n é composto, então é divisível por algum número primo menor ou igual a p. Este primo que divide n, consequentemente divide o produto dos primos até p, blocos azuis da Figura 13, e divide também 1, bloco em amarelo da Figura 13, o que é absurdo. Logo existe algum primo maior que p que divide n.

As Figuras 14, 15 e 16, ilustram geometricamente a indivisibilidade de n por nenhum primo menor ou igual a p.

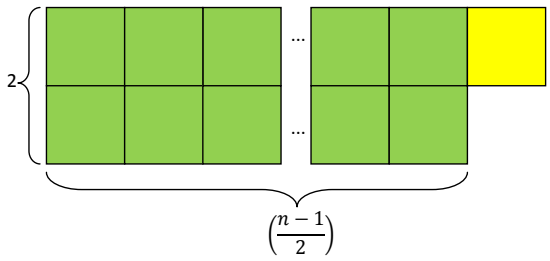


Figura 14: $2 \nmid n$**.**

Como não é possível representar n como um bloco retangular tendo como medida de um lado um número primo menor ou igual a p, pois em todas as tentativas sobra um bloco de uma unidade. Assim, n não é divisível por nenhum primo menor ou igual a p. Logo, n é primo ou existe um primo maior que p que divide n. Em ambos os casos conclui-se que sempre existirá um número primo maior do que p proposto inicialmente. Portanto existem infinitos números primos. □

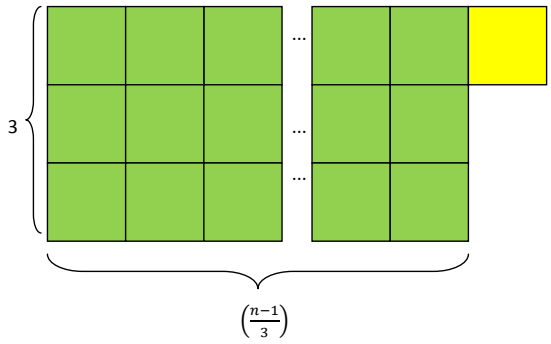


Figura 15: $3 \nmid n$**.**

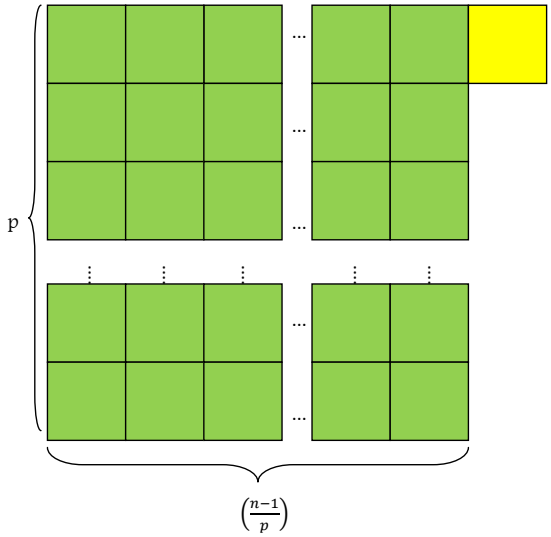
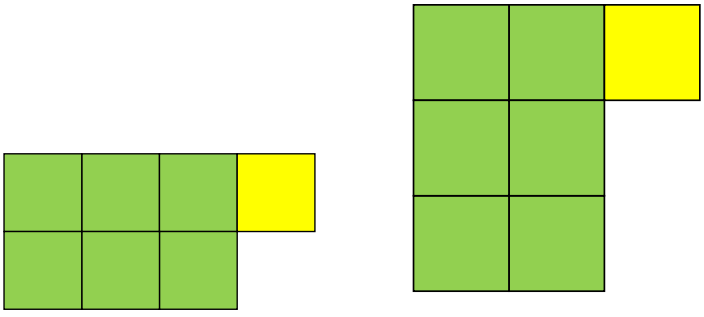


Figura 16: $p \nmid n$**.**

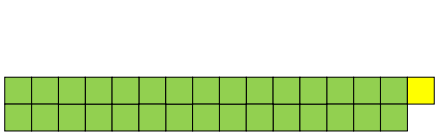
Exemplo 4.7. *Suponha que existam apenas dois números primos* 2 *e* 3*. Considere número n formado por* 1 *mais o produto dos dois números primos, assim* $n = 2 \cdot 3 + 1 = 7$*.*



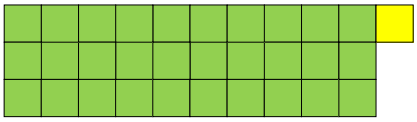
(a) $2 \nmid 7$ (b) $3 \nmid 7$

Como $2 \nmid 7$ *e* $3 \nmid 7$ *existe um primo diferente de* 2 *e* 3 *que divide n.*

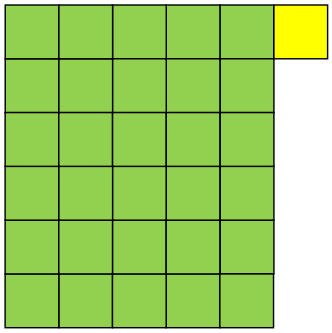
Exemplo 4.8. *Suponha que existam três números primos* 2, 3 *e* 5. *Considere número n formado por* 1 *mais o produto dos três números primos, assim* $n = 2 \cdot 3 \cdot 5 + 1 = 31$.



(c) $2 \nmid 31$



(d) $3 \nmid 31$



(e) $5 \nmid 31$

Como $2 \nmid 31$, $3 \nmid 31$ *e* $5 \nmid 31$ *existe um primo diferente de* 2, 3 *e* 5 *que divide n.*

Ilustração da demonstração do Teorema Fundamental da Aritmética, Teorema 2.7. Seguindo a mesma abordagem da ilustração já apresentada anteriormente, deve-se mostrar que todo número natural $n > 1$, ou é primo ou se escreve de modo único, exceto pela ordem, como o produto de números primos.

Existência: Seja n um número natural, tal que $n > 1$. Se n for primo, conforme a propriedade 4.1, ele possui uma única representação geométrica, e assim n é a sua própria decomposição, que portanto existe.

Se n é composto, então conforme a Propriedade 4.2 n pode ser representado geometricamente como um bloco de lados medindo h e l maiores que 1.

Seja p_1 o menor número primo que divide n, é possível representar n como um bloco de lados medindo p_1 e n_1.

Se n_1 for um número primo a decomposição de n é $p_1 \cdot n_1$.

Se n_1 for composto e p_2 o seu menor divisor primo, é possível representar n_1 como um bloco de lados medindo p_2 e n_2.

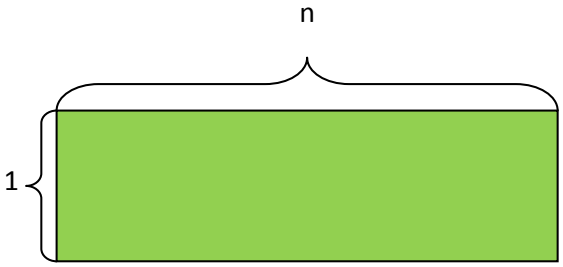


Figura 17: Representação geométrica de n primo.

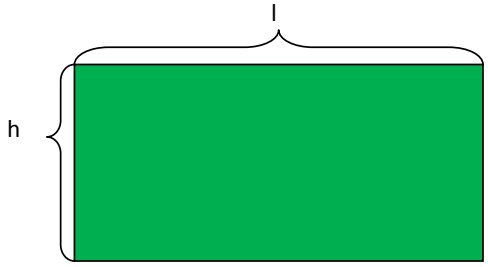


Figura 18: Representação geométrica de $n = h \cdot l$.

Se n_2 for primo a decomposição de n é $p_1 \cdot p_2 \cdot n_2$.

Se n_2 for composto, novamente possuirá um menor divisor. A cada nova representação se obtém lados com medidas menores que as da representação anterior, logo este procedimento não pode ser repetido indefinidamente.

Assim se obterá uma sequência de números primos $p_1, p_2, \ldots, p_k$ com $k \in \mathbb{N}$, não necessariamente distintos, todos divisores de n. E o produto de todos estes números é a decomposição de n com a forma $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, que portanto existe.

Unicidade: Se um número n é primo, possui uma única representação geométrica conforme a definição 4.1 ilustrada na Figura 6, sendo ele mesmo a sua única decomposição.

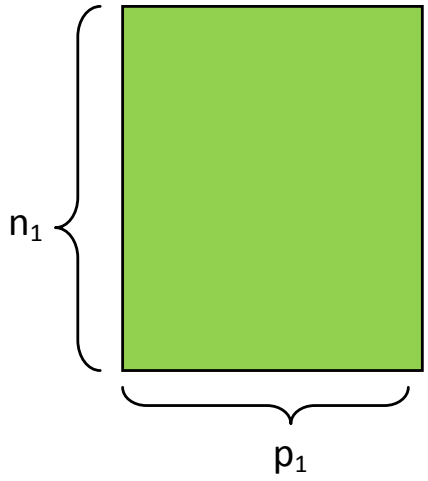


Figura 19: Representação geométrica de $n = p_1 \cdot n_l$.

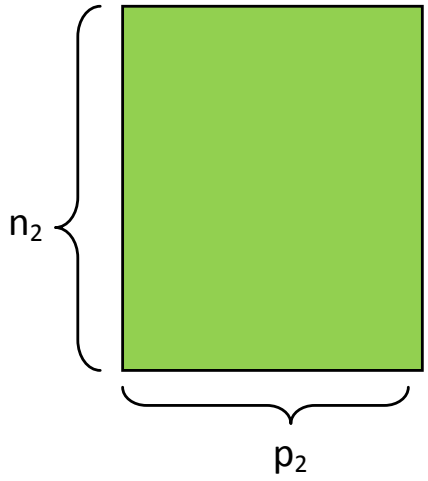


Figura 20: $p_1 \nmid n$.

Suponha que um número composto n possua duas decomposições:

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$$

com $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots q_s$ números primos.

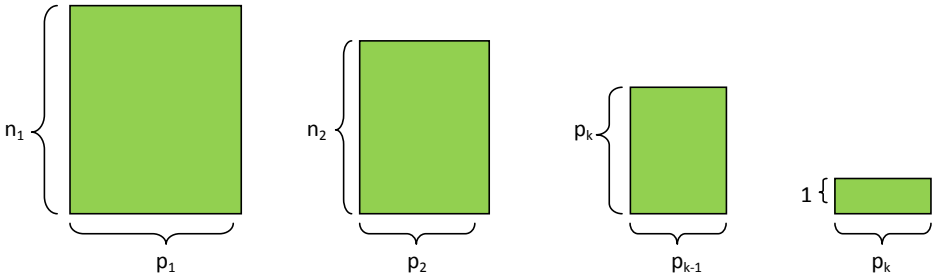


Figura 21: As medidas dos lados de n diminuindo até p_k.

Como n é um número natural pode-se escrever:

$$p_1^{\alpha_1-1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} = \frac{q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}}{p_1}.$$

O número $p_1^{\alpha_1-1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ é natural, logo $p_1 \mid q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$, ou seja p_1 é igual a algum fator de $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$. Repetindo este procedimento com todos os fatores de $p_1^{\alpha_1-1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ se verifica que todos dividem $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$.

Logo cada número primo do produto $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ é igual a algum número primo do produto $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_s^{\beta_s}$, contradizendo a suposição de que existem duas decomposições em fatores primos de n.

□

Exemplo 4.9. *Ilustração da decomposição do número* 60 *em fatores primos. Agrupa-se primeiramente* 60 *em um bloco de lados medindo* $2 \cdot 30$.

Figura 22: Representação de $60 = 2 \cdot 30$.

Em seguida agrupa-se 30 *em um bloco de lados medindo* $2 \cdot 15$.

Novamente agrupa-se 15 *em um bloco de lados medindo* $3 \cdot 5$, *e como* 5 *é um número primo, tem-se que a decomposição procurada é* $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

Nas ilustrações acima foram utilizadas divisões sucessivas por números primos, conhecidos previamente. Para saber se um dado número é primo ou não, aplica-se a ele teste de

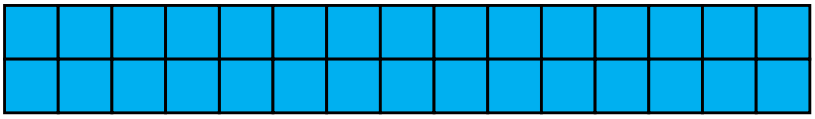


Figura 23: Representação de $30 = 2 \cdot 15$**.**

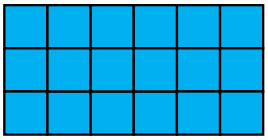


Figura 24: Representação de $15 = 3 \cdot 5$**.**

Figura 25: Representação de $5 = 5 \cdot 1$**.**

primalidade. Um método para se saber se um número é primo, já citado na Proposição 2.21 deste trabalho, é o Crivo de Eratóstenes.

Ilustração do Crivo de Eratóstenes 2.21. O Crivo de Erastótenes afirma que se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.

Sejam $2, 3, 5, \ldots, p$ todos os números primos, tal que $p^2 \leq n$ organizados em ordem crescente.

Suponha que n não seja divisível por nenhum primo até p, assim ao tentarmos representar n como um bloco de altura p seu comprimento seria $\frac{n}{p}$, e sobraria um resto r, tal que $r < p$.

Como $\frac{n}{p} \leq p$,visto que n não é divisível por $2, 3, 5, \ldots, p$, assim n não pode ser representado por um bloco tal que a medida de um dos lados seja um primo menor ou igual a p, Portanto n é primo. □

Exemplo 4.10. *Para verificar se o número* 41 *é primo ou composto, utilizando o Crivo de Erástotenes, deve-se verificar se* 41 *não é divisível pelos primos* $2, 3$ *e* 5*, ilustrado nas figuras a seguir.*

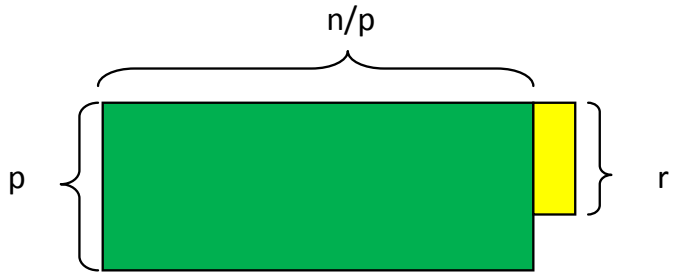


Figura 26: Representação geométrica de $p \nmid n$.

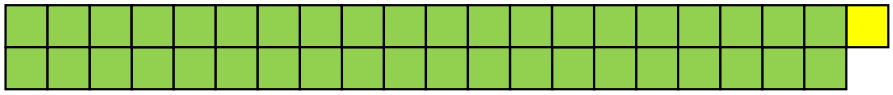


Figura 27: $2 \nmid 41$**.**

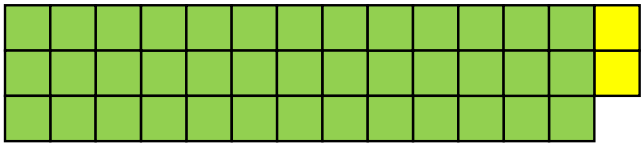


Figura 28: $3 \nmid 41$**.**

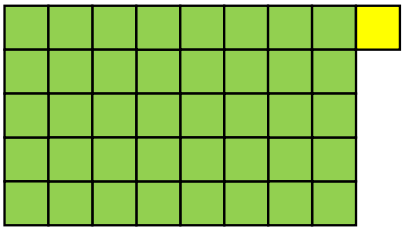


Figura 29: $5 \nmid 41$**.**

Outra forma bastante interessante de aplicar o Crivo de Eratóstenes é usar funções periódicas para marcar o múltiplos dos números ímpares, por exemplo como feito na Figura 30, com funções formadas por semicircunferências. Como 2 é primo os demais pares são compostos, assim resta analisar apenas os ímpares para determinar os demais primos. A Figura 30

é chamada de “cometa”e é constituída de “cabeça”e “cauda”. A cabeça fica centrada na origem do eixo horizontal e é constituída de camadas de círculos concêntricos de raio ímpar. No exemplo da Figura 30 a cauda é formada pelas curvas de semicircunferências de mesmos raios que aparecem na cabeça do cometa, arranjadas de forma que as curvas sejam suaves. Outras funções periódicas poderiam ser usadas para formar a cauda do cometa. Os números no eixo horizontal que estão na cabeça do cometa e com apenas uma linha passando sobre eles, são números primos. Um número no eixo horizontal que está na cauda do cometa, é primo se nenhuma curva passa sobre ele e ele é menor que o quadrado do primeiro ímpar da cauda pelo qual não passa nenhuma curva. Por exemplo, na Figura 30, temos que 3, 5 e 7 estão na cabeça do cometa e apenas uma curva passa por eles, logo são primos. Na cauda todos números pelos quais não passa nenhuma curva e que são menores que $11^2 = 121$ são primos, por exemplo $11, 13, 17, 19, 23, 29, 31, 37$ e 43.

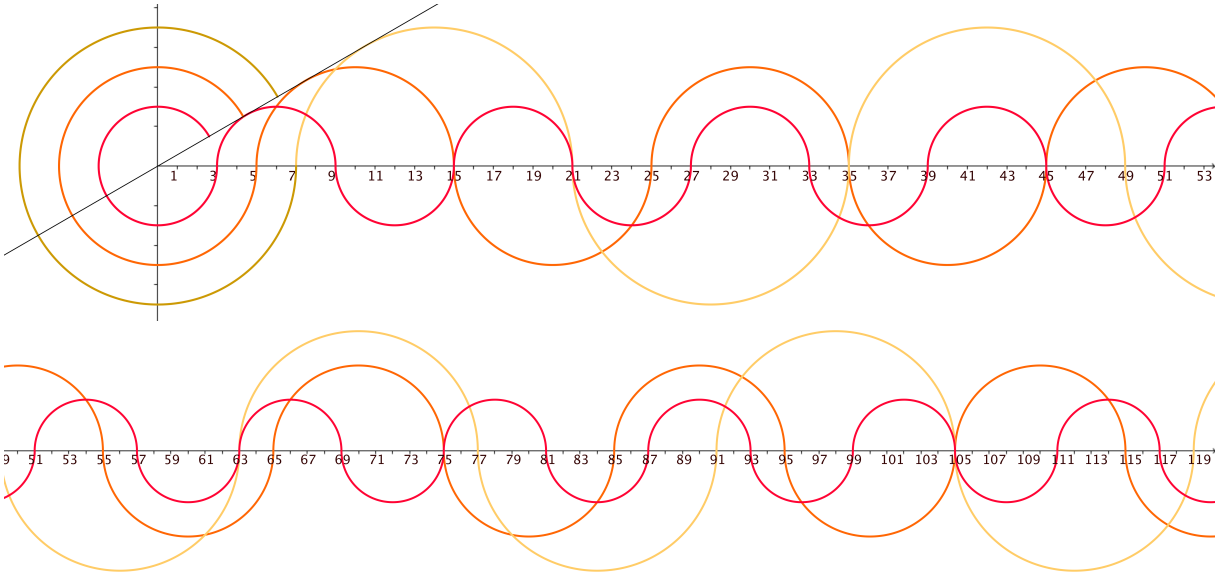


Figura 30: Cometa.

Os conteúdos de Máximo Divisor Comum e Mínimo Múltiplo Comum, também podem ser interpretados geometricamente.

Propriedade 4.11. *O Máximo Divisor Comum entre dois ou mais números é a maior medida de lado comum possível entre as suas representações geométricas.*

Exemplo 4.12. *Determine geometricamente o Máximo Divisor Comum entre* 8, 12 *e* 16.

Transformando os números em blocos, tem-se:

Comparando as medidas dos lados, verifica-se que o Máximo Divisor Comum entre 8, 12 e 6 é 4.

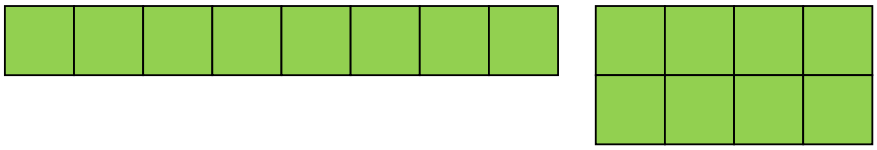


Figura 31: Representações geométricas do 8**.**

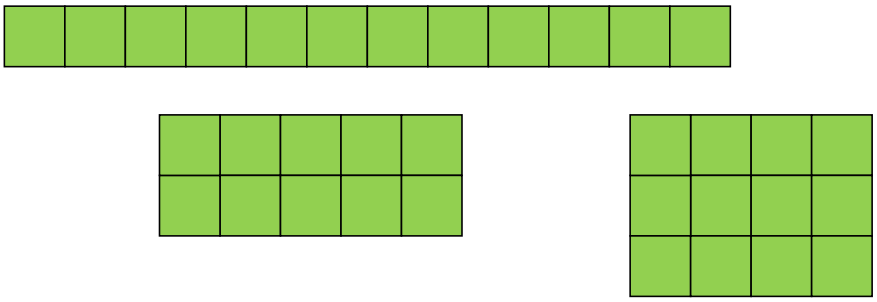


Figura 32: Representações geométricas do número 12**.**

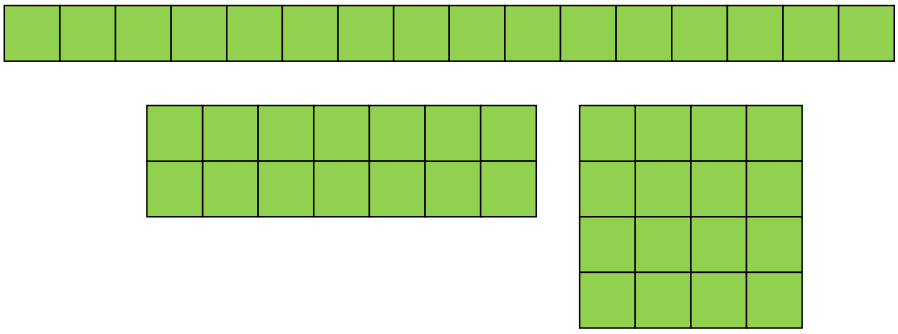


Figura 33: Representações geométricas do número 16**.**

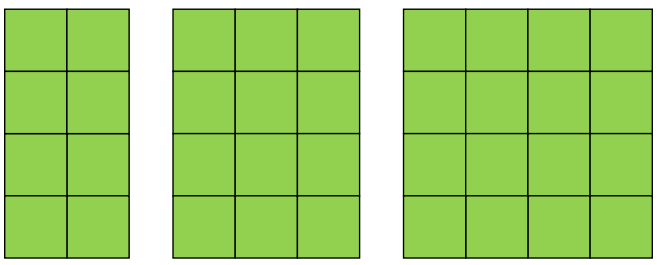


Figura 34: 4 **é a maior medida de lado comum entre os blocos** 8**,** 12 **e** 16**.**

Propriedade 4.13. *O Mínimo Múltiplo Comum entre dois ou mais números é o menor número que os comporta como medidas de lados de suas representações geométricas, simultaneamente.*

Exemplo 4.14 (Ilustração do Mínimo Múltiplo Comum entre 3, 4 e 6)**.**

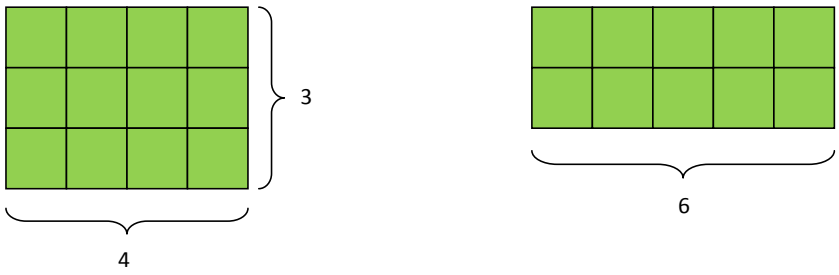


Figura 35: Representação do número 12 **como blocos com lados medindo** 3**,** 4 **e** 6**.**

5 SUGESTÕES DE ATIVIDADES

As sugestões de atividades estão divididas em duas partes. Primeiramente as atividades se referem as interpretações geométricas de propriedades, resultados e demonstrações relacionados a números primos, propostas no Capítulo 4.

As demais sugestões de atividades são exercícios e problemas envolvendo diversos assuntos, estudados na educação básica, as quais são resolvidas utilizando o Teorema Fundamental da Aritmética.

Todas as atividades a seguir foram aplicadas em sala de aula, no intuito de melhorar a compreensão dos conteúdos estudados. Se mostraram bastante atraente para os alunos, principalmente as atividades envolvendo os blocos e interpretações geométricas.

5.1 ATIVIDADES COM BLOCOS NUMÉRICOS BIDIMENSIONAIS

Para a realização deste experimento devem ser confeccionados 100 blocos quadrados de madeira ou outro material disponível. Como sugestão utilizar placa de MDF com 15 milímetros e cortar os quadrados com lados 3 cm.

As atividades propostas tem a abordagem apresentada no Capítulo 4 e exploram vários conteúdos referentes a números primos, divisibilidade, Máximo Divisor Comum e Números Primos entre Si.

Atividade 5.1 (Divisibilidade)**.** *Verifique se o número natural $n \leq 100$ é ou não divisível por uma quantidade natural $p \leq 100$.*

O aluno deverá tentar agrupar os n blocos em uma forma retangular de lado p. Se obter uma forma retangular, tem-se que n é divisível por p. Se não for possível obter um retângulo com uma dimensão p, tem-se que n não é divisível por p.

Atividade 5.2 (Divisores de um número)**.** *Determine todos os divisores do número natural n, $n \leq 100$.*

Utilizando o raciocínio análogo a atividade 5.1, o aluno deve começar representando o número n como um retângulo $n \times 1$, e em seguida tentar representar como um retângulo de lado 2, e assim sucessivamente até descobrir todos os divisores possíveis.

Atividade 5.3 (Crivo de Eratóstenes)**.** *Determinar se um número natural n é primo. O aluno receberá um número natural $n \leq 100$ e deverá verificar se este possui algum divisor primo p, tal que $p^2 \leq n$.*

Para isto o aluno deverá representar n como um retângulo de dimensões um número primo dentre $2, 3, 5$ e 7, visto que $11^2 = 121 > n$. Se não for possível representar n como um retângulo com estas dimensões, n é primo.

Atividade 5.4 (Decomposição em fatores primos)**.** *Efetuar a decomposição em fatores primos de um número natural $n \leq 100$.*

Deve-se verificar se é possível agrupar os n blocos como um retângulo de dimensão um número primo dentre $2, 3, 5, \ldots, p$.

Começa-se tentando representar como um retângulo com uma das dimensões o número 2. Caso seja possível, 2 é um dos fatores de sua decomposição. Deve-se repetir o processo apenas com os blocos que formam a outra dimensão do retângulo, caso não seja mais possível representar o número restante como um bloco com uma dimensão 2 tenta-se com o número 3, e assim sucessivamente até se obter um último fator primo. O produto de todas as dimensões possíveis é a decomposição de n.

Atividade 5.5 (Máximo Divisor Comum)**.** *Determine o Máximo Divisor Comum entre dois números naturais p e q menores que 100.*

Utilizando o mesmo raciocínio da atividade 5.2, determine todos os divisores de p e q, o maior valor dentre todos os divisores possíveis é o Máximo Divisor Comum.

Atividade 5.6 (Números Primos entre si)**.** *Determine se os números p e q são ou não primos entre si.*

O aluno deve manipular os números p e q tentando obter formas retangulares que possuem uma dimensão em comum. Se a única dimensão comum for 1 diz-se que p e q são primos entre si.

5.2 ATIVIDADES ABORDANDO O TEOREMA FUNDAMENTAL DA ARITMÉTICA

Nas atividades a seguir estão sugestões de utilização do Teorema Fundamental para resolução de exercícios de problemas envolvendo conteúdos do ensino básico.

Atividade 5.7. *Determine o máximo divisor comum entre os números abaixo:*

a) 18 *e* 42

b) 16 *e* 15

c) 210 *e* 84

Resolução: *Aplicando o Teorema Fundamental da Aritmética, verifica-se todos os fatores dos números em questão.*

a) $18 = 2 \cdot 3 \cdot 3$ *e* $42 = 2 \cdot 3 \cdot 7$*, o único fator comum é o* 3*, assim o máximo divisor comum é o próprio* 3*;*

b) $16 = 2 \cdot 2 \cdot 2 \cdot 2$ *e* $15 = 3 \cdot 5$*, não existe fator primo comum, assim o máximo divisor comum é a unidade.*

c) $210 = 2 \cdot 3 \cdot 5 \cdot 7$ *e* $84 = 2 \cdot 2 \cdot 3 \cdot 7$*, os fatores comuns são* $2 \cdot 3 \cdot 7$*, assim o máximo divisor comum é* $2 \cdot 3 \cdot 7 = 42$*.*

Atividade 5.8. *Utilizando o Teorema Fundamental da Aritmética, simplifique as seguintes frações até sua forma irredutível:*

a) $\frac{12}{15} =$

b) $\frac{14}{35} =$

c) $\frac{144}{360} =$

Resolução: *Aplicando o Teorema Fundamental da Aritmética simultaneamente no numerador e no denominador das frações os fatores comuns ficam evidenciados. Cancelando esses fatores comuns encontra-se a forma irredutível dessas frações.*

a) $\frac{12}{15} = \frac{2 \cdot 2 \cdot 3}{3 \cdot 5} = \frac{4}{5}$

b) $\frac{14}{35} = \frac{2 \cdot 7}{5 \cdot 7} = \frac{2}{5}$

c) $\frac{144}{360} = \frac{2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3}{2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5} = \frac{2}{5}$

Atividade 5.9. *Simplifique as seguintes frações algébricas:*

a) $\frac{a^2}{ab} =$

b) $\frac{x^4 y^3}{2x^3 y^5} =$

c) $\frac{20x^2}{15x} =$

Resolução: *Estendendo o conceito abordado no estudo do Teorema Fundamental da*

Aritmética pode-se, sem perder a generalidade, supor que cada variável seja um número primo diferente dos demais que possam aparecer eventualmente. Procedendo de forma semelhante a atividade 5.8 encontram-se as formas irredutíveis das frações.

a) $\frac{a^2}{ab} = \frac{a \cdot a}{a \cdot b} = \frac{a}{b}$

b) $\frac{x^4y^3}{2x^3y^5} = \frac{x \cdot x \cdot x \cdot x \cdot y \cdot y \cdot y}{2 \cdot x \cdot x \cdot x \cdot y \cdot y \cdot y \cdot y \cdot y} = \frac{x}{2y^2}$

c) $\frac{20x^2}{15x} = \frac{2 \cdot 2 \cdot 5 \cdot x \cdot x}{3 \cdot 5 \cdot x} = \frac{4x}{3}$

Atividade 5.10. *Os números* 9 *e* 72 *são termos de uma progressão geométrica de razão natural. Calcule os possíveis valores para esta razão, e quantos termos existem entre* 9 *e* 72*.*

Resolução: *Decompondo os termos da progressão obtêm-se* $9 = 3 \cdot 3$ *e* $72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$.

Pela definição de Progressões Geométricas, sabe-se que os termos posteriores são obtidos multiplicando um primeiro termo por uma razão. Como nesta progressão a razão é um número natural, seus termos estão em ordem crescente, desta forma o número 9 *ocupa uma posição anterior ao número* 72 *nesta sequência. Sendo assim se um termo anterior conter fatores diferentes de* 1*, estes fatores estarão contidos em todo termo posterior. Os fatores incomuns a esses termos fazem parte da razão. Logo as razões possíveis para esta progressão são* 8 *ou* 2*. Se a razão for* 8 *os termos* 9 *e* 72 *são consecutivos e não existem termos entre os mesmos. Se a razão for* 2*, existem os termos* 18 *e* 36 *entre* 9 *e* 72*.*

Atividade 5.11. *O volume de um paralelepípedo é* $1728cm^3$*. Suas arestas são números naturais e estão em progressão geométrica de razão natural. Quais os possíveis valores para estas arestas?*

Resolução: *Como o volume de um paralelepípedo é a multiplicação de suas três arestas, decompondo o volume encontra-se todos os fatores das arestas, assim* $1728 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$*. Para agrupar esta sequência de fatores em uma multiplicação de três fatores em progressão geométrica de razão natural, deve-se compreender que os fatores diferentes de* 1 *que aparecerem em um termo anterior, também aparecerão em todos os demais termos posteriores. Cada fator diferente em dois termos consecutivos faz parte da razão, e sua quantidade dobrará a cada termo posterior. Um fator diferente de* 1 *contido no primeiro termo, aparecerá também no segundo e terceiro, logo este fator deve existir em quantidade múltipla de três na decomposição de* 1728*. Um fator diferente que aparecer no segundo termo irá compor a razão, e também deve existir em quantidade múltipla de três pois sua quantidade dobrará no terceiro termo.*

Assim tem-se as seguintes possibilidades.

Se o primeiro termo for 1*, o segundo termo deve ser a própria razão, pois* 1 *é o elemento neutro da multiplicação, e o terceiro será o quadrado da razão e terá o dobro da quantidade de fatores da razão.*

Agrupando os fatores de 1728 *em três partes conforme descrito acima , tem-se:*

$$\overbrace{1}^{\text{primeiro termo}} \cdot \underbrace{2\cdot 2\cdot 3}_{\text{razão}} \cdot \overbrace{2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 3}^{\text{razão ao quadrado}} = 1\cdot 12\cdot 144.$$

Portando uma sequência possível é 1*,* 12 *e* 144*.*

Se o primeiro termo não for 1 *pode ser qualquer número formado agrupando os fatores de* 1728 *em grupos de três iguais. Desta forma os valores, diferentes de* 1*,possíveis para o primeiro termo são* 2*,* 3*,* 4*,* 6 *e* 12*.*

Se o primeiro termo for 2*, sobram três fatores* 2 *e* 3 *para formar a razão,*

$$\overbrace{2\cdot 2\cdot 2}^{\text{fatores do primeiro termo repetidos}} \cdot \underbrace{2\cdot 3}_{\text{razão}} \cdot \overbrace{2\cdot 2\cdot 3\cdot 3}^{\text{razão ao quadrado}} \quad \textit{que será } 2\cdot 3 = 6.$$

Portanto outra sequência possível é 2*,* 12 *e* 72*.*

Se o primeiro termo for 3*, sobram seis fatores* 2 *para formar a razão,*

$$\overbrace{3\cdot 3\cdot 3}^{\text{fatores do primeiro termo repetidos}} \cdot \underbrace{2\cdot 2}_{\text{razão}} \cdot \overbrace{2\cdot 2\cdot 2\cdot 2}^{\text{razão ao quadrado}} \quad \textit{que será } 2\cdot 2 = 4.$$

Portanto outra sequência possível é 3*,* 12 *e* 48*.*

Se o primeiro termo for 4*, sobram três fatores* 3 *para formar a razão,*

$$\overbrace{2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2}^{\text{fatores do primeiro termo repetidos}} \cdot \underbrace{3}_{\text{razão}} \cdot \overbrace{3\cdot 3}^{\text{razão ao quadrado}} \quad \textit{, que será } 3.$$

Portanto outra sequência possível é 4*,* 12 *e* 36*.*

Se o primeiro termo for 6*, sobram três fatores* 2 *para a razão,*

$$\overbrace{2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 3}^{\text{fatores do primeiro termo repetidos}} \cdot \underbrace{2}_{\text{razão}} \cdot \overbrace{2\cdot 2}^{\text{razão ao quadrado}} \quad \textit{que será } 2.$$

Portanto outra sequência possível é 6*,* 12 *e* 24*.*

Se o primeiro termo for 12*, não sobram fatores para a razão, assim:*

$$\overbrace{2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 3}^{\text{fatores do primeiro termo repetidos}} \cdot \underbrace{1}_{\text{razão}} \cdot \overbrace{1}^{\text{razão ao quadrado}} \quad \text{que será } 1.$$

Portanto outra sequência possível é 12, 12 *e* 12.

As soluções deste problema são os paralelepípedos de arestas, 1,12 *e* 144*cm;* 2, 12 *e* 72*cm;* 3, 12 *e* 48*cm;* 4,12 *e* 36*cm;* 6, 12 *e* 24*cm ou um cubo de aresta* 12*cm.*

Atividade 5.12. *Qual o quinto termo da expressão formada pelo desenvolvimento do binômio* $(2x-\frac{1}{4})^8$*?*

Resolução:

O quinto elemento desta expressão é formado pelo produto de $(2x)^4$ *por* $\frac{1}{4}^4$ *por* 70 *que é o quinto número da oitava linha do Triângulo de Pascal. Aplicando o Teorema fundamental da Aritmética neste produto, e considerando o fator x como um número primo distinto dos demais, tem-se:* $(2x)^4 \cdot (\frac{1}{4})^4 \cdot 70 = \frac{2\cdot 2\cdot 2\cdot 2\cdot x\cdot x\cdot x\cdot x\cdot 2\cdot 5\cdot 7}{2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2}$*. Cancelando os fatores comuns encontra-se o termo procurado* $\frac{35x^4}{8}$.

Atividade 5.13 (Dominó com fatoração)**.** *Substitua cada uma das* 28 *peças do jogo de dominó por* 28 *números formados pela multiplicação dois números primos ou um quadrado de um número primo.*

Desenvolvimento:

As peças são desenvolvidas tomando como base sete números primos. Como exemplo, serão utilizados os números $2,3,5,7,11,13$ *e* 17.

Recorte 28 *cartões de papel e neles escreva os números formados pela multiplicação de dois fatores primos, dentre os números acima citados. Assim os cartões deverão conter os números:* $4,6,10,14,22,26,34,9,15,21,33,39,51,25,35,55,65,85,49,77,91,119,121,143,187,169,221$ *e* 289.

Para jogar, usa-se as mesmas regras do jogo de dominó comum, as peças que possuírem os mesmos fatores primos se encaixam. Uma vez encaixado um fator, o seu outro fator fica disponível para o próximo encaixe. Vence o jogador que encaixar todos seus números primeiro.

6 CONCLUSÃO

A motivação inicial deste trabalho era oferecer uma alternativa de apresentação de conteúdos relacionados a números primos ensinados na educação básica. Visto que muitos alunos concluem a educação básica sem saber o que é um número primo e pra que serve. Estes assuntos são na maioria das vezes abordados de uma forma superficial e carente significado.

Acreditando ser possível a compreensão de demonstrações simples para alunos do ensino fundamental, o presente trabalho mostrou definições e demonstrações de resultados importantes sobre assuntos relacionados a números primos, como a da infinitude dos números primos e do Teorema Fundamental da Aritmética. Resultados estes apresentados em um breve estudo histórico da evolução dos assuntos relacionados a números primos. Desde os primeiros estudos dos gregos, até resultados mais sofisticados como os de Euler. Para leitores bem informados nestes assuntos o presente trabalho poderá servir como uma revisão.

A visualização dos números naturais como blocos proposta neste trabalho, apresentou uma alternativa de abordagem de diversos assuntos de uma maneira concreta, que facilitam compreensão de propriedades e demonstrações para alunos de 6 ano e demais séries do ensino básico.

A função geradora de primos, de Ross Honsberger, é um resultado surpreendente, visto que a mesma e sua demonstração, são desconhecidas de muitos matemáticos. Viu-se que embora esta função seja capaz de gerar todos os primos, em nada contribui para explicar a distribuição dos primos.

As sugestões de atividades propostas no trabalho fornecem alternativas de apresentação e de abordagem de assuntos relacionados a números primos e práticas de fácil aplicação no ensino básico.

Espera-se com este trabalho ter estimulado a curiosidade sobre números primos.

REFERÊNCIAS

BICUDO, I. **Os Elementos - Euclides**. São Paulo: UNESP, 2009.

BOYER, C. B. **História da matemática**. 2. ed. São Paulo: Edgard Blücher, 1996.

BREDIHIN, B. M. **Applications of the dispersion method in binary additive problems**. Dokl. Akad. Nauk. SSSR, 149:9-11, 1963.

BRUCE, J. W. *A Really Trivial Proof of the Lucas-Lehmer Test*. The American Mathematical Monthly, v. 100, n. 4, p. 370-371, Abril 1993.

FERREIRA, A. B. de H. **Dicionário Básico da Língua Portuguesa**. Rio de Janeiro: Nova Fronteira, 1988.

FREIRE, P. **Pedagogia do Oprimido**. 8. ed. Rio de Janeiro: Terra e Paz, 1980.

IEZZI, G. ; DOLCE, O. ; MACHADO, A. **Matemática e realidade**. 2. ed. São Paulo: Atual, 1991.

Great Internet Mersenne Prime Search. Disponível em: http://www.mersenne.org/

HONSBERGER, R., **Mathematical Gems**, The Mathematical Association of America., v. 2 (1976) 29–37.

LIMA, E. L. ; CARVALHO P. C. P. ; WAGNER E. ; MORGADO A. C.**A Matemática do Ensino Médio**, Coleção do Professor de Matemática. 9 ed. Rio de Janeiro: SBM, v. 1 (2006),

MILLS, W. H., *A prime-representing function*, Bull. Amer. Math. Soc., 53 (1947) 604.

RABIN, M. O., *Probabilistic algorithm for testing primality*. Journal of Number Theory, v. 12, n. 1, p. 128-138, 1980.

RIBEIRO, J. da S. **Projeto Radix - Matemática - 6º ano**. 1. ed. São Paulo: Scipione, 2009.

SOLOVAY, R.; STRASSEN, V., **A Fast Monte-Carlo Test for Primality**. SIAM Journal on Computing, v. 6, n. 1, p. 84-85, 1977.

TERADA, R., **Criptografia e a importância das suas aplicações**, Revista do Professor de matemática, volume 12. SBM, p. 1-8, 1998.

WRIGHT, E. M., **A class of representing functions**, J. London Math. Soc., 29 (1954) 63–71.