UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Natália Ojeda Mastronicola

Aritmética por apps

São José do Rio Preto
2016

Natália Ojeda Mastronicola

Aritmética por apps

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre, junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. João Carlos Ferreira Costa

São José do Rio Preto
2016

Mastronicola, Natália Ojeda.
Aritmética por apps / Natália Ojeda Mastronicola. -- São José do Rio Preto, 2016
72 f. : il., tabs.

Orientador: João Carlos Ferreira Costa
Dissertação (mestrado profissional) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas

1. Matemática (Ensino fundamental) - Estudo e ensino. 2. Aritmética - Estudo e ensino. 3. Números primos. 4. Números - Divisibilidade. 5. Aplicativos móveis. 6. Tecnologia educacional. I. Costa, João Carlos Ferreira. II. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU – 511(07)

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Natália Ojeda Mastronicola

Aritmética por apps

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre, junto ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Banca Examinadora

Prof. Dr. João Carlos Ferreira Costa
UNESP – São José do Rio Preto
Orientador

Prof. Dr. Juliano Gonçalves Oler
UFU - Uberlândia

Profª. Drª. Flávia Souza Machado da Silva
UNESP – São José do Rio Preto

São José do Rio Preto
15 de Fevereiro de 2016

AGRADECIMENTOS

A Deus, em primeiro lugar, que iluminou meu caminho durante esta jornada, me capacitou e me deu saúde e forças para realizar este trabalho.

Aos meus pais, Antônio Carlos e Valnia, por acreditarem no meu potencial, me dando apoio incondicional para que tudo isso fosse possível.

Ao meu orientador, Prof. Dr. João Carlos Ferreira Costa, por conduzir pacientemente e incentivar a concretização deste trabalho, enriquecendo-o com valiosos ensinamentos.

A todos os professores do PROFMAT de São José do Rio Preto que com dedicação fizeram a partilha do conhecimento.

Aos meus colegas de curso pela companhia e ajuda durante todo este período sendo essenciais para que eu chegasse até aqui.

À Kamila pelo suporte e incentivo constante, me lembrando a todo o momento que eu era capaz e que posso chegar ainda mais longe.

Aos alunos do Colégio Pollicare pelo carinho e dedicação com que realizaram as atividades propostas neste trabalho.

A Capes pelo importante apoio financeiro.

Por fim, a todos que fazem parte da minha vida e que contribuíram de forma direta ou indireta na minha formação acadêmica.

“Tudo é loucura ou sonho no começo. Nada do que o homem fez no mundo teve início de outra maneira – mas tantos sonhos se realizaram que não temos o direito de duvidar de nenhum.”

(Monteiro Lobato)

RESUMO

Neste trabalho, utilizamos aplicativos para smartphones e tablets (apps) no ensino da Aritmética, abordando tópicos como divisibilidade através da decomposição em fatores primos; mínimo múltiplo comum e máximo divisor comum. Este trabalho foi desenvolvido junto aos alunos do Ensino Fundamental. Além disso, tratamos também de temas normalmente não trabalhados no Ensino Básico como Teorema de Bézout e Função de Euler. O uso desses aplicativos aproveita-se dessa crescente tecnologia em poder dos alunos, auxiliando a aprendizagem de forma inovadora e tornando-a mais atraente.

Palavras-chaves: aritmética; números primos; divisibilidade; ensino de matemática; aplicativos; smartphones; tablets.

ABSTRACT

In this work, we use some special apps for smartphones and tablets to teach Arithmetic, covering topics such as divisibility, prime decomposition of numbers, least common multiple and greatest common divisor. This study was developed with the students of elementary school. We also treat topics which are not normally worked in basic Education as Bézout's theorem and Euler function. We notice the use of these apps in the classroom brought more enthusiasm for students.

Keywords: arithmetic; prime numbers; divisibility; apps for smartphones and tablets.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Ainda hoje cientistas, engenheiros, pesquisadores e professores de Matemática, gastam muito tempo com cálculos diversos manualmente. Entretanto, com o advento das novas tecnologias, vários softwares e aplicativos vêm sendo desenvolvidos com a finalidade de economizar tempo, mas de modo, que os resultados sejam ainda confiáveis.

Nas salas de aula do Ensino Fundamental e Médio podemos notar o aumento do número de computadores pessoais e smartphones entre os alunos, que despendem muito do seu tempo a estes utensílios. Assim, nossa proposta neste trabalho é aproveitar a crescente tecnologia em poder dos alunos para apresentar alguns aplicativos gratuitos e descomplicados que auxiliam o usuário a acessar vários conteúdos de Matemática.

Como sabemos a Matemática não é a disciplina mais apreciada pela maioria dos alunos. Então, tentar explorar seus conceitos via ferramentas que são de uso cotidiano dos alunos é o nosso desafio. Claro que poderíamos explorar inúmeros temas e assuntos matemáticos, mas nos restringiremos a assuntos relacionados a números primos, decomposição em fatores primos, máximo divisor comum, mínimo múltiplo comum e função de Euler. Porém, os mesmos aplicativos tratados aqui, podem ser utilizados para outros temas igualmente interessantes.

O trabalho é constituído de três capítulos descritos brevemente a seguir.

No Capítulo 1, que está dividido em três partes, apresentamos a evolução histórica dos números primos, desde seus primeiros indícios na Grécia Antiga até os dias atuais, um embasamento teórico sobre números primos e uma aplicação na criptografia.

No Capítulo 2, apresentamos os *apps* (aplicativos para plataforma Android e IOS) sugeridos para nossa atividade, elencando suas funcionalidades.

No Capítulo 3, descrevemos a aplicação das atividades em sala de aula utilizando os aplicativos sugeridos.

Analisando todo esse processo, foi possível responder a questão da nossa pesquisa: “Utilizar tecnologias no ensino, em especial,

aplicativos para smartphones e tablets, incentivam e motivam o aluno, permitindo que eles construam uma aprendizagem significativa das propriedades de divisibilidade através da decomposição de um número em fatores primos?”.

Capítulo 1

NÚMEROS PRIMOS

Neste capítulo, trataremos dos números primos, contando sua evolução histórica, apresentando alguns resultados teóricos e mostrando uma aplicação importante na criptografia.

1.1 Números Primos – Parte Histórica

Enunciaremos a seguir, um histórico sobre a evolução dos números primos e alguns matemáticos importantes que contribuíram para este desenvolvimento. É claro que é impossível citar todos.

1.1.1 Pitagóricos (570 a 495 a.C.)

Os primeiros estudos envolvendo números primos surgiram na Grécia Antiga. Acredita-se que o nome *"números primos"* vem dos pitagóricos que classificavam os números em primários (que não podem ser escritos como uma multiplicação de outros números) e secundários (que são os gerados pelos primários).

A partir dos números primos os pitagóricos definiram números curiosos:

i) Número perfeito: é aquele igual à soma dos seus divisores próprios.

Exemplo: $6 = 1 + 2 + 3$.

ii) Número abundante: é aquele que é menor que a soma de todos os seus divisores próprios.

Exemplo: $12 < 1 + 2 + 3 + 4 + 6 = 16$.

iii) Número deficiente: é aquele que é maior que a soma de todos os seus divisores próprios.

Exemplo: $15 > 1 + 3 + 5$.

iv) Números amigáveis: são pares de números, onde cada um deles é a soma dos divisores próprios do outro.

Exemplo: 220 e 284.

Divisores de 220: 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 e 110.
Divisores de 284: 1, 2, 4, 71 e 142.

Boyer (1974) conta que um matemático pitagórico, Espeusipus, afirmava que um dos motivos para o dez ser o número adorado pelos gregos é por ele ser o menor número inteiro n que possui exatamente tantos primos entre 1 e n quanto não primos.

1.1.2 Euclides (300 a.C.)

Na obra “Os Elementos”, Euclides de Alexandria, dedica os livros VII, VIII e IX para a Teoria dos Números. O livro VII se inicia com uma lista de vinte e duas definições distinguindo números, entre eles primos de compostos, além da definição de números perfeitos. Pedroso (2009) elenca algumas definições usadas por Euclides mostrando o seu enfoque geométrico:

Divisibilidade: um número é parte de outro, o menor do maior, quando ele mede o maior.

Número primo: um número é primo quando é mensurável apenas pela unidade.

Neste livro consta o algoritmo de Euclides usado para encontrar o máximo divisor comum de dois números. Eves (2011 p.181) explica este método: “Divida o maior dos dois números inteiros positivos pelo menor e então divida o divisor pelo resto. Continue esse processo de dividir o último divisor pelo último resto, até que a divisão seja exata. O divisor final é o mdc procurado.”

Ainda no sétimo livro, Euclides apresenta uma proposição que diz que: se a e b são primos com c, então ab é primo com c.

Euclides encerra esse livro com uma regra para encontrar o mínimo múltiplo comum de vários números.

No Livro IX, Euclides enuncia uma proposição equivalente ao Teorema Fundamental da Aritmética que diz: “Todo número inteiro maior que um pode ser escrito, de forma única, como um produto de número primos, salvo quanto à ordem de seus fatores”.

No nono livro Euclides também traz a demonstração da infinitude dos números primos. A proposição 20 diz que números primos são mais do que qualquer quantidade fixada de números primos. O que chama a atenção na prova de Euclides é o uso do método de redução ao absurdo. Garbi (2009 p.68) exibe sua opinião sobre esta demonstração de Euclides: “A prova de Euclides, por redução ao absurdo, é simples, precisa, surpreendente e constitui um exemplo clássico de elegância matemática.”

A prova de Euclides consiste no seguinte argumento: suponha que exista um número finito de primos, $p_1,\ p_2,\ p_3,\ p_4, \ldots p_n$. Multiplicando-se todos esses números, e adicionando 1, forma-se o número $N = p_1p_2p_3p_4 \ldots p_n + 1$. Se o número N for primo, isso contraria a hipótese, pois N não está na lista finita considerada. Se N for um número composto, ele será divisível por algum número primo, o que é impossível, pois sempre deixará resto 1 na divisão. Portanto, existem infinitos primos.

O último resultado do livro IX é um método para encontrar números perfeitos. Em notação atual; se $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$ é primo, então $2^{n-1}(2^n - 1)$ é perfeito.

1.1.3 Eratóstenes (276 a 194 a.C.)

Eratóstenes de Cirene se destacou em aritmética por desenvolver um método, que ficou conhecido como crivo de Eratóstenes, para encontrar todos os número primos menores que um certo número n dado. Du Sautoy (2007, p.31-32) explica seu procedimento e importância:

> até onde sabemos, a primeira pessoa a produzir tabelas de números primos foi o diretor da biblioteca do grande instituto de pesquisa da Grécia Antiga, localizada em Alexandria. Como um Mendeleiev matemático ancestral, Eratóstenes descobriu, no terceiro século a.C., um procedimento relativamente indolor para determinar quais números são primos em uma lista que inclua, por exemplo, os primeiros mil números. Eratóstenes escrevia inicialmente uma lista com todos os números de 1 a 1000. Em seguida, escolhia o primeiro primo, 2, e eliminava da lista todos os seus múltiplos. Como todos esses números eram divisíveis por 2, obviamente não eram primos. Logo, passava ao seguinte número que não fora eliminado, ou seja, o número 3, e eliminava também todos os seus múltiplos. Como todos eram divisíveis por 3, tampouco eram primos. Eratóstenes foi em frente, escolhendo sempre o seguinte número que não havia sido retirado da lista e eliminando todos os números divisíveis por esse novo primo. Com esse processo sistemático ele produziu tabelas de

> primos. Mais tarde, o procedimento passou a ser chamado de *crivo de Eratóstenes*. Cada novo primo gerava um "crivo" que Eratóstenes utilizava para eliminar os números não primos. O tamanho do crivo se alterava em cada etapa, mas ao atingir o número 1000, somente os números primos resistiam a todos os crivos.

Até hoje o crivo de Eratóstenes é uma importante ferramenta na busca por números primos, bastante empregada no Ensino Fundamental e Médio.

1.1.4 Fermat (Séc. XVII)

Na Idade Média, o estudo estagnou-se e apenas no século XVII Pierre de Fermat enriquece o universo dos números primos com o que ficou conhecido como o pequeno teorema de Fermat. Este teorema afirma: "se p é primo e a é primo com p, então $a^{p-1} - 1$ é divisível por p". De acordo com Boyer (1974), dois mil anos antes de Fermat havia um hipótese chinesa que afirmava que: "n é primo se, e somente se, $2^n - 2$ é divisível por n, para n maior que 1". Hoje sabemos que a recíproca dessa conjectura é falsa, pois $2^{341} - 2$ é divisível por 341, e 341 não é primo. Porém, a condição necessária é equivalente ao pequeno teorema de Fermat.

Fermat também sugeriu uma conjectura de que os inteiros da forma $F_n = 2^{2^n} + 1$ são sempre primos, ao verificar que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$. Porém Euler mostrou ser falsa quando $n = 5$, visto que $2^{2^5} + 1 = 4.294.967.297$ é divisível por 641 e, portanto, composto.

1.1.5 Mersenne (1588-1648)

Marin Mersenne foi um monge francês que se dedicou ao estudo da matemática. Ele se comunicava com Fermat e outros estudiosos da época. Mersenne estudou números primos da forma $M_p = 2^p - 1$, com p primo. Esses números ficaram conhecidos como primos de Mersenne. O número 127, por exemplo, é um primo de Mersenne, pois $127 = 2^7 - 1$. Mas o número 2047, apesar de poder ser escrito na forma $2^{11} - 1$, não é um número primo, pois $2047 = 23 \times 89$.

1.1.6 Euler (1707-1783)

Leonhard Euler redescobriu a teoria dos números de Fermat, trazendo demonstrações corretas para conjecturas de Fermat. Foi o primeiro a publicar uma demonstração para o pequeno teorema de Fermat e o generalizou com a chamada função de Euler, $\Phi(m)$, que é definida como o número de inteiros positivos menores que m que são primos com m.

Euler encontrou um contra exemplo para os primos de Fermat (vide em 1.1.4) e ainda exibiu 60 pares de números amigáveis.

1.1.7 Gauss (1777-1855)

Matemáticos eram fascinados em conseguir prever o próximo número primo, tentando criar fórmulas que gerassem tais números. Johann Carl Friedrich Gauss seguiu outro caminho, e começou a contar quantos números primos existiam até 10, depois até 100, até 1000 e assim por diante.

Gauss percebeu que os números primos eram cada vez mais raros e percebeu o surgimento de um padrão. Peruzzo (2012) apresenta uma tabela, onde x é o número considerado, $\pi(x)$ é a quantidade de primos existentes entre 1 e x, e $x/\pi(x)$ é, em média, quantos primos precisa-se contar até encontrar um número primo.

Tabela 1 – Padrões no surgimento de primos.

X	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4,0
1.000	168	6,0
10.000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

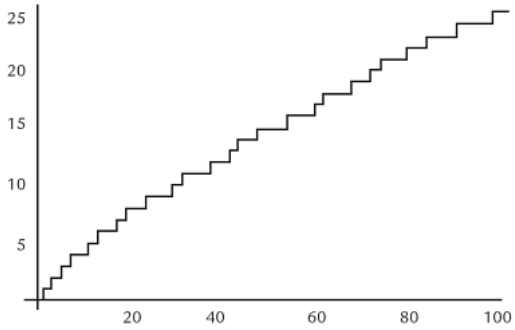
Fonte: adaptada de Peruzzo (2012, p. 70)

Note que, para x maior que 10.000, toda vez que acrescentamos um zero ao número x, na proporção de primos adiciona-se 2,3.

Peruzzo (2012) ressalta que com a análise dos dados, Gauss conjecturou que entre 1 e x, aproximadamente 1 em cada $ln(x)$ será um número primo.

Observe o gráfico de $\pi(x)$, contando a quantidade de primos de 1 até 100.

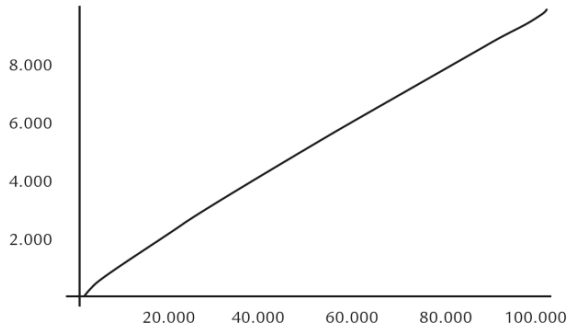
Figura 1 – Gráfico da quantidade de primos de 1 até 100.



Fonte: Du Sautoy (2007, p. 59)

Du Saltoy (2007) chama o gráfico acima de uma escada irregular, em que é difícil prever quando aparecerá um novo degrau. Porém ele mostra o mesmo resultado em uma escala maior, exibindo o número de primos até 100.000, chegando ao gráfico a seguir.

Figura 2 – Gráfico da quantidade de primos de 1 até 100.000.



Fonte: Du Sautoy (2007, p. 60)

Gauss percebeu que este gráfico tem o comportamento de uma função logarítmica. Peruzzo (2012, p.71) enaltece essa descoberta como um milagre da matemática: “O fato do gráfico ter um comportamento a princípio

bem regular, embora a posição dos números primos seja imprevisível, é um dos grandes milagres da matemática".

Gauss sabia que sua questão partia de um cálculo estimativo sobre a quantidade de números primos, mas não tinha provas e, por isso, demorou a divulgar suas descobertas. Este teorema fora provado em 1896 pelo francês J. Hadamard e pelo belga C. J. de la Vallee Poussim.

1.1.8 Dias atuais

Com a chegada dos computadores a busca pelos números primos se intensificou. Eves (2011) conta que em 1980 a revista *Crux mathematicorum* publicou uma tabela com todos os primos palindrômicos[1] de cinco dígitos, num total de 93, e todos os palindrômicos de sete dígitos, que são 668. O cálculo foi feito em um computador PDP-11/45 da Universidade de Waterloo e demorou pouco mais de um minuto.

O maior número primo conhecido até janeiro de 2016 possui mais de 22 milhões de dígitos: $2^{74207281} - 1$. Este é o 49º primo de Mersenne conhecido. A descoberta foi atribuída a Curtis Cooper que faz parte do *Great Internet Mersenne Prime Search* (GIMPS) que é um programa que interliga vários computadores voluntários na busca por números primos de Mersenne.

Ainda existem muitas questões não resolvidas com relação aos números primos. Uma delas é a conjectura de Goldbach que afirma: "todo número par maior que 2 pode ser escrito como um soma de dois primos". Já se comprovou esta hipótese para números na casa dos milhões, mas ainda não há uma resposta definitiva à conjectura de Goldbach.

Outra conjectura ainda não provada é a conjectura dos primos gêmeos que aponta para a existência de infinitos pares de primos da forma p e $p + 2$, como por exemplo, 3 e 5, 5 e 7, 11 e 13, entre outros.

Eves (2011) elenca outras questões ainda não resolvidas:

- Existem infinitos primos da forma $n^2 + 1$?
- Sempre encontramos um primo entre n^2 e $(n+1)^2$?
- Há infinitos primos de Fermat?

[1] Número que lidos da esquerda para a direita ou da direita para a esquerda representam o mesmo valor. Exemplo: 15851.

1.2 Números Primos – Parte Teórica

Os resultados apresentados nesta seção são baseados nas referências (Hefez, 2013), (Oliveira e Fernández, 2010) e (Lopes, 2015).

Denotaremos o conjunto dos números naturais por $\mathbb{N} = \{0, 1, 2, \dots\}$ e o conjunto dos números inteiros por $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ e admitiremos conhecidas as propriedades elementares da soma e produto nestes conjuntos.

1.2.1 Divisibilidade e Números Primos

Definição 1. Sejam dois números inteiros a e b. Dizemos que b divide a, e denotamos por $b|a$, se existe um inteiro c tal que $a = bc$. Podemos dizer também que b é um divisor ou um fator de a ou, ainda, que a é um múltiplo de b. Se b não for divisor de a, escreveremos $b \nmid a$.

Exemplo 1. $5|15$; $8|32$; $4|0$.
Por outro lado, $5 \nmid 7$ e $2 \nmid 3$.

Proposição 1. Sejam $a, b, c \in \mathbb{Z}$. Então

i) $1|a$; $a|a$ e $a|0$.

ii) se $a|b$ e $b|c$ então $a|c$.

Demonstração. i) Seguem das igualdades

$$a = 1.a,\ a = a.1 \text{ e } 0 = a.0,$$

respectivamente.

ii) Se $a|b$ e $b|c$ então existem inteiros q e p tais que

$$b = aq$$
$$c = bp$$

Substituindo o valor de b da primeira equação na segunda, obtemos

$$c = (aq)p = a(qp),$$

o que nos mostra que $a|c$. ■

Proposição 2. Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $a|c$ então $a|(b+c)$ e $a|(b-c)$.

.

Demonstração. Se $a|b$ e $a|c$ então existem inteiros q e p tais que

$$b = aq$$

$$c = ap.$$

Somando as equações obtemos

$$b + c = a(q + p).$$

Por outro lado, subtraindo a segunda equação da primeira obtemos

$$b - c = a(q - p).$$

Como $q + p$ e $q - p$ são ambos números inteiros, segue que $a|(b+c)$ e $a|(b-c)$, como queríamos. ■

Proposição 3. Sejam $a, b, c, d \in \mathbb{Z}$. Se $a|b$ e $c|d$, então $ac|bd$.

Demonstração. Se $a|b$ e $c|d$ então existem inteiros q e p tais que

$$b = aq$$

$$d = cp.$$

Portanto,

$$bd = (aq)(cp) = (ac)(qp).$$

Logo $ac|bd$. ■

Definição 2. Um número inteiro é dito *primo* se possuir exatamente dois divisores positivos, o 1 e ele mesmo. Os demais números que não são primos são chamados de *números compostos*.

O número 0 possui infinitos divisores, logo não é primo.

O número 1 possui apenas um divisor, ele mesmo, portanto também não é um número primo.

Exemplo 2. Os números 2, 3, 5, 7, 11 e 13 são primos e os números 4, 8, 15, 42 e 121 são compostos.

1.2.2 Divisão Euclidiana

Para demonstrar o Teorema da Divisão Euclidiana, enunciaremos uma importante propriedade dos números inteiros: o Princípio da Boa Ordenação.

Definição 3. Diremos que um subconjunto S de $\mathbb{Z}$ é *limitado inferiormente*, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. Diremos que $a \in S$ é um *menor elemento* de S se $a \leq x$ para todo $x \in S$.

Teorema 1 (Princípio da Boa Ordenação). Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Teorema 2 (Teorema da Divisão Euclidiana). Dados a *e* b números inteiros com a positivo, existem únicos inteiros q e r, tais que $b = aq + r$, $0 \leq r < a$.

Demonstração. Por simplicidade, suponhamos que b é positivo. Se $b < a$, basta tomar $q = 0$ e $r = b$. Se $b = a$, então tomamos $q = 1$ e $r = 0$. Assim, assumiremos que $b > a > 0$. Consideremos o conjunto

$$R = \{b - aq \in \mathbb{Z}; b - aq \geq 0\} \subseteq \mathbb{N}.$$

Note que o conjunto R é não vazio, pois $b - a \in R$, já que $b - a > 0$. Deste modo, pelo Princípio da Boa Ordenação, temos que R admite um menor elemento, que chamaremos de r. Obviamente $r = b - aq \geq 0$, para algum $q \geq 0$. Além disso, $r < a$ pois caso contrário teríamos

$$r = b - aq \geq a \Rightarrow b - a(q + 1) \geq 0.$$

Logo,

$$a > 0 \Rightarrow b - a(q + 1) < b - aq.$$

Das desigualdades acima segue que

$$0 \leq b - a(q + 1) < b - aq,$$

o que contradiz o fato de que $r = b - aq$ é o menor elemento não negativo de R.

Vamos provar agora a unicidade de r e q. Com efeito, suponhamos que existam também r_1 e q_1 tais que $b = aq_1 + r_1, 0 \leq r_1 < a$. Então resulta que

$$aq + r = aq_1 + r_1.$$

Logo,

$$(r - r_1) = (q_1 - q)a.$$

Sendo assim, $r - r_1$ é múltiplo de a. Mas, em virtude de $r < a$ e $r_1 < a$ segue que $|r - r_1| = |(q_1 - q)a| < |a|$, donde concluímos que $q = q_1$. ■

Observação: Note que no enunciado do Teorema 2, se $b < 0$ podemos proceder de maneira análoga, apenas tomando alguns cuidados. Podemos aplicar a prova feita para $-b > 0$ e caso o resto seja negativo, diminuímos o valor de q de forma que o resto fique positivo. Por exemplo, considere $b = -15$ e $a = 2$. Neste caso, teríamos $-15 = 2(-8) + 1$.

Os números q e r na definição acima são chamados, respectivamente, de *quociente* e *resto* da divisão de b por a.

Se $a|b$ então $r = 0$.

Exemplo 3. O quociente e o resto da divisão de 21 por 4 são $q = 5$ e $r = 1$, respectivamente.

Corolário 1. Dados inteiros a e b, com $b > 0$, existe um único número inteiro n, tal que $nb \leq a < (n + 1)b$.

Demonstração. Pelo Teorema da Divisão de Euclides, sabe-se que existem únicos inteiros q e r, com $0 \leq r < b$, tais que $a = bq + r$. Então, basta tomar $n = q$. ■

1.2.3 Máximo Divisor Comum

Definição 4. Sejam a e b números inteiros. O *máximo divisor comum* (mdc) entre a e b é o número inteiro positivo d que satisfaz as seguintes condições:

i) d é um divisor comum de a e b;

ii) se c é um divisor comum de a e b, então $c|d$, ou seja, d é o maior número natural que satisfaz a propriedade (i).

Neste caso, denotaremos o mdc entre a e b por $d = (a, b)$. Se $(a, b) = 1$, dizemos que a e b são primos entre si, ou ainda, que são relativamente primos.

Exemplo 4. O mdc entre 12 e 18 é 6. De fato, seja D_{12}, o conjunto de todos os divisores positivos de 12 e seja D_{18}, o conjunto de todos os divisores positivos de 18. Então $D_{12} = \{1, 2, 3, 4, 6, 12\}$ e $D_{18} = \{1, 2, 3, 6, 9, 18\}$. Logo o maior divisor comum entre 12 e 18 é o número 6.

Lema 1. Sejam a e b inteiros positivos e $t \in \mathbb{Z}$. Então

$$(a, b) = (a, b + at) = (a + bt, b).$$

Demonstração. Primeiramente vamos provar que $(a, b) = (a, a + bt)$. Seja $d = (a, b)$ e $d' = (a, b + at)$. Observando (a, b), temos que $d|a$ e $d|b$ então $d|a$, $d|at$ e $d|b$. Logo, $d|a$ e $d|b + at$. Assim, *d* é um divisor comum de a e $b + at$, e como d' é o maior divisor comum temos então $d' \geq d$. Agora vamos olhar para $(a, b + at)$. Temos que $d'|a$ e $d'|b + at$. Então $d'|a, d'|at$ e $d'|b + at$. Logo, $d'|a, d'|b + at - at$ e, portanto $d'|a$ e $d'|b$. Assim, d é um divisor comum de a e b, e como d é o maior divisor comum, temos então $d \geq d'$. Mas já provamos que $d' \geq d$, então $d = d'$, como queríamos. De forma análoga provamos a outra identidade. ■

A partir do Teorema da Divisão de Euclides podemos então escrever o seguinte Algoritmo de Euclides.

Algoritmo de Euclides (Método das Divisões Sucessivas)

Dados dois números inteiros positivos a e b, considere as divisões sucessivas a seguir, onde as letras q são quocientes e as letras r são restos.

$$a = q_o + r_0$$
$$b = q_1 r_0 + r_1$$
$$r_0 = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$

...

$$r_k = q_{k+1}r_{k+1} + r_{k+2}$$

$$r_{k+1} = q_{k+2}r_{k+2}$$

(observe que essas divisões sucessivas em algum momento vão acabar, pois do algoritmo da divisão temos $b > r_0 > r_1 > r_2 > \cdots$, e se a sequência de restos não acabasse em algum momento teríamos um resto negativo, o que é um absurdo).
Então $(a, b) = r_{k+2}$ é o ultimo resto não nulo das divisões sucessivas.

Através do conceito de divisibilidade, podemos introduzir a noção de congruência.

Definição 5. Seja um número natural m. Dizemos que dois números inteiros a e b são *congruentes* módulo m, se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, denotamos por $a \equiv b \bmod m$. Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b não são congruentes módulo m. Neste caso escrevemos $a \not\equiv b \bmod m$.

Exemplo 5. $32 \equiv 17 \bmod 3$, pois os restos das divisões de 32 e de 17 por 3 são iguais a 2.

Definição 6. Se $a, b \in \mathbb{Z}$, com $a \equiv b \bmod m$, então dizemos que b é um *resíduo* de a módulo m.

Definição 7. O conjunto $\{r_1, r_2, \dots, r_s\}$ é um *sistema reduzido de resíduos módulo* m se:

i) $(r_i, m) = 1, \ \forall\, i = 1, 2, \dots, s$;

ii) $r_i \not\equiv r_j \bmod m$ para $i \neq j$;

iii) Para cada $n \in \mathbb{Z}$, tal que $(n, m) = 1$, existe i tal que $n \equiv r_i \bmod m$.

Observação: Segue do Teorema da Divisão Euclidiana que se k inteiros $r_1, r_2, \dots, r_k$ formam um sistema completo de resíduos módulo m, então $k = m$.

Sistema completo de resíduos significa qualquer outro conjunto de n inteiros com nenhum par deles congruentes. Por exemplo, $\{0, 1, 2, 3\}$ é um sistema completo de resíduos módulo 4. Já $\{-5, 0, 6, 22\}$ não é um sistema completo, pois $22 \equiv 6 \bmod 4$.

A seguir, listaremos algumas propriedades básicas da Aritmética Modular.

Proposição 4. Sejam $a, b, c, d \in \mathbb{Z}$, e $m \in \mathbb{N}$, $m > 1$, tem-se que

i) $a \equiv a \bmod m$;

ii) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;

iii) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$;

iv) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$ e $ac \equiv bd \bmod m$;

v) Para todo $k \in \mathbb{N}$, se $a \equiv b \bmod m$, então $a^k \equiv b^k \bmod m$;

vi) $a + c \equiv b + c \bmod m$ se, e somente se, $a \equiv b \bmod m$;

vii) $ac \equiv bc \bmod m$ se, e somente se, $a \equiv b \; mod \; \frac{m}{(c,m)}$.

As demonstrações das propriedades anteriores estão disponíveis em (Hefez, 2013).

1.2.4 Teorema de Bézout

Teorema 3 (Teorema de Bézout). Dados a e b inteiros positivos, existem inteiros x e y tais que $ax + by = (a, b)$.

Demonstração. Considerando o método das divisões sucessivas acima mencionado, temos que

$$r_{k+2} = -q_{k+1}r_{k+1} + r_k \qquad \text{e} \qquad r_{k+1} = -q_k r_k + r_{k-1}.$$

Substituindo a segunda igualdade na primeira temos que

$$r_{k+2} = -q_{k+1}(-q_k r_k + r_{k-1}) + r_k = (q_{k+1}q_k + 1)r_k - q_{k+1}r_{k-1}.$$

Chamando $x_k = q_{k+1}q_k + 1$ e $y_k = -q_{k+1}$, temos x_k e y_k inteiros e

$$r_{k+2} = x_k r_k + y_k r_{k-1}.$$

Agora vamos observar $r_k = -q_{k-1}r_{k-1} + r_{k-2}$, de modo que, ao substituirmos r_k na equação acima obtemos

$$r_{k+2} = x_k(-q_{k-1}r_{k-1} + r_{k-2}) + y_k r_{k-1} = (-q_{k-1}x_k + y_k)r_{k-1} + x_k r_{k-2}.$$

Chamando $x_{k-1} = -q_{k-1}x_k + y_k$ e $y_{k-1} = x_k$, temos x_{k-1} e y_{k-1} inteiros e

$$r_{k+2} = x_{k-1}r_{k-1} + y_{k-1}r_{k-2}.$$

Continuando esse processo sucessivas vezes, chegaremos que existem inteiros x_1 e y_1 tais que $r_{k+2} = x_1 r_1 + y_1 r_0$.

Agora, sendo $r_1 = b - q_1 r_0$ e $r_0 = a - q_0 b$, substituindo r_1 e depois r_0, na última expressão, temos que

$$r_{k+2} = x_1(b - q_1 r_0) + y_1 r_0 = (y_1 - x_1 q_1)r_0 + x_1 b =$$

$$= (y_1 - x_1 q_1)(a - q_0 b) + x_1 b = a(y_1 - x_1 q_1) + b(-q_0 y_1 + x_1 q_0 q_1 + x_1).$$

Chamando $x = y_1 - x_1 q_1$ e $y = -q_0 y_1 + x_1 q_0 q_1 + x_1$, temos que x e y são inteiros e como $r_{k+2} = (a, b)$, segue que $(a, b) = ax + by$, mostrando assim a existência dos inteiros x e y. ■

Observação 1. Observe que é possível encontrar x e y, simplesmente encontrando x_k e y_k, em seguida x_{k-1} e y_{k-1} e assim sucessivamente.

Observação 2. Note que todo múltiplo de (a, b) pode ser escrito na forma $ax + by$. Com efeito, se $M = k(a, b)$ é um múltiplo de (a, b), então

$$M = k(ax + by) = a(kx) + b(ky).$$

Além disso, todos os números da forma $ax + by$, com x e y inteiros, são múltiplos de (a, b), já que a e b são múltiplos também.

Teorema 4. Seja n um inteiro positivo e seja a um inteiro tal que $(a, n) = 1$. Então, existe x inteiro tal que $ax \equiv 1 \bmod n$. Além disso, o valor de x é único módulo n.

Demonstração. Pelo Teorema de Bézout, existem inteiros x e y tais que

$$ax + ny = (a, n) = 1 \Rightarrow ax = 1 - ny \equiv 1 \bmod n,$$

pois $ny \equiv 0 \bmod n$.

Portanto, o valor de x do teorema de Bézout é um possível inverso multiplicativo, mostrando que inversos multiplicativos de fato existem. Para mostrar que x é único módulo n, basta provar que $ax \equiv ax' \bmod n$ implica

$x \equiv x' \bmod n$. Isso decorre de maneira direta do fato de que podemos “cortar” termos primos com o módulo. Observe que

$$ax \equiv ax' \bmod n \Rightarrow n|a(x-x').$$

Ora, pelo Teorema de Bézout, existem inteiros y e z tais que $ay + nz = 1$, e então $ay = 1 - nz$. Daí, como

$$n|a(x-x') \Rightarrow n|ay(x-x') \Rightarrow n|(1-nz)(x-x') \Rightarrow n|x-x',$$

provando que $x \equiv x' \bmod n$, como queríamos.

Observação: Não vale a recíproca do Teorema de Bézout.

Proposição 5. Dados $d, \lambda \in \mathbb{N}$ e $a, b, c \in \mathbb{Z}$. Então as seguintes afirmações são verdadeiras:

i) Se $d|a$ e $d|b$, então $d|(a,b)$.

ii) (a,b) é o menor valor positivo de $ax + by$, onde x e y percorrem todos os números inteiros.

iii) $(\lambda a, \lambda b) = \lambda(a,b)$.

iv) Se $d|a$ e $d|b$, então $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a,b)$. Consequentemente,

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

v) Se $(a,c) = (b,c) = 1$, então $(ab,c) = 1$.

vi) Se $c|ab$ e $(b,c) = 1$, então $c|a$.

Demonstração. i) Segue da definição de mdc.

ii) Segue da demonstração dada no Teorema de Bézout.

iii) Observe que $(\lambda a)x + (\lambda b)y = \lambda(ax + by)$, com $x, y \in \mathbb{Z}$. Usando o item (i) e o fato de λ ser positivo, da igualdade acima segue que

$$(\lambda a, \lambda b) = \min\{(\lambda a)x + (\lambda b)y > 0;\ x, y \in \mathbb{Z}\} = \lambda \min\{ax + by;\ x, y \in \mathbb{Z}\} = \lambda(a,b).$$

iv) Segue diretamente do item (ii), observando que

$$(a,b) = \left(d\frac{a}{d}, d\frac{b}{d}\right) = d\left(\frac{a}{d}, \frac{b}{d}\right).$$

v) De $(a,c) = (b,c) = 1$, segue que existem inteiros x_j e y_j, com $j = 1,2$, tais que

$$ax_1 + cy_1 = 1 \text{ e } bx_2 + cy_2 = 1.$$

Multiplicando as equações acima temos

$$(x_1x_2)ab + (ax_1y_2 + y_1x_2 + cy_1y_2)c = 1.$$

Usando a igualdade acima e o item (ii) concluímos que $(ab, c) = 1$.

vi) Temos que existem inteiros x_0 e y_0 tais que

$$bx_0 + cy_0 = 1.$$

Multiplicando a igualdade acima por a obtemos

$$abx_0 + acy_0 = a.$$

Por outro lado, $ab = cq$ para algum inteiro q. Usando esta condição na última igualdade temos que

$$cqx_0 + acy_0 = c(qx_0 + ay_0) = a,$$

Logo $c|a$. ■

1.2.5 Aplicação do Teorema de Bézout

Agora vamos dar uma breve pausa nas contas e ver uma história baseada no texto de (Lopes, 2015), que por incrível que pareça, tem tudo a ver com o Teorema de Bézout.

Considere um jogo de rúgbi adaptado, que chamaremos de rúgbi bezoutiano, entre duas equipes, na qual as formas de pontuação são cinco pontos ou três pontos dependendo do lugar da quadra de onde os jogadores fizerem os pontos.

Podemos usar o Teorema de Bézout para saber, por exemplo, que não pode ocorrer o placar 7 a 1, pois ambos os números 7 e 1 não podem ser escritos na forma $3x + 5y$, com x e y inteiros não negativos. Mas, como $(3,5) = 1$, pelo Teorema de Bézout todo inteiro pode ser escrito na forma $3x + 5y$, inclusive o 1 e o 7, mas neste caso as soluções x e y não seriam inteiros não negativos!

De um modo mais geral podemos fazer a seguinte pergunta: “inspirados pelo problema do jogo de rúgbi bezoutiano, dados a e b inteiros positivos com $(a, b) = 1$ e um inteiro não negativo n, é possível escrever $n = ax + by$, com x e y inteiros não negativos? A resposta é: depende do valor de n. Mas como é essa dependência? Para responder a isso, recorreremos ao Teorema de Bézout.

Inicialmente faremos uma pequena observação: considere x_0, y_0, x_1 e y_1 inteiros, de modo que $n = ax_0 + by_0 = ax_1 + by_1$ (eles existem pela observação 2, pois $(a, b) = 1$). Sabemos que

$$b|0 \Rightarrow b|ax_0 + by_0 - (ax_1 + by_1) \Rightarrow b|a(x_0 - x_1) + b(y_0 - y_1) \Rightarrow$$
$$b|a(x_0 - x_1) \Rightarrow b|x_0 - x_1.$$

Como $b|x_0 - x_1$, temos que $x_0 \equiv x_1 \bmod b$. De forma análoga chegamos que $y_0 \equiv y_1 \bmod a$.

Outra observação útil é que, ao escrevermos

$$n = ax_0 + by_0 = a(x_0 + kb) + b(y_0 - ka),$$

e variarmos o valor de k nos inteiros, percebemos que todo número que deixa o mesmo resto que x_0 na divisão por b pode assumir o lugar de x na relação de Bézout, $n = ax + by$, e todo número que deixa o mesmo resto que y_0 na divisão por a pode assumir o lugar de y na equação. Assim, notamos que, embora a equação $n = ax + by$ tenha infinitas soluções para x e y, o resto de x por b e o resto de y por a são únicos.

Agora, finalmente, podemos responder nossa pergunta. Considere $n = ax_0 + by_0$, com $x_0, y_0 \in \mathbb{Z}$ e seja r o resto de x por b. Vamos escrever $n = ar + by_1$. Se $y_1 \geq 0$, n pode ser escrito na forma desejada. Se $y_1 < 0$, n não pode ser escrito na forma desejada, pois caso $n = ar + by_1 = ax + by$, com $x, y \geq 0$, e sabendo que x deixa resto r na divisão por b, temos que $x \geq r$, donde

$$ar - ax \leq 0 \Rightarrow by - by_1 \leq 0 \Rightarrow y_1 \leq y < 0 \Rightarrow y_1 \leq 0,$$

o que é um contradição.

Portanto, no nosso rúgbi bezoutiano, é impossível obter 1, 2, 4 e 7 pontos, pois:

$$1 = 3(2) + 5(-1)$$
$$2 = 3(4) + 5(-2)$$
$$4 = 3(3) + 5(-1)$$
$$7 = 3(4) + 5(-1).$$

Por outro lado, conseguimos obter 3, 5, 6 e 8 pontos, pois

$$3 = 3(1) + 5(0)$$
$$5 = 3(0) + 5(1)$$

$$6 = 3(2) + 5(0)$$
$$8 = 3(1) + 5(1).$$

Geralmente, escreveremos $n = ax + by$ com x e y inteiros e $0 \leq x \leq b - 1$, pois é útil tomarmos a primeira variável como sendo o resto da divisão por b, de modo a podermos analisar se n se encaixa ou não no que queremos.

1.2.6 Mínimo Múltiplo Comum

Definição 8. Sejam a *e* b números inteiros diferentes de zero. O *mínimo múltiplo comum* (mmc) entre a e b é o número inteiro positivo m que satisfaz as seguintes condições:

i) $a|m$ e $b|m$.

ii) Se c é um múltiplo comum de a e b, então $m|c$.

Neste caso, denotaremos o *mmc* entre a e b por $m = [a, b]$.

Exemplo 6. 24 é um múltiplo comum de 3 e 4, mas não é o mmc desses números. O número 12 é o mmc entre 3 e 4.

Proposição 6. Sejam $a, b, c, \lambda \in \mathbb{Z}$. Então as seguintes afirmações são verdadeiras:

i) Se c é múltiplo comum de a e b, então $[a, b]|c$.

ii) $[\lambda a, \lambda b] = \lambda[a, b]$.

iii) $|ab| = [a, b].(a, b)$.

Demonstração. Começaremos com a prova de (*i*). Dividindo c por $[a, b]$ temos $c = [a, b]q + r$, com $a \leq r < [a, b]$. Basta mostrarmos que $r = 0$. Suponhamos, por absurdo, que $0 < r < [a, b]$. Note que a e b dividem c e $[a, b]$. Logo, pela Proposição 2 e pela igualdade $c = [a, b]q + r$, temos que a e b também dividem r, ou seja, r é múltiplo comum de a e b e não pode ser menor que $[a, b]$, o que contradiz nossa suposição.

Agora vamos provar o item (*ii*). Note que $\lambda[a, b]$ é múltiplo comum de λa e λb, então pelo item (*i*) vale que $[\lambda a, \lambda b] \leq \lambda[a, b]$. Por outro lado, $[\lambda a, \lambda b] = q_1 \lambda a =$

$q_2\lambda b$, para q_1 e q_2 inteiros quaisquer. Logo, $\frac{[\lambda a,\lambda b]}{\lambda}$ é um múltiplo comum de a e b. Portanto,

$$[a,b] \leq \frac{[\lambda a,\lambda b]}{\lambda} \Leftrightarrow \lambda[a,b] \leq [\lambda a,\lambda b].$$

Como já mostramos que $[\lambda a,\lambda b] \leq \lambda[a,b]$, concluímos que $[\lambda a,\lambda b] = \lambda[a,b]$.

Vamos provar o item (*iii*). Se $a = 0$ ou $b = 0$ a igualdade é trivialmente satisfeita. Vamos então supor, sem perda de generalidade, que a e b são positivos devido às igualdades $[a,b] = [a,-b] = [-a,b] = [-a,-b]$. Seja $m = \frac{ab}{(a,b)}$. Como $m = a\frac{b}{(a,b)} = b\frac{a}{(a,b)}$, temos que $a|m$ e $b|m$. Então m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b. Logo, $c = na = n'b$ e daí segue que

$$n\frac{a}{(a,b)} = n'\frac{b}{(a,b)}.$$

Como, pelo item (i*v*) da Proposição 5, $\frac{a}{(a,b)}$ e $\frac{b}{(a,b)}$ são primos entre si, segue-se do item (*vi*) da Proposição 5, que $\frac{a}{(a,b)}$ divide n' , e, portanto, $m = \frac{a}{(a,b)}b$ divide $n'b$ que, é igual a c. ■

1.2.7 Outras propriedades dos números primos

Proposição 7 (Lema de Euclides). Sejam a, b e p inteiros, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração. Seja p um número primo tal que $p \nmid a$ então

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

Pelo item (*vi*) da Proposição 5, temos que $p|b$. ■

Corolário 2. Sejam $p, p_1, p_2, p_3, \ldots p_n$ números primos. Se $p|p_1p_2p_3 \ldots p_n$, então $p = p_i$, para algum $i = 1, \ldots, n$.

Demonstração. Vamos demonstrar por indução sobre n.

Para $n = 1$. Se $p|p_1$, é trivial que $p = p_1$.

Vamos supor a afirmação válida para $n = k$. Assim se $p|p_1p_2p_3 \ldots p_k$, então $p = p_i$, para algum $i = 1, \ldots, k$.

Vamos mostrar que o resultado é válido para $n = k + 1$.

De fato, se $p|p_1p_2p_3 \dots p_kp_{k+1}$ então pelo Lema de Euclides $p|p_1p_2p_3 \dots p_k$ ou $p|p_{k+1}$. Se $p|p_1p_2p_3 \dots p_k$, pela hipótese de indução temos que $p = p_i$ para algum $i = 1, \dots, k$. Se $p|p_{k+1}$ então $p = p_{k+1}$. Assim a afirmação é válida também para $n = k + 1$. Logo, pelo princípio de indução, a afirmação é verdadeira para todo n inteiro maior ou igual a 1. ■

Teorema 5 (Teorema Fundamental da Aritmética). Todo número natural n maior que 1 pode ser escrito de forma única (a menos da ordem de seus fatores) como um produto $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$, onde $m \geq 1$ e α_i são números naturais, e p_i é primo com $1 \leq i \leq m$.

Demonstração. Sejam n um inteiro maior que 1. Seja p_1 seu menor divisor primo. Tem-se $n = p_1\beta_1,\ 1 \leq \beta_1 < n$. Se $\beta_1 = 1$, então $n = p_1$ e a obtemos a fatoração desejada. Caso contrário, denotamos por p_2 o menor divisor primo de β_1 e tem-se que $n = p_1p_2\beta_2,\ 1 \leq \beta_2 < \beta_1$. Se $\beta_2 = 1$, então $n = p_1p_2$ e obtemos novamente a fatoração desejada. Caso contrário, denotamos por p_3 o menor divisor primo de β_2 e tem-se que $n = p_1p_2p_3\beta_3,\ 1 \leq \beta_3 < \beta_2$. Continuando este processo sucessivamente obtemos uma sequência estritamente decrescente de números naturais β_n, ou seja,

$$n > \beta_1 > \beta_2 > \beta_3 > \cdots > \beta_n > \beta_{n+1} > \cdots \geq 1.$$

Então, pelo princípio da boa ordenação, só pode existir um quantidade finita de índices n tais que $\beta_n > 1$ e, consequentemente, $\beta_{n+1} = 1$, de onde segue que $n = p_1p_2 \dots p_n$. Note que os p_i podem ser repetidos, resultando na representação desejada $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$.

Vamos provar agora a unicidade dessa fatoração. Vamos supor que existam duas fatorações

$${p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m} = n = {q_1}^{\beta_1}{q_2}^{\beta_2} \dots {q_s}^{\beta_s}.$$

Cada p_i divide algum q_j. Como ambos são primos, temos que $p_i = q_j$. Como os $p_i's$ e os $q_j's$ são diferentes dois a dois e organizados em ordem crescente, temos $m = s$, reduzindo a igualdade à ${p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m} = {p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_m}^{\beta_m}$. Suponha agora que α_1 seja diferente de β_1 e sem perda de generalidade, vamos supor que $\alpha_1 < \beta_1$. Logo ${p_2}^{\alpha_2} \dots {p_m}^{\alpha_m} = {p_1}^{\beta_1-\alpha_1}{p_2}^{\beta_2} \dots {p_m}^{\beta_m}$. E como

$\beta_1 - \alpha_1 > 0$ então pela Proposição 7 temos que p_1 divide algum p_j, com $j > 1$, o que é impossível. Logo, $\alpha_1 = \beta_1$. De forma análoga provamos que $\alpha_i = \beta_i$, com $i = 2, \dots, n$. ■

Proposição 8. Considere o número natural $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$. Se n' é um divisor positivo de n, então $n' = {p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_m}^{\beta_m}$, com $0 \leq \beta_i \leq \alpha_i$, para $i = 1,2, \dots, m$.

Demonstração. Seja n' um divisor positivo de n e seja p^{β} a potência de um primo p que está na decomposição em fatores primos de n. Como $p^{\beta} | n$, segue que p^{β} divide algum ${p_i}^{\alpha_i}$, por ser primo como os demais ${p_j}^{\alpha_j}$ e, consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. ■

Teorema 6. Sejam $a = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_m}^{\alpha_m}$ e $b = {p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_m}^{\beta_m}$. Tome os números, $\gamma_i = \min\{\alpha_i, \beta_i\}$ e $\delta_i = \max\{\alpha_i, \beta_i\}$, para $i = 1,2, \dots, m$. Temos que $(a, b) = {p_1}^{\gamma_1}{p_2}^{\gamma_2} \dots {p_m}^{\gamma_m}$ e $[a, b] = {p_1}^{\delta_1}{p_2}^{\delta_2} \dots {p_m}^{\delta_m}$.

Demonstração. Pela Proposição 8, note que ${p_1}^{\gamma_1}{p_2}^{\gamma_2} \dots {p_m}^{\gamma_m}$ é um divisor comum de a e b. Tome outro divisor comum de a e b, o qual chamaremos de c. Então $c = {p_1}^{\varepsilon_1}{p_2}^{\varepsilon_2} \dots {p_r}^{\varepsilon_r}$, onde $\varepsilon_i \leq \min\{\alpha_i, \beta_i\}$ e, portanto, $c | {p_1}^{\gamma_1}{p_2}^{\gamma_2} \dots {p_m}^{\gamma_m}$. Do mesmo modo prova-se a afirmação sobre o *mmc*. ■

Teorema 7. Existem infinitos números primos.

Demonstração. Vamos supor que exista um número finito de números primos, digamos $p_1, p_2, \dots, p_k$. Consideremos o número natural $n = p_1 p_2 \dots p_k + 1$.
Seja q o menor divisor primo de n. Obviamente q não coincide com nenhum dos $p_i's$, $1 \leq i \leq k$, pois caso contrário, como ele divide n, também deveria dividir 1, o que é impossível. Assim, temos uma contradição à hipótese de que a quantidade de números primos é finita. ■

Usando o Teorema 3 podemos demonstrar os seguintes teoremas extremamente úteis em Teoria dos Números.

Teorema 8 (Teorema de Wilson). Seja p um número primo. Então

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

Teorema 9 (Pequeno Teorema de Fermat). Seja p um primo, n natural e a inteiro. Então $a^p \equiv a \bmod p$.

Uma outra versão do Pequeno Teorema de Fermat está enunciada a seguir.

Teorema 10 (Pequeno Teorema de Fermat – Segunda Versão). Se p é um número primo e se a é um número inteiro não divisível por p, tem-se que

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

Uma prova completa destes teoremas pode ser encontrada em (Hefez, 2013).

Aplicação do Pequeno Teorema de Fermat

Encontre o resto da divisão de $2^{1.000.000}$ por 17.

Temos que 17 é primo e não divide 2, então pelo Pequeno Teorema de Fermat $2^{16} \equiv 1 \bmod 17$. Mas $1.000.000 = 6250 \times 16$. Portanto,

$$2^{1.000.000} = [(2^{16})^{6250}] \equiv 1^{6250} \bmod 17 \equiv 1 \bmod 17.$$

Assim, temos pelo Pequeno Teorema de Fermat que o resto divisão de $2^{1.000.000}$ por 17 é 1.

1.2.8 Função de Euler

Definição 9. A função $\phi(n)$ de Euler é definida como sendo a quantidade de inteiros positivos que não excedem um inteiro positivo n, que são relativamente primos com n.

A tabela a seguir apresenta valores de $\phi(n)$ para $1 \leq n \leq 10$.

Tabela 2 – Valores de $\boldsymbol{\phi(n)}$ para $\mathbf{1 \leq n \leq 10}$.

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Fonte: autora

Proposição 9. Se $p > 1$, então $\phi(p) = p - 1$ se, e somente se, p for primo.

Demonstração. $\Rightarrow$) Se $\phi(p) = p - 1$, então p é relativamente primo com $p - 1$ números inteiros positivos, todos menores que o próprio p. Os únicos inteiros positivos que satisfazem essa condição são $1, 2, \ldots, p - 1$, que correspondem a todos os inteiros positivos menores que p. Então nenhum desses números dividem p, logo p é primo.
$\Leftarrow$) De fato, se p é primo, então os inteiros positivos, que não excedem p, que são relativamente primos com p são $1, 2, \ldots, p - 1$ e então $\phi(p) = p - 1$. ■

Teorema 11 (Teorema de Euler). Sejam m e a inteiros, com $m > 1$ e $(a, m) = 1$, então $a^{\phi(m)} \equiv 1 \bmod m$.

Demonstração. Seja $r_1, r_2, \ldots, r_{\phi(m)}$ um sistema reduzido módulo m. Não é difícil ver que, como $(a, m) = 1$ então também $ar_1, ar_2, \ldots, ar_{\phi(m)}$ forma um sistema reduzido módulo m. Usando propriedades da Aritmética Modular, segue que

$$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} = (ar_1)(ar_2) \ldots \left(ar_{\phi(m)}\right) \equiv r_1 r_2 \ldots r_{\phi(m)} \bmod m.$$

Como $\left(r_1 r_2 \ldots r_{\phi(m)}, m\right) = 1$, podemos concluir (novamente usando propriedades da Aritmética Modular) que $a^{\phi(m)} \equiv 1 \bmod m$. ■

Um resultado importante da função de Euler é dado a seguir. Tal proposição não será demonstrada nesse trabalho. Uma prova completa poderá ser encontrada em (Hefez, 2013).

Proposição 10. Sejam m e m' naturais tais que $(m, m') = 1$. Então

$$\phi(mm') = \phi(m)\phi(m').$$

Aplicação do Teorema de Euler

Encontre o resto da divisão de 3^{100} por 34.

Pela Proposição 9, temos que

$$\phi(34) = \phi(2)\phi(17) = (2-1)(17-1) = 16.$$

Então pelo Teorema de Euler $3^{16} \equiv 1 \bmod 34$. Assim

$$3^{100} = ((3^{16})^6)3^4 \equiv (1^6)3^4 \bmod 34 \Rightarrow 3^{100} \equiv 3^4 = 81 \equiv 13 \bmod 34.$$

Portanto o resto da divisão de 3^{100} por 34 é 13.

1.3 Números Primos – Aplicações na Criptografia

O nome criptografia vem do grego kryptos que significa "secreto" e grafos que significa "escrita", ou seja, criptografia é a arte de escrever de maneira secreta. Peruzzo (2012) relata que desde os tempos antigos o homem escrevia em linguagem criptografada como, por exemplo, trocando uma letra por outra, para evitar que pessoas indesejadas pudessem ler tal mensagem. Porém as mensagens criptografadas dessa forma eram facilmente decifradas, com uma análise de um número maior de informações. Peruzzo (2012 p.118) explica

> "Para poder escrever numa linguagem criptografada necessita-se de uma criptografia. Para decifrar a mensagem criptografada necessita-se de uma chave criptográfica. Quanto mais segura essa chave, mais difícil a quebra do código. Isso tudo é decorrência da luta intelectual contínua entre criptógrafos (criadores de códigos) e criptoanalistas (quebradores de códigos). Uma chave criptográfica é uma informação restrita que controla toda a operação dos algoritmos de criptografia. No processo de codificação é a chave quem dita a transformação do texto original em texto criptografado, e na decodificação é ela quem faz a transformação do texto criptografado no texto original."

Foi a partir da primeira guerra mundial que a criptografia teve avanços significativos. Com o avanço da tecnologia e a chegada dos computadores e da internet, tornou-se mais importante ainda a troca de informações privadas com segurança.

A dificuldade de se encontrar os divisores primos de números muito grandes faz dos números primos uma poderosa ferramenta de criptografia.

Ribenboim (2014) destaca que o grande progresso em criptografia veio com a criação dos cripto-sistemas de chave pública, que tem como principais características sua simplicidade, sua chave pública e a extrema dificuldade em violar o código.

Esse sistema de codificação foi proposto por Whitfield Diffie e Martin Hellman em 1976. Peruzzo (2012, p. 105) descreve o seu funcionamento:

> "Nesse sistema fórmulas matemáticas permitem que cada usuário tenha um par de chaves de criptografia, matematicamente relacionadas, sendo uma privada e a outra pública. O nome chave pública deve-se ao fato de que, ao usá-lo, uma pessoa pode revelar abertamente o modo como a outra pessoa que pretenda enviar-lhe uma mensagem secreta deverá codificá-la. Dessa forma, embora qualquer pessoa possa codificar uma mensagem para enviar à primeira, só esta a pode decodificar. Consequentemente, torna-se completamente desnecessário a cada par de utilizadores trocar e guardar a mesma chave, antes de tomarem a decisão de efetuar qualquer comunicação. Cada receptor possui o seu próprio segredo de decodificação e só ele tem necessidade de protege-lo."

A criptografia RSA é o método mais utilizado no mundo atualmente. A maioria das transações efetuadas pela internet, principalmente as transações bancárias, são protegidas pela criptografia RSA. Ronald Rivest, Adi Shamir e Leonard Adleman a desenvolveram em 1978, inspirados no trabalho de Diffie e Hellman.

Uma referência para o método RSA está em (Coutinho, 2000).

A seguir, faremos um breve resumo do funcionamento da criptografia RSA de acordo com Peruzzo (2012) .

Para gerar as chaves escolhem-se dois números primos, p e q, da ordem de no mínimo 10^{100} cada. Calculamos o produto n de p e q. Em seguida calculamos a função de Euler $\phi(n) = (p-1)(q-1)$. Escolhemos um número inteiro D com $1 < D < \phi(n)$, de modo que D e $\phi(n)$ sejam

relativamente primos. Calcula-se E, de modo que $ED \equiv 1(mod\ \phi(n))$. Assim, temos que a chave pública é o par de números n e D e a chave privada é o par n e E.

É preciso que se transforme a mensagem composta de palavras em números. Para transformar uma mensagem cifrada usando a chave pública do destinatário (n e D), basta fazer: $C \equiv M^D(mod\ n)$.

Para recuperar a mensagem M da mensagem cifrada C usamos a respectiva chave privada do receptor (n e E) fazendo:

$$M \equiv C^E(mod\ n).$$

O sucesso da criptografia está na ineficiência dos métodos de fatoração conhecidos, já que os números envolvidos são muito grandes e o tempo gasto para fatorá-los é astronômico, mesmo com o uso de computadores.

Capítulo 2

APLICATIVOS PARA SMARTPHONES E TABLETS

Neste capítulo descreveremos os aplicativos (apps) sugeridos para a realização das atividades deste trabalho. Acompanhando o título de cada aplicativo consta entre parênteses o seu desenvolvedor.

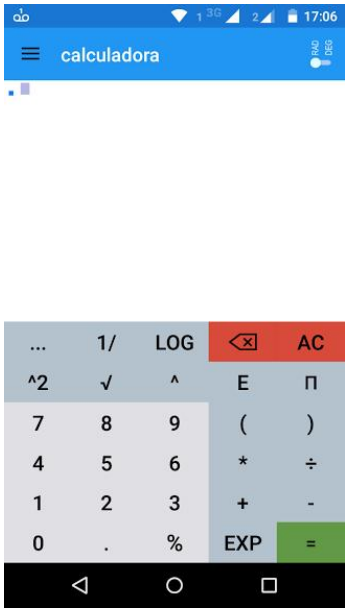
2.1 Mathematics (daboApps)

Valor: Gratuito
Plataforma: Android

O “Mathematics” é um aplicativo que possui várias ferramentas matemáticas, entre elas calculadora e conversor de unidades de medida. É capaz de resolver equações (linear, quadrática, cúbica); encontrar a função (linear, polinomial, racional, exponencial) dadas as raízes, pontos ou extremos; derivar; integrar; trabalhar com matrizes e vetores; calcular dados estatísticos (média, desvio padrão, distribuição normal e binomial, etc.); calcular combinação e permutação; trabalhar com sistemas numéricos alternativos, como o binário; fazer cálculos com números complexos; calcular congruência módulo *m*; decomposição do número em fatores primos, exibindo máximo divisor comum, mínimo múltiplo comum, identidade de Bézout e função de Euler; entre outros.

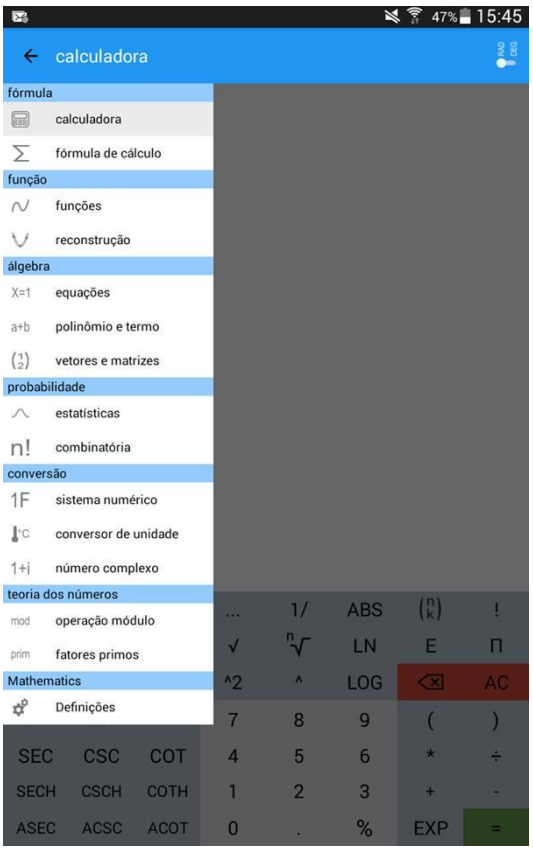
Segue uma imagem da tela inicial do aplicativo, exibindo a ferramenta calculadora, capturada por um smartphone Android e em seguida imagem do menu do aplicativo capturada por um tablet Android.

Figura 3 – Tela inicial do aplicativo “Mathematics”.



Fonte: autora

Figura 4 – Menu do aplicativo “Mathematics”.



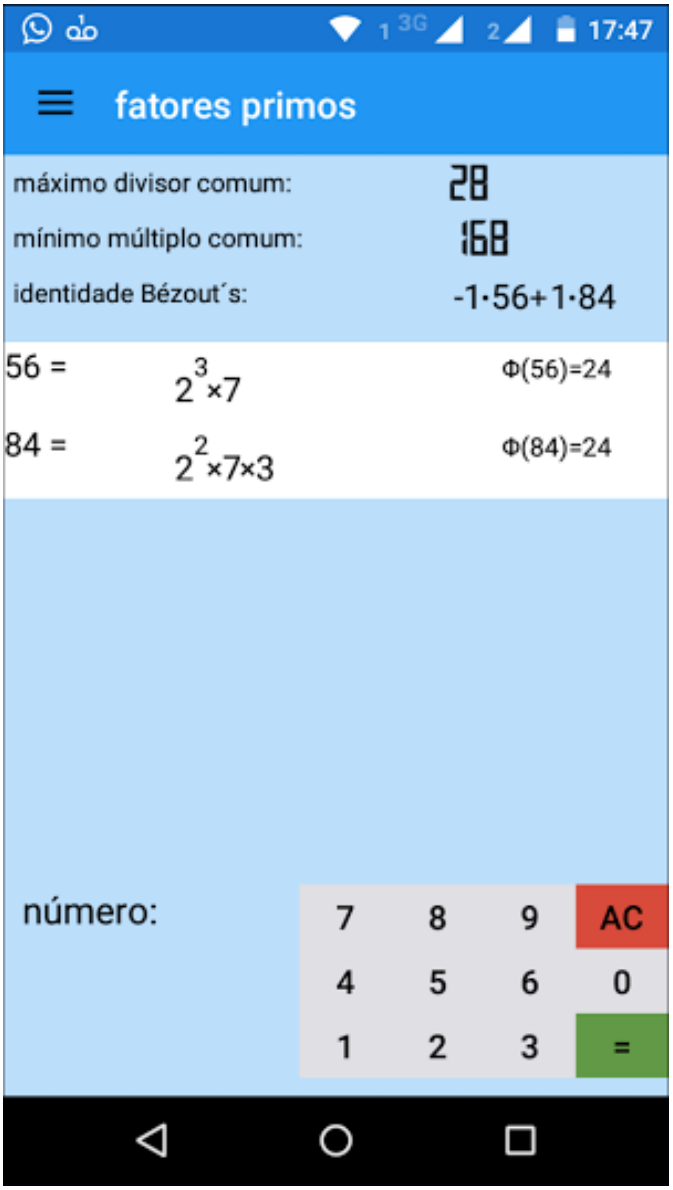
Fonte: autora

Neste trabalho utilizaremos a ferramenta “fatores primos”, que exibe a fatoração completa em fatores primos de qualquer número e a função de Euler.

Ao incluir um par de números, o aplicativo mostra o mínimo múltiplo comum e o máximo divisor comum entre eles e a identidade de Bezout.

Com 3 ou mais números, o aplicativo deixa de exibir a identidade de Bezout, porém calcula o mmc e mdc entre todos os números dados.

Figura 5 – Ferramenta “fatores primos” do app “Mathematics” incluídos os números 56 e 84.



Fonte: autora

2.2 Fatoração Prime (Tastesoft)

Valor: Gratuito

Plataforma: Android

O “Fatoração Prime” é um aplicativo simples que realiza a fatoração de qualquer número com no máximo 18 dígitos em fatores primos.

A única vantagem do Fatoração Prime para o Mathematics é a quantidade de dígitos suportada: 18 do Fatoração Prime contra 12 do Mathematics.

Segue uma imagem do aplicativo capturada por um smartphone Android.

Figura 6 – Interface do aplicativo “Fatoração Prime”.

Fonte: autora

Note que a tela apresenta a fatoração do número 98 e do número 544.659.834.846.868.386.

2.3 Factors (Fluocode)

Valor: Gratuito

Plataforma: Android e IOS

O “Factors” é um aplicativo utilizado para obter o mínimo múltiplo comum e máximo divisor comum entre os números inseridos. O mmc e o mdc são apresentados também na sua forma fatorada.

Ao inserir um número primo ele aparece em uma caixa amarela. Se inserir um número composto, ele aparecerá em uma caixa azul.

Segue a imagem capturada por um iPad da interface deste aplicativo, com a inclusão dos números 54, 13 e 88.

Figura 7 – Interface do aplicativo “Factors”.

Fonte: autora

Vale ressaltar o significado das siglas em inglês GCM (greatest common divisor) e LCD (least common multiple) que são, respectivamente, em português o MDC (máximo divisor comum) e o MMC (mínimo múltiplo comum).

2.4 Factorizer, numbers to factors (Fernando Fernandez)

Valor: Gratuito

Plataforma: IOS

O “Factorizer, numbers to factors” é um aplicativo simples capaz de fatorar um número em fatores primos e também simplificar frações.

É uma opção para plataforma IOS.

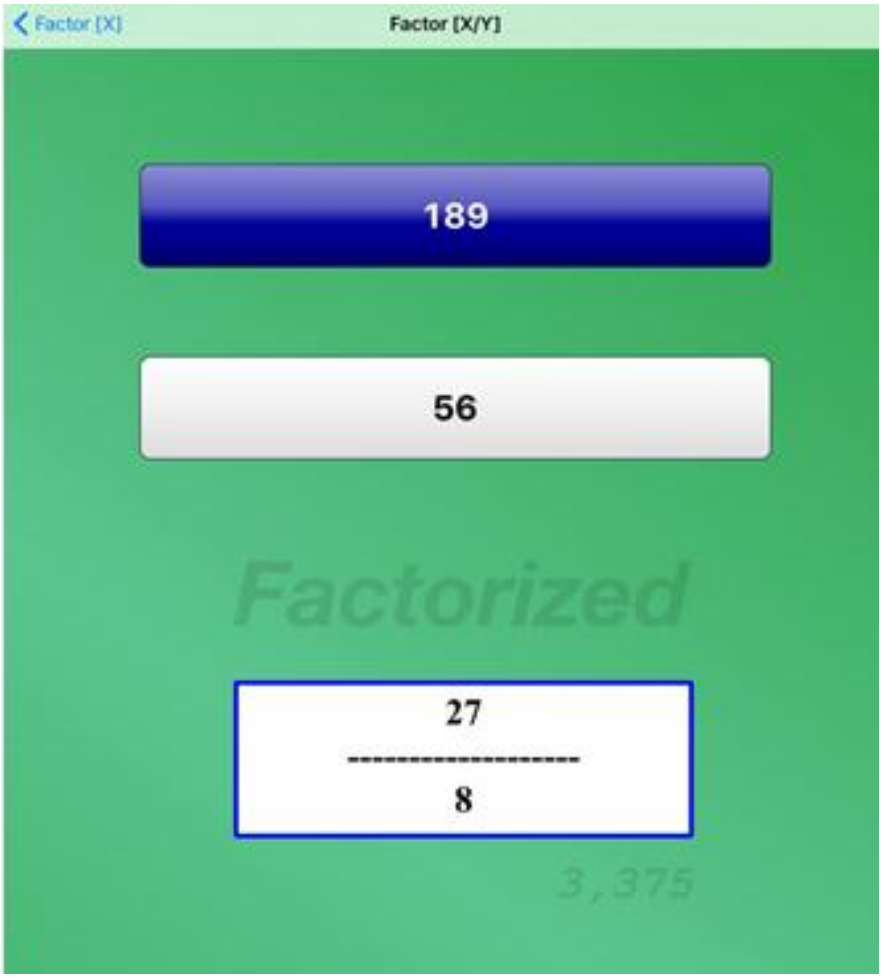
Na figura 8 o aplicativo apresenta a decomposição em fatores primos do número 126 e na figura 9 o aplicativo mostra a fração irredutível equivalente à fração $\frac{189}{56}$.

Seguem imagens das interfaces do aplicativo capturadas por um iPad.

Figura 8 – Interface do aplicativo “Factorizer, numbers to factors”- função fatoração em primos.

Fonte: autora

Figura 9 – Interface do app “Factorizer, numbers to factors”- função simplificação de fração.



Fonte: autora

2.5 PrimeShooter (EnukeSoftware)

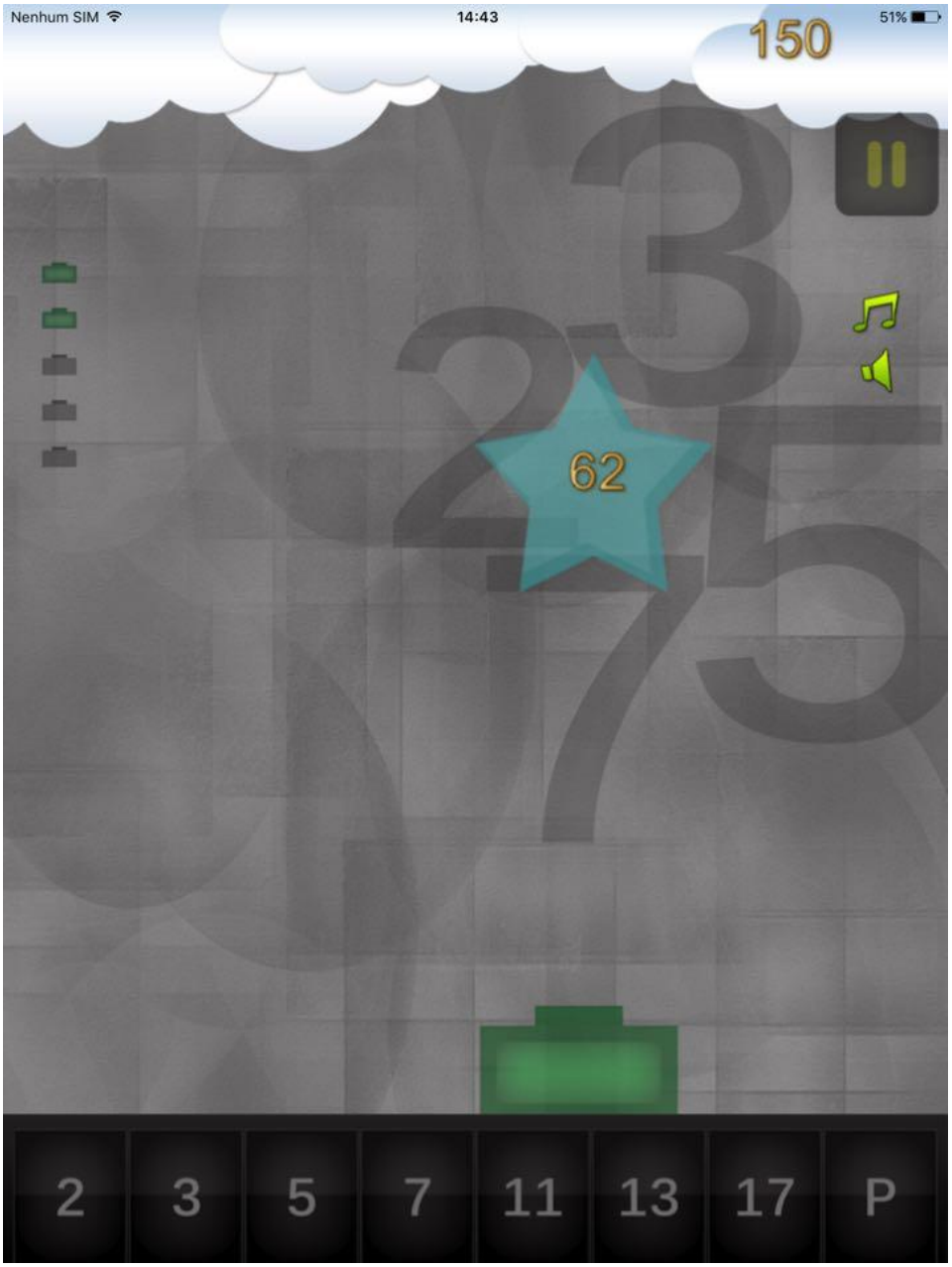
Valor: Gratuito
Plataforma: IOS

O “PrimeShooter” é um aplicativo que possui um jogo interativo e envolvente para treinar fatoração e números primos.

Na parte inferior da tela são listados os números primos. Caem da tela polígonos contendo números a serem fatorados. Assim que o número começa a cair o objetivo é atirar os primos que são múltiplos dele até fatorá-lo por completo.

Segue uma imagem da interface do aplicativo capturada por um iPad.

Figura 10 – Interface do aplicativo “PrimeShooter”.



Fonte: autora

Note que a figura 10 mostra o número 62. Antes que a estrela contendo o número 62 chegue no bloco verde, o jogador deve atirar o número 2, fazendo com que o 62 se transforme em 31 (que é o resultado da divisão de 62 por 2), e em seguida, como o 31 é um número primo, deve-se clicar no *P*. Feito isso, um novo número começa a rolar pela tela.

2.6 Factors! (45454 Studios)

Valor: Gratuito

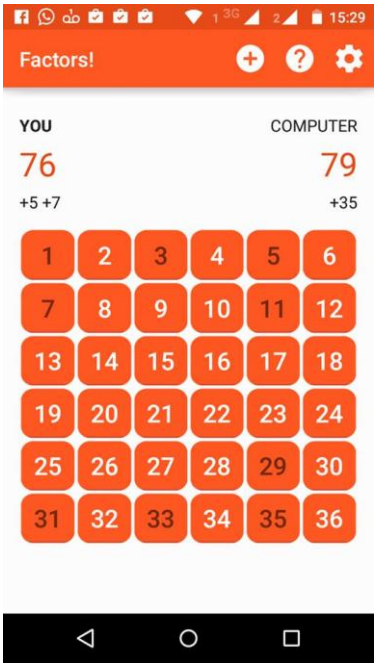
Plataforma: Android

O “Factors!” é um aplicativo com um jogo disputado contra o computador, e ganha quem somar mais pontos.

É exibida uma lista de números onde o jogador deve escolher um número entre 1 e 36 que será adicionado a sua pontuação, porém o outro jogador ganha como pontuação a soma de todos os divisores ainda ativos desse número na tela, e esses números são desativados. Em seguida, o outro jogador escolhe até que todos os números da lista sejam desativados. Ganha quem ao final obtiver a maior pontuação.

Segue uma imagem do jogo capturada por um smartphone Android.

Figura 11 – Interface do jogo “Factors!”.



Fonte: autora

As configurações iniciais do aplicativo podem ser alteradas, possibilitando diminuir a dificuldade do jogo contra o computador, aumentar a quantidade de números para 42, além de possibilitar que duas pessoas joguem uma contra a outra usando o mesmo dispositivo.

2.7 fatores primos (Antonio Luis Climent Albaladejo)

Valor: Gratuito

Plataforma: Android

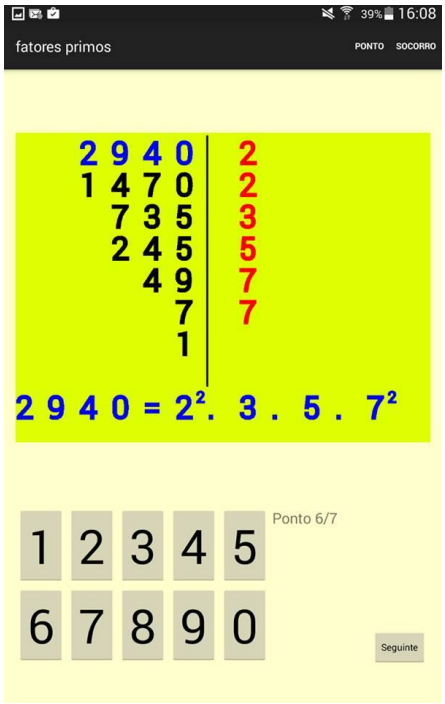
O “fatores primos” é um jogo em que números são dados aleatoriamente para decomposição em fatores primos.

Na parte inferior da tela são listados todos os algarismos de 0 a 9, que devem ser escolhidos em ordem crescente como fatores do número dado. Escolhendo o algarismo incorreto você deixa de ganhar o ponto e pode escolher um novo algarismo até fatorar o número por completo.

O diferencial deste aplicativo é que a decomposição é feita manualmente e o aluno é informado instantaneamente em caso de acerto ou erro.

Segue uma imagem da interface do aplicativo capturada por um tablet Android.

Figura 12 - Interface do app "fatores primos".



Fonte: autora

Capítulo 3

ATIVIDADES APLICADAS

Nosso objetivo nesse trabalho é aplicar em sala de aula uma pesquisa sobre os números primos, fatoração e divisibilidade através de aplicativos para smartphones e tablets e verificar a eficiência dessas tecnologias no sistema de aprendizagem.

Os aplicativos descritos aqui possuem uma enorme aplicabilidade nos assuntos do Ensino Fundamental e Médio, seja para a resolução de problemas propostos em sala de aula, como também em trabalhos escolares e outras tarefas.

O uso destes aplicativos tem como principais objetivos: despertar talentos, aguçar o interesse dos alunos, estimular a inovação no ensino da Matemática, descobrir novas alternativas para resolução de velhos problemas, estimular a pesquisa. Além disso, através dos aplicativos foi possível alcançar: agilidade nos procedimentos, maior confiabilidade nos resultados, geração de maior variedade de casos, concentração dos alunos no conceito e abordagem de novos aspectos de velhos problemas.

As tecnologias da informação e comunicação já estão presentes na sociedade, e isso traz à sala de aula, alunos nascidos em um ambiente virtual, onde tudo é muito rápido, superficial e dinâmico. Conhecer bem essa geração nos ajuda a planejar a prática docente, como destaca Passarelli e Junqueira (2012, p.311)

> Quanto mais conhecermos sobre crianças e adolescentes brasileiros conectados melhor poderemos planejar aplicações futuras, nestas telas, que motivem e propiciem a aprendizagem lúdica, a construção do conhecimento e a socialização em rede. A continuidade desta pesquisa e sua atualização sistematizada e sistêmica contribuirão, sobremaneira, para o mapeamento das literacias digitais destas crianças e jovens, podendo servir de base para o design de futuros ambientes de ensino e lazer de forma sinérgica para diluir a barreira entre ensino e lazer, onde o lúdico ensine e o ensino seja lúdico.

Mesmo com todas as vantagens, em sala de aula o uso dessas tecnologias ainda é bem escasso. Ainda notamos o uso de práticas arcaicas, remontando à época em que professores ainda eram alunos.

Convém lembrar que documentos como os Parâmetros Curriculares Nacionais (PCNs) incentivam a utilização de tecnologia nas escolas, nos mais diversos níveis e áreas: “As tecnologias, em suas diferentes formas e usos, constituem um dos principais agentes de transformação da sociedade, pelas modificações que exercem nos meios de produção e por suas consequências no cotidiano das pessoas” (BRASIL, 1998, p.43). E ainda destaca a função do professor nesse processo:

> A utilização de recursos como o computador e a calculadora pode contribuir para que o processo de ensino e aprendizagem de Matemática se torne uma atividade experimental mais rica, sem riscos de impedir o desenvolvimento do pensamento, desde que os alunos sejam encorajados a desenvolver seus processos metacognitivos e sua capacidade crítica e o professor veja reconhecido e valorizado o papel fundamental que só ele pode desempenhar na criação, condução e aperfeiçoamento das situações de aprendizagem.

A vantagem de usar aplicativos para smartphones no ensino, é que dispomos de ferramentas acessadas instantaneamente na palma da mão. Goodwin (2012) afirma que o principal benefício da utilização desses dispositivos móveis é que eles nos permite aprender em qualquer lugar e a qualquer hora, fazendo com que a aprendizagem não se limite apenas a sala de aula e ao horário escolar.

Participaram dessa pesquisa os alunos de 6°, 7° e 8° anos do Ensino Fundamental de um colégio particular localizado no município de São José do Rio Preto-SP.

3.1 Análises prévias

Os alunos tem contato com os números primos no 6° ano do Ensino Fundamental, logo após estudarem os critérios de divisibilidade. É apresentado a eles o crivo de Eratóstenes e o algoritmo para a fatoração completa de um número em fatores primos. Depois disso, os números primos e sua fatoração são aplicados no cálculo da raiz quadrada, na determinação dos

divisores de um número, cálculo do mdc e mmc e redução de frações ao mesmo denominador. Depois disso, até a conclusão do Ensino Médio, nenhuma nova aplicação é ensinada.

Os alunos que participaram desta pesquisa tinham total domínio de como fatorar um número manualmente, e isto nos possibilitou a sugerir o uso dos aplicativos para acelerar o processo de descobertas envolvidos na fatoração de um número, principalmente no que diz respeito a divisibilidade.

3.2 Análise *a priori*

Para tornar o processo de aprendizagem mais prazeroso e significativo, as atividades foram desenvolvidas inserindo o uso das tecnologias. O objetivo foi que os alunos descobrissem propriedades de divisibilidade através da análise do número decomposto em fatores primos, gerando ferramentas para resolução de problemas, em especial para problemas de Olímpiadas de Matemática.

3.3 As folhas de atividades (Experimentação)

As folhas de atividades foram preparadas para que os alunos aprendam de forma autônoma, sendo o professor apenas um mediador do processo de ensino aprendizagem.

Na primeira folha é apresentado o Teorema Fundamental da Aritmética, e propõe aos alunos verificar se 7 e 47 são divisores de 59220. Espera-se que os alunos façam a divisão e observem o resto encontrado para responder. Em seguida sugere que os alunos analisem a decomposição desse número em fatores primos, utilizando algum aplicativo citado anteriormente, e relatem suas conclusões. Feito isso, outros números são dados para que se faça o mesmo.

A segunda folha apresenta questões sobre divisibilidade do livro (Fomin, 2012). Estas questões estão relacionadas com o Teorema Fundamental da Aritmética e de acordo com Fomin (2012, p. 22): “Os alunos deveriam compreender que as propriedades de divisibilidade estão quase que

completamente determinadas pela representação de um número natural como produto de número primos.” O objetivo é verificar a entendimento dos alunos da atividade da primeira folha.

Na folha três pede-se a fatoração em número primos, sem fazer contas, apenas observando a fatoração de um primeiro número dado. E ao fim propõe um problema da Olímpiada Brasileira de Matemática de 2010.

A quarta folha leva os alunos a encontrarem todos os divisores de um número natural através da sua fatoração em números primos, e encerra com três problemas de Olimpíadas.

A quinta e última folha de atividades leva o aluno, usando os aplicativos, a relacionar o mínimo múltiplo comum e o máximo divisor comum de um número natural com as decomposições dos números dados. Também conclui a atividade com exercícios de Olimpíadas.

Todas as folhas de atividades encontram-se no Apêndice A.

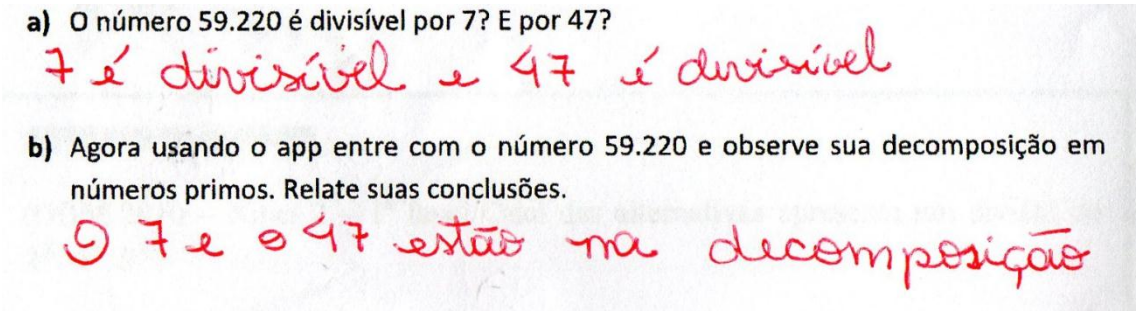
3.3.1 Atividades dentro da sala de aula

A primeira folha de atividades enuncia o Teorema Fundamental da Aritmética, e convida os alunos a explorarem os números primos. Para isso, foram instruídos a fazer o download de algum dos aplicativos listados anteriormente. A preferência para a plataforma Android foi o “Mathematics” e para IOS, o “Factorizer, numbers to factors”.

Divididos em grupos de até cinco integrantes, os alunos foram questionados sobre possíveis divisores do número 59220. A princípio, os alunos efetuaram a divisão para verificar o resto e determinar se é divisor ou não. Então dividiram 59220 por 7 e por 47 e notaram que o resto é zero e portanto, são divisores do 59220. Em seguida pede-se que, usando o aplicativo, os alunos observem a fatoração do 59220, e relatem suas conclusões.

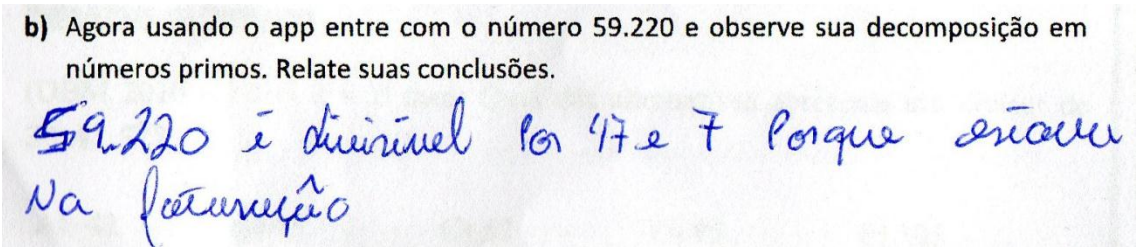
Seguem as respostas de alguns grupos para as questões da primeira folha.

Figura 13 – Respostas de um grupo para os itens a e b da 1ª folha.



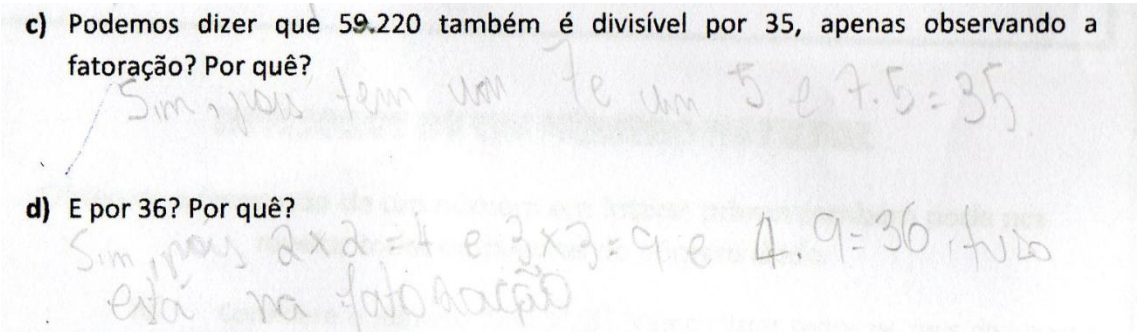
Fonte: autora

Figura 14 – Respostas de outro grupo para o item b da 1ª folha.



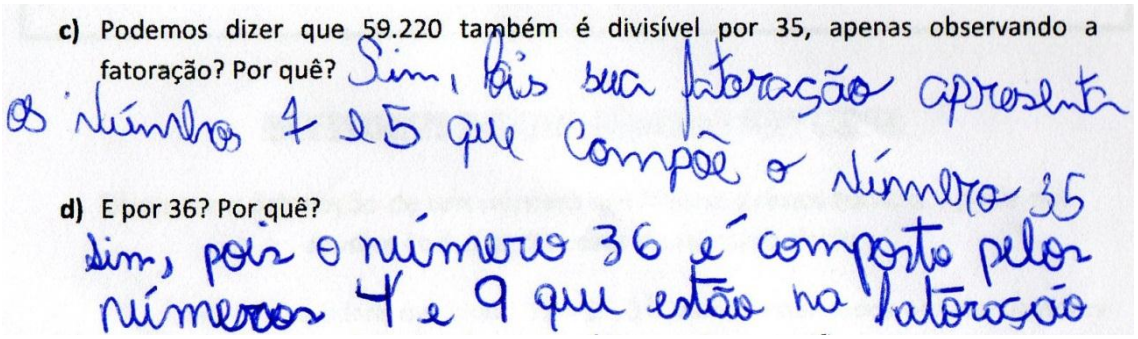
Fonte: autora

Figura 15 – Respostas de um grupo para os itens c e d da 1ª folha.



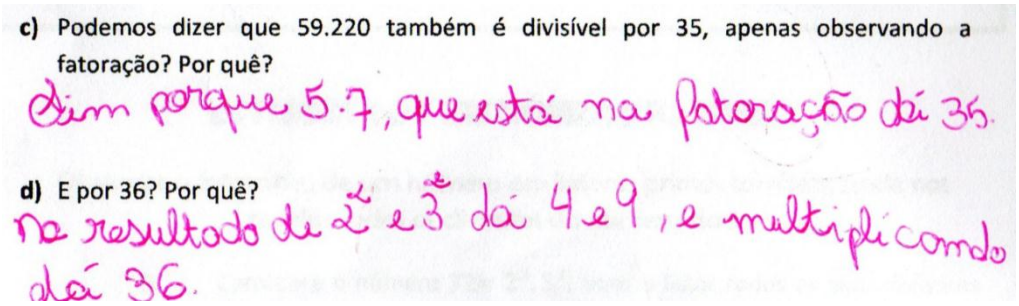
Fonte: autora

Figura 16 – Respostas de outro grupo para os itens c e d da 1ª folha.



Fonte: autora

Figura 17 – Respostas de um terceiro grupo para os itens c e d da 1ª folha.



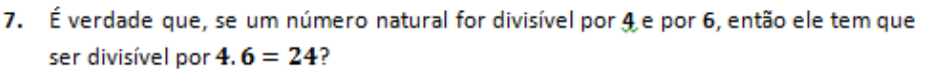
Fonte: autora

Todos os grupos responderam com facilidade quando o candidato a divisor era um número primo, pois aparecia explicitamente na decomposição. Quando se tratava de um número composto, exigia-se bom domínio de tabuada e raciocínio lógico.

Na folha número dois, questões sobre divisibilidade do livro "Círculos matemáticos A experiência Russa" de Fomin foram propostas com o objetivo de validar a aprendizagem da folha anterior. As questões 7 e 11 foram as que geraram mais dúvidas entre os alunos.

Todos os grupos imediatamente responderam SIM na questão 7. Alguns grupos, ao perguntar para a professora, foram levados a pensar no número 12. E prontamente alteraram sua resposta para NÃO, que é a resposta correta.

Figura 18 – Questão 7 da segunda folha de atividades.



Fonte: autora

Fomin (2012) apresenta a resposta desejada e seu argumento:

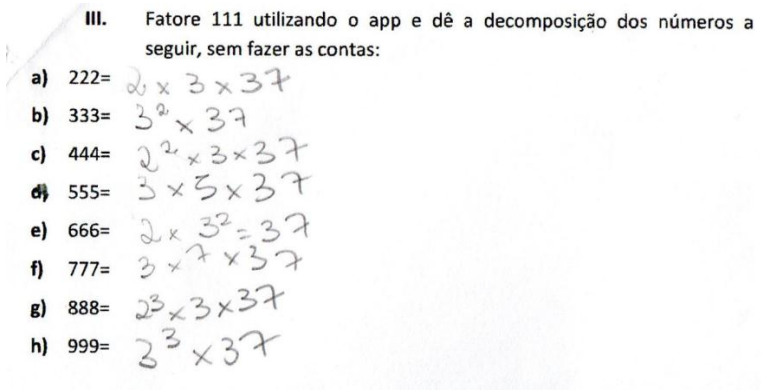
> "Não. Por exemplo, o número 12 pode servir como um contraexemplo. A razão é que, se um número for divisível por 4, então sua decomposição tem que conter pelo menos dois fatores iguais a 2; se o mesmo número for divisível por 6, isto significa que sua decomposição contém 2 e 3. Portanto, podemos ter certeza que sua decomposição tem dois fatores iguais a 2 (mas não necessariamente três!) e um igual a 3, de modo que só podemos garantir a divisibilidade por 12."

O mesmo caso ocorreu na questão 11, que afirmava erroneamente que se $15A$ é divisível por 6, então A tem que ser divisível por 6. O contraexemplo usado pela professora foi para $A = 2$. O motivo é que o número 3 que é fator do número 6, também pertence à decomposição do número 15. A única garantia que temos é que A é um número par.

E complementando a verificação da aprendizagem, a terceira folha, pede a decomposição do número 111 através do app, para que a partir dela os alunos, sem fazer contas, indiquem a decomposição dos números 222, 333, 444, 555, 666, 777, 888 e 999 em fatores primos.

Todos os grupos realizaram de forma correta essas fatorações.

Figura 19 – Decomposições pedidas na 3ª folha feitas por um dos grupos.



Fonte: autora

Por fim é proposto o problema mostrado a seguir da 1ª fase da Olímpiada Brasileira de Matemática de 2010 aplicada para o nível 2 (alunos do 8° e 9 ano do ensino fundamental).

Figura 20 – Problema da 1ª fase da OBM 2010 (Nível 2).

DESAFIO OLÍMPICO

(OBM 2010 – Nível 2 – 1ª fase) Qual das alternativas apresenta um divisor de $3^5.4^4.5^3$?

A) 42 B) 45 C) 52 D) 85 E) 105

Fonte: autora

Para listar todos os divisores de um número, é dado como exemplo o número 72. Através da decomposição em fatores primos ($72 = 2^3.3^2$), o aluno deve variar os expoentes de 2 e 3 corretamente, encontrando todas as combinações possíveis, ou seja, todos os divisores de 72.

Todos os divisores do 72 são da forma $2^m.3^n$, com $0 \leq m \leq 3$ e $0 \leq n \leq 2$. Variando os expoentes, chegamos a lista dos divisores do 72, que são 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72.

Na sequência chama a atenção dos alunos para a quantidade de divisores de um número. No caso do 72, temos quatro possibilidades para m (0, 1, 2 ou 3) e três possibilidades para n (0, 1 ou 2). Pelo princípio multiplicativo um total de $4.3 = 12$ divisores.

Para a verificação da aprendizagem, pede-se a lista de divisores dos números 60, 126 e 684 e em seguida dois problemas da 1ª fase da Olímpiada Brasileira de Matemática, um de 2011 e outro de 2012, aplicados no nível 2 e 3 (Ensino Médio), respectivamente. Propõem também um problemas da 2ª fase da Olímpiada de Matemática de Rio Preto de 2014, aplicado para o nível 1 (6° e 7° ano do Ensino Fundamental).

Figura 21 – Grupo utilizando o smartphone para realizar a atividade e relatando suas conclusões.

Fonte: autora

Figura 22 – Aluno utilizando o smartphone para realizar a atividade.

Fonte: autora

3.3.2 Atividades para casa

Para complementar o estudo feito em sala de aula, sugere-se que os alunos façam o download de aplicativos que são jogos sobre os números primos. O objetivo é treinar o aluno, de forma divertida, dando-lhe mais domínio e rapidez na divisão e capacitando-o para a resolução de problemas sobre o assunto.

No IOS, o app “Prime Shooter”, é um jogo bastante desafiador e divertido. Na parte inferior da tela são listados os números primos. Caem da tela polígonos contendo números a serem fatorados. Assim que o número começa a cair o objetivo é atirar os primos que são múltiplos dele até fatorá-lo por completo.

Para a plataforma Android, temos duas sugestões, o “Factors!” e o “fatores primos”.

O Factors! exige muito raciocínio. Tem alto grau de dificuldade. É disputado contra o computador, e o vencedor é quem somar mais pontos. O jogador deve escolher um número entre 1 e 36 que será adicionado a sua pontuação, porém o outro jogador ganha como pontuação a soma de todos os divisores ainda ativos desse número na tela, e esses números são desativados. Em seguida o outro jogador escolhe até que todos os números da lista sejam desativados.

No “fatores primos” quem faz a fatoração é o próprio jogador, que escolhe os números primos que são divisores do número dado, em ordem crescente. Caso escolha o número errado, o app informa o erro e o jogador pode escolher um novo número.

3.4 Análise a posteriori

Fazendo uma análise qualitativa do comportamento dos alunos nas atividades e das respostas apresentadas nas folhas de atividades, avaliamos que em geral o objetivo foi alcançado, pois os alunos se interessaram pelas atividades e se empenharam na realização das tarefas.

O diferencial de ter uma aula usando o smartphone ou o tablet deixou os alunos motivados e mesmo semanas depois eles ainda perguntavam quando poderiam usar os aplicativos novamente na sala de aula. Além disso, muitos deles exploraram outras funcionalidades dos aplicativos, ficando impressionados com a riqueza da Matemática, sobretudo com a função de Euler.

A aplicação da folha de atividades em sala de aula e as respostas dadas pelos alunos mostrou que algumas alterações deixariam as atividades mais claras, permitindo uma maior autonomia por parte do aluno.

Isto serviu de motivação para a reformulação da folha de atividades número 1. A folha de atividades reformulada será apresentada na íntegra no Apêndice B.

Nesta pesquisa pretendeu-se responder à seguinte questão: “Utilizar tecnologias no ensino, em especial, aplicativos para smartphones e tablets, incentivam e motivam o aluno, permitindo que eles construam um aprendizagem significativa das propriedades de divisibilidade através da decomposição de um número em fatores primos?”.

Diante das constatações dessa pesquisa, podemos responder positivamente esta questão, pois o uso dos smartphones aproxima o conteúdo a ser ensinado, do cotidiano dos alunos, além de possibilitar uma melhor visualização das propriedades de divisibilidade e permitir que os alunos explorem-nas de maneira mais rápida.

CONCLUSÃO

Diante do exposto, pode-se concluir que o uso de novas tecnologias, sobretudo aquelas de fácil acesso aos alunos (como é o caso dos aplicativos de smartphones) são excelentes para o ensino da Matemática. Ferramentas computacionais, softwares, jogos, entre outros, despertam a curiosidade, interesse e criatividade dos alunos, elevando a qualidade das aulas e do aprendizado.

Os aplicativos listados neste texto mostraram-se extremamente funcionais e aplicáveis; uma excelente ferramenta motivadora do ensino.

REFERÊNCIAS

BRASIL. Secretaria de Educação Fundamental. **Parâmetros curriculares nacionais: Matemática**. Brasília: MEC/SEF, 1998.

BOYER, Carl B. **História da Matemática**. Tradução: Elza F. Gomide. São Paulo: Edgar Blucher, Editora da Universidade de São Paulo, 1974.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. 1ª ed. Rio de Janeiro: IMPA/SBM 2000.

DU SAUTOY, Marcus. **A Música dos Números Primos: um problema não resolvido na matemática**. Tradução: Diego Alfaro. Rio de Janeiro: Zahar, 2007.

EVES, Howard. **Introdução à história da matemática**. Tradução: Hygino H. Domingues. 5ª edição - Campinas: Editora da Unicamp, 2011.

FOMIN, Dmitri. **Círculos Matemáticos: A Experiência Russa**. Tradução: Valéria M. Iório. Rio de Janeiro: IMPA, 2012.

GARBI, Gilberto Geraldo. **A Rainha das Ciências: um passeio histórico pelo maravilhoso mundo da matemática**. São Paulo: Editora Livraria da Física, 2009.

GOODWIN, Kristy. **Use of Tablet Technology in the Classroom**. 2012. Disponível em http://www.tale.edu.au/tale/live/teachers/shared/next_practice/iPad_Evaluation_Sydney_Region.pdf. Acesso em 21/12/2015.

HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2013 (Coleção PROFMAT).

LOPES, Davi. **Bézout e outros Bizus**. Material da 18ª Semana Olímpica. Olimpíada Brasileira de Matemática, 2015. Disponível em http://www.obm.org.br/export/sites/default/semana_olimpica/docs/2015/bezout_e_outros_bizus.pdf. Acesso em 15/11/2015.

OLIVEIRA, Krerley Irraciel Martins; FERNÁNDEZ, Adán José Corcho. **Iniciação à Matemática: um curso com problemas e soluções**. Rio de Janeiro: SBM, 2010.

PASSARELLI, Brasilina; JUNQUEIRA, Antonio Hélio. **Gerações Interativas Brasil – Crianças e Adolescentes diante das telas**. São Paulo: Escola do Futuro/USP, 2012. Disponível em http://ccvap.futuro.usp.br/gerinter2012.pdf. Acesso em 20/12/2015.

PEDROSO, Hermes Antonio. **História da Matemática**. 2009. Disponível em http://www.mat.ibilce.unesp.br/personal/hermes/apostila_hist_mat.pdf. Acesso em 10/11/2015.

PERUZZO, Jucimar. **O Fascínio dos Números Primos**. Irani (SC): 2012.

RIBENBOIM, Paulo. **Números primos. Velhos mistérios e novos recordes**. Rio de Janeiro: IMPA, 2014.

APÊNDICE A - Folhas de atividades aplicadas

FOLHA DE ATIVIDADES 1

EXPLORANDO OS NÚMEROS PRIMOS

Os números primos são imprescindíveis na Matemática, pois todos os números naturais são formados pela multiplicação de primos. Este é o chamado Teorema Fundamental da Aritmética: *"todo número natural maior que 1 pode ser escrito como um produto de números primos"*.

Vamos explorar um pouco mais esse universo mágico dos números primos? Para isso vamos utilizar algum dos aplicativos sugeridos anteriormente.

I. Responda:

a) O número 59.220 é divisível por 7? E por 47?

b) Agora usando o app entre com o número 59.220 e observe sua decomposição em números primos. Relate suas conclusões.

c) Podemos dizer que 59.220 também é divisível por 35, apenas observando a fatoração? Por quê?

d) E por 36? Por quê?

e) Agora pela decomposição do número em fatores primos, verifique se:

i) 696 é divisível por 29? E por 7?

ii) 49.800 é divisível por 83? E por 75? E por 24? E por 16?

FOLHA DE ATIVIDADES 2

Decompor um número em fatores primos é testar quais primos são divisores do número dado.

II. Responda (FOMIN):

1. O número $\mathbf{2^9.3}$ é divisível por **2**?

2. O número $\mathbf{2^9.3}$ é divisível por **5**?

3. O número $\mathbf{2^9.3}$ é divisível por **8**?

4. O número $\mathbf{2^9.3}$ é divisível por **9**?

5. O número $\mathbf{2^9.3}$ é divisível por **6**?

6. É verdade que, se um número natural for divisível por **4** e por **3**, então ele tem que ser divisível por $\mathbf{4.3 = 12}$?

7. É verdade que, se um número natural for divisível por **4** e por **6**, então ele tem que ser divisível por $\mathbf{4.6 = 24}$?

8. O número **a** não é divisível por **3**. É possível que o número **2a** seja divisível por **3**?

9. O número **a** é par. É verdade que **3a** tem que ser divisível por **6**?

10. O número **5a** é divisível por **3**. É verdade que **a** tem que ser divisível por **3**?

11. O número **15a** é divisível por **6**. É verdade que **a** tem que ser divisível por **6**?

FOLHA DE ATIVIDADES 3

III. Fatore 111 utilizando o app e dê a decomposição dos números a seguir, sem fazer as contas:

a) 222=

b) 333=

c) 444=

d) 555=

e) 666=

f) 777=

g) 888=

h) 999=

DESAFIO OLÍMPICO

(OBM 2010 – Nível 2 – 1ª fase) Qual das alternativas apresenta um divisor de $3^5.4^4.5^3$?

A) 42

B) 45

C) 52

D) 85

E) 105

FOLHA DE ATIVIDADES 4

DIVISORES DE UM NÚMERO NATURAL

Observar a fatoração de um número em fatores primos também pode nos revelar todos os divisores do número dado.

IV. Considere o número 72= $\mathbf{2}^3.\mathbf{3}^2$. Vamos listar todos os seus divisores positivos.

Já sabemos que todo divisor de 72 deve ser obtido apenas usando os primos 2 e 3, variando apenas o seu expoente. Podemos então escrever que todos os divisores de 72 são da forma $2^m.3^n$, com $0 \leq m \leq 3$ e $0 \leq n \leq 2$. Temos então:

$m = 0 \; e \; n = 0 \; \rightarrow 2^0.3^0 = 1.1 = 1$	$m = \quad e \; n = \quad \rightarrow$
$m = 1 \; e \; n = 0 \; \rightarrow 2^1.3^0 = 2.1 = 2$	$m = \quad e \; n = \quad \rightarrow$
$m = \quad e \; n = \quad \rightarrow$	$m = \quad e \; n = \quad \rightarrow$
$m = \quad e \; n = \quad \rightarrow$	$m = \quad e \; n = \quad \rightarrow$
$m = \quad e \; n = \quad \rightarrow$	$m = \quad e \; n = \quad \rightarrow$
$m = \quad e \; n = \quad \rightarrow$	$m = \quad e \; n = \quad \rightarrow$

Assim
$D_{72} = \{ \qquad \qquad \}$

Note que temos 4 possibilidades para *m* e 3 possibilidades para *n*, então $4.3 = 12 \; divisores$.

V. Determine os divisores dos números a seguir:

a) 60 b) 126 c) 684

DESAFIO OLÍMPICO

(OBM 2012 – Nível 2 – 1ª fase) Qual é o menor número ímpar que possui exatamente 10 divisores positivos incluindo o 1 e o próprio número?

A) 1875 B) 405 C) 390 D) 330 E) 105

(OBM 2011 – Nível 2 e 3 – 1ª fase) Quantos números inteiros positivos menores que 30 têm exatamente quatro divisores positivos?

A) 6 B) 7 C) 8 D) 9 E) 10

(OMRP 2014 – Nível 1 – 2ª fase) A soma de todos os divisores de 100 é:

a) 11. b) 217. c) 221. d) 222. e) 250

FOLHA DE ATIVIDADES 5

MÍNIMO MÚLTIPLO COMUM E MÁXIMO DIVISOR COMUM

VI. Entre com os números a seguir no app e observe sua decomposição, mmc e mdc:

(6,10)

(10, 12)

(42, 55)

(110, 210)

(132, 30)

(504, 1260)

1. Explique como é obtido o mdc.

2. Explique como é obtido o mmc.

DESAFIO OLÍMPICO

(OMRP 2014 – Nível 1 – 2ª fase) Num jogo de videogame, dois pilotos, Zé da Álgebra e Chico das Contas, disputam uma corrida de motos. Zé completa cada volta em 45 segundos e Chico, em 48 segundos. As motos de Zé e de Chico só se encontram no momento em que Zé termina (e vence) a corrida. Quantas voltas tem a corrida?

a) 15 voltas. b) 16 voltas. c) 18 voltas. d) 20 voltas. e) 21 voltas

APÊNDICE B - Folha de atividades número 1 - reformulada

FOLHA DE ATIVIDADES 1 - REFORMULADA

EXPLORANDO OS NÚMEROS PRIMOS

Os números primos são imprescindíveis na Matemática, pois todos os números naturais são formados pela multiplicação de primos. Este é o chamado Teorema Fundamental da Aritmética: *"todo número natural maior que 1 pode ser escrito como um produto de números primos"*.

Vamos explorar um pouco mais esse universo mágico dos números primos? Para isso vamos utilizar algum dos aplicativos sugeridos anteriormente.

VII. Responda:

a) Faça as divisões e responda: O número 59.220 é divisível por 7? E por 47? E por 11?

b) Agora usando o app entre com o número 59.220 e observe sua decomposição em números primos. Relacione com o item anterior relatando aqui suas conclusões.

c) Podemos dizer que 59.220 também é divisível por 35, apenas observando a fatoração? Por quê?

d) Confira se sua resposta do item c está correta efetuando a divisão de 59.220 por 35, relatando suas conclusões.

e) Observando apenas a decomposição responda: 59.220 é divisível por 36?

f) Agora pela decomposição do número em fatores primos, verifique se:

iii) 696 é divisível por 29? E por 7?

iv) 49.800 é divisível por 83? E por 15? E por 24? E por 16?