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

RAFAEL LUIZ SIMÃO

UM APLICATIVO EM TEORIA DOS NÚMEROS E SUA UTILIZAÇÃO COMO RECURSO DIDÁTICO

DISSERTAÇÃO

CORNÉLIO PROCÓPIO

2018

RAFAEL LUIZ SIMÃO

UM APLICATIVO EM TEORIA DOS NÚMEROS E SUA UTILIZAÇÃO COMO RECURSO DIDÁTICO

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 em Matemática.

Orientadora: Dra. Débora Aparecida Francisco Albanez

CORNÉLIO PROCÓPIO

2018

Dados Internacionais de Catalogação na Publicação

S593 Simão, Rafael Luiz

Um aplicativo em teoria dos números e sua utilização como recurso didático / Rafael Luiz Simão. – 2018.
71 f. : il. color. ; 31 cm.

Orientadora: Débora Aparecida Francisco Albanez.
Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. Cornélio Procópio, 2018.
Bibliografia: p. 71.

1. Computadores de bolso. 2. Aplicativos móveis. 3. Teoria dos números. 4. Matemática – Dissertações. I. Albanez, Débora Aparecida Francisco, orient. II. Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD (22. ed.) 510

Biblioteca da UTFPR - Câmpus Cornélio Procópio
Bibliotecários/Documentalistas responsáveis:
Simone Fidêncio de Oliveira Guerra – CRB-9/1276
Romeu Righetti de Araujo – CRB-9/1676

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação-Câmpus Cornélio Procópio
Programa de Mestrado Profissional em Matemática em Rede Nacional

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS CORNÉLIO PROCÓPIO

PROFMAT

Título da Dissertação Nº. 008

"Um Aplicativo em Teoria dos Números e sua Utilização como Recurso Didático."

por

Rafael Luiz Simão

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de Mestre, pelo Programa de Mestrado em Matemática em Rede Nacional - PROFMAT - da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Cornélio Procópio, às 13h00min do dia 12 de junho de 2018. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

Profª. Débora Aparecida Frrancisco Albanez, Dra.
(Presidente - UTFPR/CP)

Prof. Anderson Paião dos Santos, Dr.
(UTFPR/CP)

Prof. Maicon José Benvnutti, Dr.
(UFSC/Blumenau)

Visto da coordenação:

Prof. Thiago Pinguello de Andrade, Dr.
(Coordenador do PROFMAT-CP)

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

À minha família.
À minha mãe, Dona Sônia.

AGRADECIMENTOS

Apresento meus sinceros agradecimentos aos meus pais Sônia Maria Tavares Simão e Valdir Simão, que sempre me guiaram e me motivaram em meus estudos.

Jamais terei como agradecer todo o amor, toda a compreensão e motivação que minha esposa Daniela Ap. de Melo e meu filho Rafael Melo Simão tiveram durante todo este trabalho, pois sem eles não teria forças para concluí-lo.

À CAPES, pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior e pelo incentivo financeiro.

Ao meu grande amigo que fiz nesta trajetória Alisson Lucas de Souza, pela grande ajuda no desenvolvimento do aplicativo.

A todos os professores da PROFMAT-UTFPR-CP, que me ajudaram a alcançar meus objetivos.

Por fim, tenho muito a agradecer a minha orientadora, professora Dra. Débora Aparecida Francisco Albanez pelas orientações na elaboração deste trabalho, sem a qual esse trabalho não seria possível.

“Tente! (Tente!)
E não diga
Que a vitória está perdida
Se é de batalhas
Que se vive a vida
Han!
Tente outra vez!”

Tente Outra Vez (Raul Seixas)

RESUMO

SIMÃO, Rafael Luiz. UM APLICATIVO EM TEORIA DOS NÚMEROS E SUA UTILIZAÇÃO COMO RECURSO DIDÁTICO. 71 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2018.

Neste trabalho desenvolvemos um aplicativo do tipo *quiz* para dispositivos móveis, isto é, um jogo com questões e soluções relacionadas a tópicos em Teoria de Números elementar. A criação deste aplicativo tem como intuito servir como ferramenta de apoio a docentes de matemática, além de motivar estudantes do ensino fundamental e médio. Além disso, o aplicativo também é voltado à qualquer pessoa que possa se interessar pelo tema, pois ele estará disponível nas lojas online de aplicativos.

Palavras-chave: dispositivos móveis, aplicativos, Teoria de números

ABSTRACT

SIMÃO, Rafael Luiz. . 71 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2018.

In this work a *quiz* app were developed for mobile devices, namely, a game with questions and solutions related to elementar Number Theory concepts. The creation of the app is intended to be a support tool for maths teachers of elementary and high school and also motivating students. Besides, this app is aimed at anyone who might be interested in the topics, since it is avaliable on online app stores.

Keywords: mobile devices, apps, Number Theory

LISTA DE FIGURAS

FIGURA 1 – Aplicativo disponível na loja virtual *Play Store* 49
FIGURA 2 – Tela inicial de *Teoria dos Números - Quiz Show* 50
FIGURA 3 – Menu principal de *Teoria dos Números - Quiz Show*. 51
FIGURA 4 – Menu de temas de *Teoria dos Números - Quiz Show* 51
FIGURA 5 – Exemplo de pergunta do tema *DIVISIBILIDADE* 52
FIGURA 6 – Tela de confirmação da resposta 53
FIGURA 7 – Opção *SOLUÇÃO* 54
FIGURA 8 – Solução referente à pergunta 55
FIGURA 9 – Contador de acertos 55
FIGURA 10 – Mensagem de motivação para continuação. 56
FIGURA 11 – Mensagem de erro 56
FIGURA 12 – Exemplos de telas com resultados satisfatórios 56
FIGURA 13 – Exemplos de telas com resultados abaixo do esperado 57
FIGURA 14 – Opções de salvar os resultados 57
FIGURA 15 – Tela *SCORE* 58
FIGURA 16 – Passos para visualizar os pontos salvos 58
FIGURA 17 – Tela *SOBRE* 59
FIGURA 18 – Passos para a 2ª aula de Divisibilidade 61
FIGURA 19 – Exemplo de questão disponível no aplicativo 62
FIGURA 20 – Score dos alunos durante a aula de Divisibilidade. 63
FIGURA 21 – Exemplo de questão disponível no aplicativo 64
FIGURA 22 – Aluno utilizando aplicativo *Teoria dos Números - Quiz Show*. 65
FIGURA 23 – Exemplo de questão disponível no aplicativo 66
FIGURA 24 – Utilização do aplicativo por um aluno 67
FIGURA 25 – Exemplo de questão disponível no aplicativo 68
FIGURA 26 – Alunos utilizando o aplicativo como recurso didático 69
FIGURA 27 – SCORE com Opção Geral 69

SUMÁRIO

1 INTRODUÇÃO 16
2 FUNDAMENTOS DE TEORIA DOS NÚMEROS 18
2.1 PRINCÍPIO DA INDUÇÃO FINITA 18
2.2 DIVISIBILIDADE 21
2.2.1 Alguns Critérios de Divisibilidade 26
2.3 MDC, MMC E ALGORITMO DE EUCLIDES 31
2.3.1 Máximo Divisor Comum 32
2.3.2 Algoritmo de Euclides 35
2.3.3 Mínimo Múltiplo Comum 40
2.4 NÚMEROS PRIMOS 41
2.5 EQUAÇÕES DIOFANTINAS LINEARES 45
3 ESTRUTURA E FUNCIONAMENTO DO APLICATIVO TEORIA DOS NÚMEROS - QUIZ SHOW 49
3.1 APRESENTAÇÃO DO APLICATIVO *TEORIA DOS NÚMEROS - QUIZ SHOW* ... 50
4 PROPOSTA DE ATIVIDADE EM SALA DE AULA 60
4.1 *TEORIA DOS NÚMEROS - QUIZ SHOW:* DIVISIBILIDADE 60
4.2 *TEORIA DOS NÚMEROS - QUIZ SHOW:* NÚMEROS PRIMOS 63
4.3 *TEORIA DOS NÚMEROS - QUIZ SHOW:* MDC/MMC 65
4.4 *TEORIA DOS NÚMEROS - QUIZ SHOW:* EQUAÇÕES DIOFANTINAS 67
5 CONCLUSÃO 70
REFERÊNCIAS 71

1 INTRODUÇÃO

Segundo os Parâmetros Curriculares Nacionais (PCN)(EDUCAÇÃO, 1998)

> É consensual a ideia de que não existe um caminho que possa ser identificado como único e melhor para o ensino de qualquer disciplina, em particular, da Matemática. No entanto, conhecer diversas possibilidades de trabalho em sala de aula é fundamental para que o professor construa sua prática. Dentre elas, destacam-se a História da Matemática, as tecnologias da comunicação e os jogos como recursos que podem fornecer os contextos dos problemas, como também os instrumentos para a construção das estratégias de resolução.

Com esta percepção, este trabalho não vem com o intuito de identificar a melhor prática do ensino da Matemática, mas contribuir com tantas outras já existentes para que o processo de ensino e aprendizagem da Matemática seja melhorado. Nele, visamos o uso da tecnologia via um aplicativo para dispositivos móveis como estratégia de ensino em resolução de problemas relacionados aos tópicos de Teoria de Números elementar, que são abordados no ensino fundamental e médio. Além disso, tal aplicativo também aborda um tópico relacionado à equações diofantinas.

É fato que a tecnologia se faz presente no cotidiano de estudantes de todos os níveis, e com o aumento do acesso a aparelhos eletrônicos, principalmente dispositivos móveis como *tablets* e celulares por parte de crianças e adolescentes, cada vez mais os docentes vem "disputando" espaço com estes aparelhos dentro da sala de aula. Assim, cabe aos educadores se adequarem a realidade que a educação deve evoluir, pois assim como as tecnologias evoluíram para melhorar a qualidade de vida do homem, ela pode e deve também ser usada para melhorar a qualidade da educação, em todos os aspectos.

Segundo (KENSKI, 2011) página 103,

> O uso criativo das tecnologias pode auxiliar os professores a transformar o isolamento, a indiferença e a alienação com que costumeiramente os alunos frequentam as salas de aula, em interesse e colaboração, por meio dos quais eles aprendam a aprender, a respeitar, a aceitar, a serem pessoas melhores e cidadãos participativos.

Por outro lado, percebemos muitas vezes que o uso incorreto de dispositivos móveis tem tido efeito contrário ao desejado, que é o de ser uma ferramenta de auxílio a aprendizagem. Vários estudantes, quando lhes é permitido o uso de tecnologia em sala de aula para busca de um assunto acadêmico, permanecem dispersos e sem foco, navegando em redes sociais e sites não-relacionados às disciplinas e ao conteúdo escolar. Desta maneira, faz-se necessário o desenvolvimento de programas e aplicativos que tenham foco no ensino e aprendizagem de determinado tema ao qual o professor está abordando em sua aula.

Tendo em vista tal necessidade, o objetivo deste trabalho foi desenvolver um aplicativo para dispositivos móveis do tipo perguntas e respostas com soluções, nomeado *Teoria de Números-Quiz Show*, isto é, um jogo de perguntas e respostas em diferentes níveis do conhecimento acerca de teoria de números elementar, conteúdo este abordado no ensino fundamental e médio. O aplicativo *quiz* possui problemas variados, desde questões de manipulação algébrica para que o aluno possa se familiarizar com contas de divisão até problemas contextualizados envolvendo divisibilidade. Maiores detalhes são explicitados no Capítulo 3.

Este trabalho está organizado da seguinte maneira: o Capítulo 2 traz os fundamentos de teoria dos números nos quais estão baseadas as questões criadas para o aplicativo, dentre eles o princípio da indução finita, as propriedades de divisibilidade nos inteiros, os conceitos de máximo divisor comum (como o algoritmo de Euclides), os conceitos de mínimo múltiplo comum, os números primos, e ainda, as propriedades das Equações Diofantinas.

No Capítulo 3, exibimos a estrutura e funcionamento do aplicativo desenvolvido *Teoria dos Números - Quiz Show*, apresentando a instalação e as funcionalidades do aplicativo.

No Capítulo 4, apresentamos o roteiro da atividade desenvolvida em sala de aula usando o aplicativo *Teoria de Números - Quiz Show*, de uma turma de 9º ano do ensino médio de um colégio municipal. Tal roteiro pode ser utilizado por qualquer professor que deseje utilizar o aplicativo em sala de aula, para estimular os estudantes.

2 FUNDAMENTOS DE TEORIA DOS NÚMEROS

Este capítulo aborda alguns conceitos relacionados à teoria de números, no qual se encontra a teoria básica e complementar para a resolução das questões desenvolvidas no aplicativo *Teoria dos Números - Quiz Show*. As referências utilizadas aqui são as obras (MOREIRA et al., 2012), (HEFEZ, 2014), (SANTOS, 2017) e (MILIES; COELHO, 2013).

2.1 PRINCÍPIO DA INDUÇÃO FINITA

No desenvolvimento da matemática, muitos resultados e fórmulas foram "descobertos" por grandes matemáticos através da verificação de sua validade apenas para um conjunto finito, por exemplo. Mas como ter certeza que tais resultados eram realmente verdadeiros? Em outras palavras, seriam essas fórmulas válidas para um conjunto infinito de elementos, onde não conseguimos "testar" sua validade um-a-um? Um método para concluir se um resultado é verdadeiro para propriedades relacionadas aos números naturais é o *Princípio da Indução Finita*.

O *Princípio da Indução Finita* baseia-se em verificar duas etapas:

Seja $P(n)$ uma propriedade agregada ao número natural n, tal que n_1 seja seu primeiro elemento. Devemos verificar os seguintes passos:

1. (Passo Base ou Base de Indução) $P(n_1)$ é verdadeira,
2. (Passo Indutivo) Se $P(n)$ é verdadeira para algum número natural $n \geq n_1$, então $P(n+1)$ também é verdadeira.

No passo base é verificado se a propriedade $P(n)$ é válida para o menor valor positivo que n pode admitir. A segunda etapa é considerar $P(n)$ verdadeiro para todo $n \in \mathbb{N}$, que nada mais é do que nossa *hipótese de indução*, e verificar se a propriedade é válida para $P(n+1)$.

O *Princípio de Indução Finita* possui uma variante, chamada de *Princípio da Indução Completa*, que baseia-se em verificar duas etapas:

Seja $P(n)$ uma propriedade agregada ao número natural n, tal que n_1 seja seu menor elemento. Devemos verificar os seguintes passos:

1. (Passo Base ou Base de Indução) $P(n_1)$ é verdadeira e
2. (Passo Indutivo) Se $P(k)$ é verdadeira para todo natural k tal que $n_1 \leq k \leq n$, então $P(n+1)$ também é verdadeira.

Este processo significa supor a propriedade $P(n)$ válida para $1,2,3,4,\cdots,n-2,n-1,n$, ou seja, se é valido até o número natural n, também deverá ser para $n+1$, não importando o tão grande ele seja.

Vamos mostrar por exemplo a sequência de Fibonacci, que é muito conhecida pelos amantes da matemática, que é estabelecida de forma recursiva onde a partir dos termos $F_1 = 1$ e $F_2 = 1$ obtemos os próximos termos somando os dois termos anteriores ao termo desejado. Mais precisamente

$$F_{n+1} = F_n + F_{n-1}, \quad \text{para} \quad n \geq 2,$$

estabelecendo a sequência a seguir:

$$F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \cdots$$

Facilmente conseguimos encontrar os primeiros termos desta sequência, porém qual seria o termo F_{100}, F_{300} ou ainda o termo F_{2018}? Para determinar qualquer termo da sequência de Fibonacci podemos contar com a *fórmula de Binet*, que é representada a seguir

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} \tag{1}$$

onde n representa a posição do *n-ésimo* termo. Verificaremos sua veracidade utilizando o Princípio da Indução Finita sobre o número natural n. Primeiramente, note que esta sequência é definida a partir de dois termos, logo devemos verificar a fórmula para os dois termos iniciais, ou seja, para $n = 1$ e $n = 2$, teremos que

1. Base de Indução :

$$F_1 = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1$$

e

$$\begin{aligned} F_2 &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} = \frac{\frac{1+2\sqrt{5}+5}{4} - \frac{1-2\sqrt{5}+5}{4}}{\sqrt{5}} \\ &= \frac{\frac{1+2\sqrt{5}+5-1+2\sqrt{5}-5}{4}}{\sqrt{5}} = \frac{\frac{4\sqrt{5}}{4}}{\sqrt{5}} = 1 \end{aligned}$$

e portanto, a igualdade é válida para $n = 1$e $n = 2$. Suponha agora que a afirmação é verdadeira para algum natural $n > 2$, isto é, vale a igualdade (1) para $n > 2$. Devemos verificar que

$$F_{n+1} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}.$$

Segue da lei de formação recursiva da sequência de Fibonacci que

$$F_{n+1} = F_n + F_{n-1},$$

e da hipótese de indução segue

$$\begin{aligned} F_{n+1} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} \cdot \left(\frac{1+\sqrt{5}}{2} + 1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \cdot \left(1 + \frac{1-\sqrt{5}}{2}\right)}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} \cdot \left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} \cdot \left(\frac{3-\sqrt{5}}{2}\right)}{\sqrt{5}}. \end{aligned} \tag{2}$$

Note que

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{2}{2} \cdot \left(\frac{3+\sqrt{5}}{2}\right) = \frac{3+\sqrt{5}}{2}, \tag{3}$$

e, além disso,

$$\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{2}{2} \cdot \left(\frac{3-\sqrt{5}}{2}\right) = \frac{3-\sqrt{5}}{2}. \tag{4}$$

Substituindo (3) e (4) na igualdade (2), temos

$$\begin{aligned} F_{n+1} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^{2}-\left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^{2}}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1+2}-\left(\frac{1-\sqrt{5}}{2}\right)^{n-1+2}}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}}. \end{aligned}$$

Portanto, pelo Princípio da Indução Finita a *fórmula de Binet* é válida para todo $n \in \mathbb{N}$.

2.2 DIVISIBILIDADE

Nesta seção, relembramos o conceito de divisibilidade e estudamos algumas de suas propriedades.

Definição 2.1. *Dados dois números inteiros a e b, dizemos que a divide b ou que a é um divisor de b e ou ainda que b é um múltiplo de a, e representamos por $a|b$, se existir um $c \in \mathbb{Z}$, tal que*

$$b = ac,$$

caso contrário dizemos que "a não divide b", representado por $a \nmid b$.

Exemplo 2.2. *Temos que 2 divide 10, pois inteiro $c = 5$ tal que $10 = 2 \cdot c$. No entanto, 2 não divide 17, já que não existe nenhum inteiro que satisfaça a igualdade $17 = 2 \cdot c$, uma vez que 17 não é um número par.*

Proposição 2.3. *Sejam a, b, c, $d \in \mathbb{Z}$ quaisquer. Temos:*

(i) $1|a$, $a|0$ *e* $a|a$.

(ii) Se $a|b$ *e* $b|c$, *então* $a|c$.

(iii) Se $a|b$ *e* $c|d$, *então* $ac|bd$.

(iv) Se $a|b$ *e* $a|c$, *então* $a|(b+c)$.

(v) Se $a|b$, *então para todo* $m \in \mathbb{Z}$, *tem-se que* $a|mb$.

(vi) Se $a|b$ *e* $a|c$, *então, para todos* $m,n \in \mathbb{Z}$, *tem-se que* $a|(mb+nc)$.

Demonstração. As demonstrações a seguir seguem diretamente da definição de divisibilidade:

(i) Decorre das igualdades $a = a \cdot 1$, $0 = a \cdot 0$ e $1 = 1 \cdot a$.

(ii) Se $a|b$ e $b|c$, por definição, existem $f, g \in \mathbb{Z}$, tais que $b = af$ e $c = bg$. Substituindo o valor de b da primeira equação na segunda, obtemos

$$c = (af) \cdot g,$$

e consequentemente

$$c = (fg) \cdot a.$$

Logo, $a|c$.

(iii) Dados que $a|b$ e $c|d$, por definição existem $t, t' \in \mathbb{Z}$, tais que $b = ta$ e $d = t'c$. Multiplicando a primeira igualdade por d e a segunda igualdade a, obtemos

$$bd = tad$$

e

$$ad = at'c.$$

Fazendo as devidas substituições encontramos $bd = (tt')ac$, e portanto $ac|bd$.

(iv) Dados que $a|b$ e $a|c$, por definição existem $d, d' \in \mathbb{Z}$, tais que $b = ad$ e $c = ad'$. Somando ordenadamente ambas as igualdades, temos

$$b + c = ad + ad' = a \cdot (d + d'),$$

e consequentemente $a|(b + c)$.

(v) Suponha que $a|b$, sabemos por definição que existe um inteiro y tal que $b = ay$. Multiplicando tal igualdade por um inteiro m, obtemos $bm = a \cdot (ym)$, e assim segue que $a|bm$.

(vi) Se $a|b$ e $a|c$, temos que existem $f, g \in \mathbb{Z}$, tais que $b = af$ e $c = ag$. Logo, para m e n inteiros, temos

$$mb + nc = m(af) + n(ag) = a(mf + ng),$$

e portanto $a|(mb + nc)$.

□

A seguir, apresentamos dentre as mais variadas ferramentas matemáticas, um método

muito útil para resolução de diversos problemas matemáticos, a saber, *A Divisão Euclidiana* ou *divisão com restos*, como o próprio nome sugere foi apresentado por Euclides.

Antes de apresentarmos tal ferramenta, relacionada à divisões de números inteiros, enunciaremos um princípio útil para a demonstração desta, denominado *Princípio da Boa Ordenação* (ou Princípio da Boa Ordem).

Axioma 2.4. *(Princípio da Boa Ordenação) Todo conjunto não-vazio de inteiros não-negativos contém um elemento mínimo.*

Proposição 2.5. *Seja a um inteiro tal que $0 \leq a \leq 1$. Então, $a = 0$ ou $a = 1$.*

Demonstração. Suponhamos por absurdo que exista um inteiro a diferente de 0 e 1 nessas condições. Assim, o conjunto $S = \{\, a \in \mathbb{Z} \mid 0 < a < 1\}$ seria não-vazio e pelo *Princípio da Boa Ordenação* existiria $m = min\ S$.

Como $m \in S$ temos que $m > 0$ e $m < 1$. Multiplicando por m a segunda desigualdade, obtemos $m^2 < m$. Assim, $m^2 > 0$ e, como $m < 1$, da propriedade transitiva temos $m^2 < 1$. Logo, $m^2 \in S$ e é menor que seu elemento mínimo, uma contradição. □

Antes de apresentarmos *A Divisão Euclidiana*, estudaremos um caso particular:

Lema 2.6. *Sejam a e b inteiros, tais que $a \geq 0$ e $b > 0$. Então, existem q e r, tais que $a = bq + r$ e $0 \leq r < b$, onde q e r são chamados o quociente e resto da divisão de a por b.*

Demonstração. Consideremos o seguinte conjunto

$$S = \{a - bx \,|\, x \in \mathbb{Z}, a - bx \geq 0\}.$$

Quando $x = 0$, temos que $a - bx = a \geq 0$ é um elemento de S, logo, $S \neq \varnothing$. Pelo *Princípio da Boa Ordenação*, existem $r = min\ S$. Como $r \in S$, ele também é da forma $r = a - bq \geq 0$, para algum $q \in \mathbb{Z}$. Para mostrar que as condições do enunciado estão verificadas, bastará provar que $r < b$. De fato, se fosse $r \geq b$, teríamos que:

$$a - b(q+1) = a - bq - b = r - b \geq 0,$$

logo, $a - b(q+1)$ também pertenceria a S. Mas $a - b(q+1) = r - b < r = min\ S$, uma contradição. □

Teorema 2.7. *(Divisão Euclidiana) Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tal que*

$$a = bq + r \quad e \quad 0 \leq r < |b|,$$

onde q e r são chamados o quociente e resto da divisão de a por b.

Demonstração. Mostraremos inicialmente que podemos determinar q e r quando $b > 0$ e a é qualquer.

O caso $a \geq 0$ está dado pelo Lema 2.6. Se $a < 0$ podemos, ainda pelo Lema 2.6, determinar q' e r' tais que

$$|a| = bq' + r' \quad \text{e} \quad 0 \leq r' < b.$$

Se $r' = 0$, temos $-|a| = a = b(-q') + 0$, e o par $q = q'$, $r = 0$ verifica as condições do teorema. Caso $r' > 0$, temos

$$a = -|a| = b(-q') - r' = b(-q') - b + b - r' = b(-q' - 1) + (b - r').$$

Obviamente, $0 < b - r' < b$; logo, os inteiros $q = -q' - 1$ e $r = b - r'$ verificam as condições do enunciado.

Agora provaremos que o resultado também vale quando $b < 0$. Qualquer que seja a, pela parte anterior, podemos determinar q' e r' tais que

$$a = |b|q' + r' \quad \text{e} \quad 0 \leq r' < |b|.$$

Quando $b < 0$, temos que $|b| = -b$, logo,

$$a = |b|q' + r' = (-b)q' + r' = b(-q') + r',$$

e os inteiros $q = -q'$ e $r = r'$ estão nas condições do enunciado.

Finalmente, provaremos que, se (q, r) e (q', r') são dois pares de inteiros verificando as condições do enunciado, então $q = q'$ e $r = r'$. De fato, temos que

$$qb + r = a = q'b + r'. \tag{5}$$

Podemos supor, por exemplo, que $r' \geq r$. Da igualdade acima, temos $(q - q')b = r' - r$. Como $|b| > r'$, também temos $r' - r < |b|$. Substituindo, $(q - q')b < |b|$ e, tomando módulos,

$$0 \leq |q - q'||b| < |b|.$$

Sendo $|b| > 0$, podemos cancelar e obteremos $0 \leq |q - q'| < 1$. Da Proposição 2.5 vem que $|q - q'| = 0$, isto é, $q = q'$. Na igualdade (5), temos agora $qb + r = qb + r'$. Cancelando, segue $r = r'$.

□

Exemplo 2.8. *Na divisão de 45 por 6, o quociente é $q = 7$ e o resto $r = 3$.*

O próximo exemplo pode ser encontrado no aplicativo *Teoria dos Números - Quiz Show*.

Exemplo 2.9. *O número 523 quando dividido por 7 deixa um resto diferente de zero. A alternativa que representa o número 523 dividido por 7 é:*

a) $7 \cdot 74 + 1$

b) $7 \cdot 74 + 3$

c) $7 \cdot 74 + 4$

d) $7 \cdot 74 + 5$

Solução. *Pelo algoritmo da divisão, dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$, tais que todo número é da forma*

$$a = bq + r \quad e \quad 0 \leq r < b,$$

onde q é o quociente e r o resto da divisão.

Primeiramente podemos efetuar a divisão de 523 por 7 e verificar qual é o resto desejado, assim:

$$\begin{array}{r|l} 523 & 7 \\ \hline 33 & 74 \\ 5 & \end{array}$$

Logo o resto da divisão de 523 por 7 será 5 e assim podemos escrever o número 523 da forma

$$523 = 7 \cdot 74 + 5.$$

Observação 2.10. *Do Algoritmo da Divisão Euclidiana podemos concluir que todo número inteiro maior ou igual a 2, quando dividido por 2, tem resto 0 ou 1. Aos números da forma $n = 2k + 1$, com $k \in \mathbb{Z}$ denominamos ímpar e da forma $n = 2k$ denominamos par.*

Exemplo 2.11. *Usando o Algoritmo da Divisão Euclidiana temos que todo inteiro ímpar é da forma $4k + 1$ ou $4k + 3$.*

Solução. *Seja N um inteiro ímpar. Pelo Algoritmo da Divisão Euclidiana podemos escrever* $N = 2m+1$ *para* $m \in \mathbb{Z}$*. Note que m poder ser par ou ímpar. Para m par, teremos* $m = 2k$ *com* $k \in \mathbb{Z}$*, logo*

$$N = 2m+1 = 2\cdot(2k)+1 = 4k+1.$$

Por outro lado, temos que se m for ímpar, $m = 2k+1, k \in \mathbb{Z}$*, portanto*

$$N = 2m+1 = 2\cdot(2k+1)+1 = 4k+3.$$

Logo todo inteiro ímpar é da forma $4k+1$ *ou* $4k+3$*.*

2.2.1 ALGUNS CRITÉRIOS DE DIVISIBILIDADE

A seguir apresentaremos alguns critérios de divisibilidade e suas respectivas demonstrações. Para isso, seja $m = a_n a_{n-1} \ldots a_1 a_0$, um número inteiro positivo cuja expressão na base 10 é

$$m = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10^1 + a_0, \tag{6}$$

onde a_i, com $i \in \{0,1,\cdots,n\}$, representa os algarismos de m.

Teorema 2.12 (Divisibilidade por 2)**.** *Um número é divisível por 2 se o algarismo das unidades for divisível por 2, mais precisamente* $a_0 \in \{0,2,4,6,8\}$*.*

Demonstração. Seja m um inteiro positivo, da forma dada em (6). Como $10 = 2\cdot 5$, podemos reescrever esta expressão como

$$m = a_n(2\cdot 5)^n + a_{n-1}(2\cdot 5)^{n-1} + \cdots + a_1(2\cdot 5)^1 + a_0; \tag{7}$$

Colocando em evidência o número 2 da expansão (7), temos

$$m = 2\cdot(a_n 2^{n-1}5^n + a_{n-1}2^{n-2}5^{n-1} + \cdots + a_1 5^1) + a_0.$$

Seja $k = a_n 2^{n-1}5^n + a_{n-1}2^{n-2}5^{n-1} + \cdots + a_1 5^1$, então podemos representar m da forma

$$m = 2k + a_0,$$

como a_0 é um algarismo, vamos analisar cada caso:
$a_0 = 0 \Rightarrow m = 2k \Rightarrow 2|m$,
$a_0 = 1 \Rightarrow m = 2k+1 \Rightarrow 2 \nmid m$,
$a_0 = 2 \Rightarrow m = 2k+2 = 2\cdot(k+1) \Rightarrow 2|m$,
$a_0 = 3 \Rightarrow m = 2k+3 = 2\cdot(k+1)+1 \Rightarrow 2 \nmid m$,

$a_0 = 4 \Rightarrow m = 2k+4 = 2\cdot(k+2) \Rightarrow 2|m$,
$a_0 = 5 \Rightarrow m = 2k+5 = 2\cdot(k+2)+1 \Rightarrow 2 \nmid m$,
$a_0 = 6 \Rightarrow m = 2k+6 = 2\cdot(k+3) \Rightarrow 2|m$,
$a_0 = 7 \Rightarrow m = 2k+7 = 2\cdot(k+3)+1 \Rightarrow 2 \nmid m$,
$a_0 = 8 \Rightarrow m = 2k+8 = 2\cdot(k+4) \Rightarrow 2|m$,
$a_0 = 9 \Rightarrow m = 2k+9 = 2\cdot(k+4)+1 \Rightarrow 2 \nmid m$. Portanto, 2 divide m se o algarismo das unidades for $a_0 = 0,2,4,6$ ou 8. □

Para definirmos o critério de divisibilidade por 3 e respectivamente por 9, é necessário o lema a seguir.

Lema 2.13. *Seja $n \in \mathbb{Z}$ com $n \geq 1$. Então, existe $q \in \mathbb{N}$ tal que $10^n = 9q+1$.*

Demonstração. Demonstraremos por indução. Para $n = 1$, temos que

$$10^1 = 9\cdot 1 + 1,$$

e portanto o resultado é válido para o passo base. Agora suponha que $10^n = 9q+1$ é válido para $n \in \mathbb{N}$, provaremos que o resultado também é válido para $n+1$. Da hipótese de indução, multiplicamos ambos os lados por 10, logo

$$10^{n+1} = (9q+1)\cdot 10 = 90q+10 = 90q+9+1 = 9\cdot(10q+1)+1,$$

mostrando que o resultado é válido para $n+1$ e, consequentemente, para todo $n \in \mathbb{N}$. □

Observação 2.14. *Do Lema 2.13 podemos concluir que se $10^n = 9q+1$ é válido para todo $n \in \mathbb{N}$, também será válido que $10^n = 3(3q)+1$ e portanto $10^n = 3q'+1$, para todo $n \in \mathbb{N}$.*

Teorema 2.15 (Divisibilidade por 3)**.** *Um número inteiro será divisível por 3 se, e somente se, a soma dos valores absolutos de seus algarismos for divisível por 3.*

Demonstração. Seja m um inteiro positivo cuja expressão na base 10 é

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

Pelo Lema 2.13, podemos reescrever m da seguinte maneira

$$\begin{aligned} m &= a_n(3q_n+1) + a_{n-1}(3q_{n-1}+1) + \cdots + a_1(3q_1+1) + a_0 \\ &= 3a_nq_n + a_n + 3a_{n-1}q_{n-1} + a_{n-1} + \cdots + 3a_1q_1 + a_1 + a_0 \\ &= 3\cdot(a_nq_n + a_{n-1}q_{n-1} + \cdots + a_1q_1) + (a_n + a_{n-1} + \cdots + a_1 + a_0). \end{aligned}$$

Seja $k = a_n q_n + a_{n-1} q_{n-1} + \cdots + a_1 q_1$. Então escrevemos m da forma

$$m = 3k + (a_n + a_{n-1} + \cdots + a_1 + a_0). \tag{8}$$

Suponha que m seja divisível por 3. Então $m = 3q$, para algum $q \in \mathbb{Z}$. Usando a representação dada em (8), temos que $a_n + a_{n-1} + \cdots + a_1 + a_0 = 3(q-k)$, com $q-k \in \mathbb{Z}$, mostrando que $a_n + a_{n-1} + \cdots + a_1 + a_0$ é divisível por 3.

Reciprocamente, se $a_n + a_{n-1} + \cdots + a_1 + a_0$ é divisível por 3, temos que $a_n + a_{n-1} + \cdots + a_1 + a_0 = 3k'$, com $k' \in \mathbb{Z}$. Pela representação (8), temos que

$$m = 3k + 3k' = 3(k + k'),$$

mostrando que m é divisível por 3.

□

A seguir, para exemplificar o critério de divisibilidade por 3, segue uma questão trabalhada no aplicativo *Teoria dos Números - Quiz Show*.

Exemplo 2.16. *Sabendo-se que o número* $15d2$ *é um número divisível por 3, use o critério de divisibilidade por 3 para concluir que uma das alternativas abaixo é uma possibilidade para o algarismo* d*:*

a) 1

b) 2

c) 3

d) 5

Solução. *É dado que o número* $15d2$ *é divisível por* 3*, logo a soma dos algarismos deve ser um número divisível por 3. Como*

$$1 + 5 + d + 2 = 8 + d,$$

então $8 + d$ *deve ser um número múltiplo de três. Testando os possíveis valores para o algarismo* d*, temos:*
$d = 0 \Rightarrow 8 + 0 = 8$*, e 8 não é divisível por 3;*
$d = 1 \Rightarrow 8 + 1 = 9$*, e 9 é divisível por 3;*
$d = 2 \Rightarrow 8 + 2 = 10$*, e 10 não é divisível por 3;*

$d = 3 \Rightarrow 8+3 = 11$, *e 11 não é divisível por 3;*
$d = 4 \Rightarrow 8+4 = 12$, *e 12 é divisível por 3;*
$d = 5 \Rightarrow 8+5 = 13$, *e 13 não é divisível por 3;*
$d = 6 \Rightarrow 8+6 = 14$, *e 14 não é divisível por 3;*
$d = 7 \Rightarrow 8+7 = 15$, *e 15 é divisível por 3;*
$d = 8 \Rightarrow 8+8 = 16$, *e 16 não é divisível por 3;*
$d = 9 \Rightarrow 8+9 = 17$, *e 17 não é divisível por 3.*

Logo o valor de d será 1, 4 ou 7. Assim a única alternativa que contém um destes valores é a alternativa a).

Apresentamos agora um critério para identificar quando um número é divisível por 5.

Teorema 2.17 (Divisibilidade por 5)**.** *Um número será divisível por 5 se, e somente se, o algarismo das unidades for 0 ou 5.*

Demonstração. Seja m um inteiro positivo. Temos que sua expressão na base 10 é

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

onde $a_i \in \mathbb{Z}$, com $i = 0, 1, \cdots, n$. Note que $10 = 2 \cdot 5$, assim podemos reescrever a expressão como

$$m = a_n (2 \cdot 5)^n + a_{n-1} (2 \cdot 5)^{n-1} + \cdots + a_1 (2 \cdot 5)^1 + a_0,$$

isto é,

$$m = 5 \cdot (a_n 2^n 5^{n-1} + a_{n-1} 2^{n-1} 5^{n-2} + \cdots + a_1 2^1) + a_0.$$

Se $k = a_n 2^n 5^{n-1} + a_{n-1} 2^{n-1} 5^{n-2} + \cdots + a_1 2^1$, então

$$m = 5k + a_0. \tag{9}$$

Suponha inicialmente que m é divisível por 5. Então temos que $m = 5q$, onde $q \in \mathbb{Z}$. Logo $5q = 5k + a_0$, o que implica $a_0 = 5(q-k)$, onde $q - k \in \mathbb{Z}$, e portanto a_0 é divisível por 5. Mas os únicos números entre 0 e 9 divisíveis por 5 são 0 e o próprio 5. Isso mostra que $a_0 = 0$ ou $a_0 = 5$.

Reciprocamente, suponha que $a_0 = 0$ ou $a_0 = 5$ e considere m com a representação da forma (9). Se $a_0 = 0$, então $m = 5k$ e temos o desejado. Se $a_0 = 5$, então $m = 5(k+1)$, mostrando que m é divisível por 5.

□

O próximo exemplo é uma questão encontrada no aplicativo *Teoria dos Números - Quiz Show*, para trabalharmos os critérios de divisibilidade por 5.

Exemplo 2.18. *Qual número abaixo é divisível por 5:*

a) 51025

b) 541269

c) 25413

d) 12031

Solução. *Pelo Teorema 2.17, um número é divisível por 5 se, somente se, o algarismo das unidades for zero ou 5. Logo a única alternativa que apresenta esta característica é* ***a) 51025****.*

Teorema 2.19 (Divisibilidade por 9)**.** *Um número $m \in \mathbb{Z}$ é divisível por 9 se, somente se, a soma dos valores de seus algarismos for divisível por 9.*

Demonstração. Seja m um inteiro positivo e considere sua expressão na base 10:

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

onde $a_i \in \mathbb{Z}$, com $i = 0, 1, \cdots, n$. Note que, pelo Lema 2.13, podemos reescrever m da seguinte maneira

$$\begin{aligned} m &= a_n(9q_n + 1) + a_{n-1}(9q_{n-1} + 1) + \cdots + a_1(9q_1 + 1) + a_0 \\ &= 9a_nq_n + a_n + 9a_{n-1}q_{n-1} + a_{n-1} + \cdots + 9a_1q_1 + a_1 + a_0 \\ &= 9 \cdot (a_nq_n + a_{n-1}q_{n-1} + \cdots + a_1q_1) + (a_n + a_{n-1} + \cdots + a_1 + a_0). \end{aligned}$$

Denotando $k' = a_nq_n + a_{n-1}q_{n-1} + \cdots + a_1q_1$, temos

$$m = 9k' + (a_n + a_{n-1} + \cdots + a_1 + a_0)$$

sendo assim, 9 divide m se, somente se, $9|(a_n + a_{n-1} + \cdots + a_1 + a_0)$ onde $a_n + a_{n-1} + \cdots + a_1 + a_0$ representa a soma dos algarismo do número m. □

Exemplo 2.20. *O número* $12ab$*, onde a e b são os algarismos de dezena e unidade, respectivamente, é um número divisível por 9. O valor máximo da soma dos algarismos* $a + b$ *será de:*

a) 17

b) 15

c) 16

d) 20

Solução: *Sabendo que o número* $12ab$ *é divisível por 9, a soma de seus algarismos deve ser um número divisível por 9. Assim, temos que* $1+2+a+b = 3+a+b$ *deve ser divisível por 9. Para selecionarmos os valores dos algarismos a e b, devemos nos atentar que buscamos a maior soma possível de a e b. Se escolhermos* $a = 3$ *e* $b = 3$ *obteremos o número* 1233*, onde*

$$1+2+3+3 = 9,$$

sendo portanto 1233 divisível por 9. Como não sabemos se essa é a maior soma possível, para continuar a solução devemos fazer uma análise com os maiores valores para os algarismos a e b, sendo assim

$$a = 9 \text{ e } b = 9 \Rightarrow 3+9+9 = 21,$$

não é divisível por 9. Diminuindo o valor de a,

$$a = 8 \text{ e } b = 9 \Rightarrow 3+8+9 = 20, \text{ não é divisível por 9;}$$
$$a = 7 \text{ e } b = 9 \Rightarrow 3+7+9 = 19, \text{ não é divisível por 9;}$$
$$a = 6 \text{ e } b = 9 \Rightarrow 3+6+9 = 18 \text{ é divisível por 9.}$$

Como encontramos para $a = 6$ *e* $b = 9$ *um resultado divisível por 9, o número formado por estes algarismos é 1269, onde o resultado de* $a+b$ *será 15.*

Notação 2.21. *Representamos por* $D(a)$ *o conjunto dos divisores positivos do número inteiro a.*

Exemplo 2.22. *Para o número 28, temos* $D(28) = \{1,2,4,7,14,28\}$.

2.3 MDC, MMC E ALGORITMO DE EUCLIDES

Apresentamos agora a teoria básica referente a conceitos essenciais em teoria dos números, como o máximo divisor comum, mínimo múltiplo comum e o Algoritmo de Euclides.

2.3.1 MÁXIMO DIVISOR COMUM

Definição 2.23. *Sejam $a,b \in \mathbb{Z}$. Um número $d \in \mathbb{Z}$ é considerado um divisor comum de a e b se $d|a$ e $d|b$. Generalizando, definimos um divisor comum d dos n números inteiros $a_1, a_2, \ldots, a_n$ se $d|a_1, d|a_2, \ldots, d|a_n$.*

Notação 2.24. *Representamos por $D(a,b)$ o conjunto dos divisores positivos comuns dos números inteiros a e b.*

Exemplo 2.25. *Obtenha o conjunto dos divisores comuns de 36 e 48.*
Solução. *Temos que*

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

e

$$D(48) = \{1,2,3,4,6,8,12,16,24,48\}.$$

Logo, $D(36) \cap D(48) = \{1,2,3,4,6,12\}$. ou ainda, representado por

$$D(36,48) = \{1,2,3,4,6,12\}.$$

Definição 2.26. *Denominamos o máximo divisor comum (mdc) dos números inteiros a e b como o maior de seus divisores, isto é,*

$$mdc(a,b) = max\, D(a,b).$$

Generalizando $mdc(a_1, \ldots, a_n) = max\, D(a_1, \ldots, a_n)$.

Observação 2.27. *É evidente que dados n números inteiros, sempre existirá pelo menos um divisor comum a todos eles, já que o número 1 é divisor comum de todos os inteiros.*

Proposição 2.28. *Dados números inteiros $a_1, \cdots, a_n$, não todos nulos, existe o seu mdc e*

$$mdc(a_1, \cdots, a_n) = mdc(a_1, \cdots, a_{n-2}, mdc(a_{n-1}, a_n)).$$

Demonstração. Pode ser encontrada em (HEFEZ, 2014) página 98. □

Exemplo 2.29. *Do Exemplo 2.25, concluímos que o máximo divisor comum entre 36 e 48 é $mdc(36,48) = 12$.*

Lema 2.30. *Sejam $a,b,t \in \mathbb{Z}$. Então, $mdc(a,b) = mdc(a-tb,b)$.*

Demonstração. Se $d = mdc(a,b)$ temos que $d|a$ e $d|b$, logo pela Proposição 2.3(vi) segue que $d|(a-tb)$ e portanto $d|mdc(a-tb,b)$. E ainda seja $d' = mdc(a-tb,b)$ temos que $d'|(a-$

tb) e $d'|b$ logo $d'|(a-tb+tb)$, pela Proposição 2.3(iv), ou seja, $d'|a$, portanto $d' = mdc(a-tb,b)|mdc(a,b)$.

Como $d|d'$ e $d'|d$, concluímos que $mdc(a,b) = mdc(a-tb,b)$. □

Teorema 2.31. *Sejam $a,b \in \mathbb{Z}$. Então existem inteiros x e y tais que*

$$ax+by = mdc(a,b).$$

Demonstração. Como o resultado é uma combinação linear de a e b, considere o conjunto

$$\mathbb{X} = \{ax+by \mid x,y \in \mathbb{Z} \quad \text{e} \quad ax+by \geq 0\}.$$

Seja $m = ax+by$ o menor elemento positivo de $\mathbb{X}$. Pelo algoritmo da divisão euclidiana $a = mq+r$, com $0 \leq r < m$ e $q,r \in \mathbb{Z}$. Então

$$r = a-mq = a-(ax+by)q = a-qax-qby = a(1-x)+b(yq).$$

Observe que $(1-x)$, $yq \in \mathbb{Z}$, logo $r \in \mathbb{X}$, porém note que $r < m$ e m é o menor elemento de $\mathbb{X}$, logo temos uma contradição e podemos concluir que $r = 0$ e $a = mq$, ou seja, $m|a$. Escrevendo $b = mq'+r'$, com $0 \leq r' < m$ e $q',r' \in \mathbb{Z}$, obtemos de maneira análoga que $m|b$.

Note que se $d = mdc(a,b)$, isso significa que $d|a$ e $d|b$, assim podemos representar $a = q_1 d$ e $b = q_2 d$, e assim, podemos reescrever como

$$m = q_1 dx + q_2 dy = d \cdot (q_1 x + q_2 y)$$

assim, $d|m$ ocasionando que $d \leq m$, pelo fato de $m > 0$. Mas como $m|a$, $m|b$ e $d \leq m$, só podemos concluir que $d = m$, logo

$$ax+by = mdc(a,b).$$

□

Observação 2.32. *Dados $a,b \in \mathbb{Z}$, dizemos que a e b são primos entre si, ou coprimos, se o $mdc(a,b) = 1$; Ou em outras palavras, se o único divisor comum positivo de a e b for 1.*

O exemplo abaixo é a questão trabalhada no aplicativo *Teoria dos Números - Quiz Show*, onde abordamos o conceito de primos entre si, ou coprimos.

Exemplo 2.33. *Dizemos que dois números naturais são denominados números primos entre si, quando apresentam como único divisor comum o número 1. Sendo assim qual dos itens abaixo apresenta um exemplo de número primo entre si?*

a) 20 e 25

b) 6 e 18

c) 25 e 26

d) 40 e 60

Solução. *Note que*

a) $D(20) = \{1,2,4,5,10,20\} \quad e \quad D(25) = \{1,5\}$

perceba que além do número 1, o número 5 é um divisor comum entre 20 e 25, logo não são primos entre si.

b) $D(6) = \{1,2,3,6\} \quad e \quad D(18) = \{1,2,3,6,9,18\}$

perceba que além do número 1, os números 2, 3 e 6 também são divisores comuns de 6 e 18 logo não são primos entre si.

c) $D(25) = \{1,5\} \quad e \quad D(26) = \{1,2,13\}$

note que somente o número 1 é divisor comum entre 25 e 26, logo estes números são primos entre si.

d) $D(40) = \{1,2,4,5,8,10,20,40\} \quad e \quad D(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$

perceba que além do número 1, os números 2, 4, 5, 10 e 20 também são divisores comuns de 40 e 60, logo não são primos entre si.

O próximo resultado apesar de simples, se mostra muito útil em teoria dos números, principalmente em demonstrações.

Teorema 2.34 (Teorema de Euclides)**.** *Sejam a, b e c inteiros positivos, tais que $a|bc$ e $mdc(a,b) = 1$, então $a|c$.*

Demonstração. Dado que $mdc(a,b) = 1$, pelo Teorema 2.31, existem inteiros x e y, tais que

$$ax + by = 1.$$

Multiplicando a igualdade acima por c, temos que $acx + bcy = c$. Ainda, temos por hipótese que $a|bc$ e, pela Proposição 2.3, que $a|ac$. Logo, $a|(bcy + acx)$, para $x, y \in \mathbb{Z}$. Portanto $a|c$. $\square$

2.3.2 ALGORITMO DE EUCLIDES

A seguir apresentaremos um método bastante prático para determinar o máximo divisor comum de dois números inteiros. Tal método foi apresentado por *Euclides* em sua obra *Elementos* (para uma abordagem da obra Elementos de Euclides, ver (HEATH, 1956)) porém evidências históricas indicam que este método é anterior à Euclides.

Lema 2.35. *Sejam $a,b \in \mathbb{Z}$, com $b \neq 0$, q e r o quociente e o resto da divisão de a por b, respectivamente. Então, $D(a,b) = D(b,r)$ e além disso $mdc(a,b) = mdc(b,r)$.*

Demonstração. Para realizarmos esta demonstração, mostraremos que $D(a,b) \subset D(b,r)$ e $D(b,r) \subset D(a,b)$, consequentemente $D(a,b) = D(b,r)$.

Pela divisão euclidiana podemos escrever $a = bq + r$, considerando $b < a$. Seja $y \in D(a,b)$. Então, $y|a$ e $y|b$. Note que $r = a - bq$ e como y divide cada um dos fatores, pela Proposição 2.3 *(vi)*, temos que $y|r$. Portanto, $y|b$ e $y|r$, isto é, $y \in D(b,r)$. Assim mostramos que $D(a,b) \subset D(b,r)$. Mostraremos agora que um elemento $t \in D(b,r)$ qualquer, também pertence a $D(a,b)$. Se t pertence ao conjunto de divisores comuns de b e r, temos que $t|b$ e $t|r$, e como $r = a - bq$, segue que $t|(a - bq)$. Concluímos assim que $t|a$, pois $a = a - bq + bq$ e portanto $t \in D(a,b)$.

Finalmente, se os conjuntos de divisores comuns são iguais, logo seus máximos divisores são iguais, isto é, $mdc(a,b) = mdc(b,r)$. □

Note que do Lema 2.35 concluímos que encontrar o $mdc(a,b)$ é equivalente a encontrar o $mdc(b,r)$, que é o mesmo que o $mdc(r,r_1)$, o mesmo que o $mdc(r_1,r_2)$ e assim sucessivamente. Ou seja, repetindo esse processo das divisões sucessivas, teremos

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 \leq r_1 < |b|. \\
b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1. \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2. \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1}. \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Observe que os restos das divisões diminuem a cada passo e o resto é um inteiro maior ou igual a zero, logo podemos concluir que em algum momento encontraremos resto zero nas

divisões. Suponha que r_{n+1} seja o primeiro resto nulo. Do Lema 2.35, temos que

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots = mdc(r_{n-1},r_n),$$

onde $r_n | r_{n-1}$, e assim temos que $mdc(r_{n-1},r_n) = r_n$. Desta maneira, demonstramos que o máximo divisor comum entre dois números inteiros é o último resto diferente de zero.

Exemplo 2.36. *Determine o Máximo Divisor Comum entre 200 e 355.*

Solução. Apliquemos o Algoritmo de Euclides das divisões sucessivas até obtermos resto zero:

$$\begin{array}{r|l} 355 & 200 \\ \underbrace{155}_{resto} & 1 \end{array} \qquad \begin{array}{r|l} 200 & 155 \\ \underbrace{45}_{resto} & 1 \end{array} \qquad \begin{array}{r|l} 155 & 45 \\ \underbrace{20}_{resto} & 3 \end{array} \qquad \begin{array}{r|l} 45 & 20 \\ \underbrace{5}_{resto} & 2 \end{array} \qquad \begin{array}{r|l} 20 & 5 \\ \underbrace{0}_{resto} & 4 \end{array}$$

Após aplicarmos o Algoritmo de Euclides, verificamos que o último resto antes de zero é 5, portanto $mdc(200,355) = 5$.

Agora será apresentado um método prático para aplicar o *Algoritmo de Euclides*.

Ao dividir a por b, com q e r representando o quociente e o resto desta divisão, respectivamente, podemos montar uma "grade" com estes resultados, como abaixo:

Quociente $\rightarrow$		q	
	a	b	
Resto $\rightarrow$	r		

Assim será fácil dispor os quocientes e os restos das divisões até obter o resto zero. Então o processo do cálculo do $mdc = (a,b)$ ficará:

Quociente $\rightarrow$		q_1	q_2	q_3	$\cdots$	$\cdots$	q_n	q_{n+1}
	a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	r_n
Resto $\rightarrow$	r_1	r_2	r_3	$\cdots$	$\cdots$	r_n	0	

O próximo exemplo é uma questão do aplicativo desenvolvido, na resolução ficará claro como é útil o *Algoritmo de Euclides* para resolver problemas do tipo a seguir.

Exemplo 2.37. *Ciro é um lenhador muito experiente, que acabou de cortar três toras de madeira, uma com 16 metros de comprimento, outra com 20 metros e a terceira com impressionantes 36 metros. Ciro precisa cortar as toras em pedações menores, porém ele deve cortar no maior tamanho possível e todas com o mesmo comprimento. Assim o comprimento de cada tora e a quantidade de toras serão:*

a) 5 metros cada uma, obtendo um total de 10 toras;

b) 4 metros cada uma, obtendo um total de 18 toras;

c) 4 metros cada uma, obtendo um total de 26 toras;

d) 7 metros cada uma, obtendo um total de 18 toras;

Solução. *Ciro precisa cortar as toras com o máximo tamanho que conseguir e de maneira igual (comum) entre os comprimentos da tora, sendo assim devemos achar o máximo divisor comum entre 16, 20 e 36, isto é* $mdc(16,20,36)$. *Pela Proposição (2.28), temos que*

$$mdc(a,b,c) = mdc(mdc(a,b),c)$$

logo

$$mdc(16,20,36) = mdc(mdc(16,20),36).$$

Assim calcularemos o $mdc(16,20)$ *usando o Algoritmo de Euclides:*

Primeiramente construímos uma grade com os números 16 e 20 em ordem decrescente (do maior para o menor), onde devemos efetuar a divisão de 20 por 16 e ir anotando os resultados (quocientes na primeira linha), e os restos na terceira linha:

Quociente $\rightarrow$		1		
	20	16		
Resto $\rightarrow$	4			

Como o resto ainda não é igual a zero, devemos agora dividir 16 pelo resto 4:

Quociente $\rightarrow$		1	4	
	20	16	4	
Resto $\rightarrow$	4	0		

Logo, o $mdc(16,20) = 4$.

Agora podemos calcular

$$mdc(16,20,36) = mdc((16,20),36) = mdc(4,36)$$

Aplicando o Algoritmo de Euclides novamente para o calculo $mdc(4,36)$*:*

Quociente →		9	
	36	4	
Resto →	0		

Concluímos que o $mdc(4,36) = 4$*, sendo assim:*

$$mdc(16,20,36) = 4.$$

Então o lenhador Ciro deve cortar suas toras com o comprimento de 4 metros cada uma, sendo assim as toras serão divididas por 4.

1ª Tora de 16 m dividida por 4 é igual a 4 toras menores cada uma com 4 metros.

2ª Tora de 20 m dividida por 4 é igual a 5 toras menores cada uma com 4 metros.

3ª Tora de 36 m dividida por 4 é igual a 9 toras menores cada uma com 4 metros.

Logo, Ciro terá toras de 4 metros cada uma, obtendo um total de 18 toras menores (4+5+9).

Exemplo 2.38. *Dona Sônia cria galinhas poedeiras e suas galinhas produzem ovos pequenos, médios e grandes. Num certo dia, Dona Sônia coletou 120 ovos pequenos, 200 médios e 380 grandes. Se Dona Sônia pretende embalar estes ovos de maneira que não haja tamanhos misturados e que as embalagens tenham o maior número possível de ovos, todos com a mesma quantidade, qual deve ser o número de ovos de cada embalagem?*

a) 36 ovos em cada embalagem;

b) 35 ovos em cada embalagem;

c) 20 ovos em cada embalagem;

d) 22 ovos em cada embalagem.

Solução. *Para resolver o problema de Dona Sônia devemos perceber que ela precisa do máximo de ovos distribuídos em embalagens com a mesma quantidade e com ovos de mesmo tamanho, logo devemos encontrar o máximo divisor comum entre 120, 200 e 380, isto é,* $mdc(120,200,380)$.

Pela Proposição (2.28), temos que

$$mdc(120,200,380) = mdc(mdc(120,200),380)$$

Assim devemos primeiramente calcular $mdc(120,200)$ *usando o Algoritmo de Euclides: inicialmente construímos uma grade com os números 120 e 200 em ordem decrescente (do maior para o menor), onde devemos efetuar a divisão de 200 por 120 e anotar os resultados (quocientes na primeira linha), e os restos na terceira linha:*

Quociente →		1				
	200	120				
Resto →	80					

Como o resto ainda não é igual à zero, devemos agora dividir 120 pelo resto 80:

Quociente →		1	1			
	200	120	80			
Resto →	80	40				

E assim repetimos as divisões pelos restos até encontrar resto zero:

Quociente →		1	1	2		
	200	120	80	40		
Resto →	80	40	0			

Note que quando efetuada a última divisão por 40, encontramos resto igual à zero, assim o $mdc(120,200) = 40$*. Agora devemos calcular o* $mdc(40,380)$*, usando o Algoritmo de Euclides da mesma forma como feito anteriormente:*

Quociente →		9	1			
	380	40	20			
Resto →	20	0				

Como na última divisão por 20 obtemos resto zero, logo o $mdc(40,380) = 20$*, e consequentemente:*

$$mdc(120,200,380) = 20.$$

Isso nos mostra que a maior distribuição comum da quantidade de ovos será 20. Então, Dona Sônia deverá colocar 20 ovos de cada qualidade em cada embalagem.

Lema 2.39. *Dados* $a,b \in \mathbb{Z}$ *não-nulos e* $mdc(a,b) = d$*, tal que* $a = dk_1$ *e* $b = dk_2$*, então* $mdc(k_1,k_2) = 1$.

Demonstração. Suponhamos que $mdc(k_1,k_2)=t$, com $t>1$. Assim teremos que

$$t|k_1 \Longrightarrow k_1 = t\alpha_1 \overset{k_1=\frac{a}{d}}{\Longrightarrow} a = dt\alpha_1 \Longrightarrow dt|a$$

e

$$t|k_2 \Longrightarrow k_2 = t\alpha_2 \overset{k_2=\frac{b}{d}}{\Longrightarrow} b = dt\alpha_2 \Longrightarrow dt|b.$$

Assim podemos concluir que dt é um divisor comum de a e b, e por hipótese temos que $t>1$, logo podemos concluir que $dt>d$, que é um absurdo já que d é o maior divisor comum de a e b. Portanto $mdc(k_1,k_2)=1$. □

2.3.3 MÍNIMO MÚLTIPLO COMUM

Definição 2.40. *Sejam $a,b\in\mathbb{Z}$ não-nulos. Dizemos que $t\in\mathbb{Z}$ é um múltiplo comum de a e b, se $a|t$ e $b|t$. Indicaremos os múltiplos comuns positivos de a e b por $M(a,b)$.*

Definição 2.41. *É denominado mínimo múltiplo comum de inteiros não-nulos a e b, e indicado por $mmc(a,b)=m$, o menor inteiro positivo que é divisível por a e b ao mesmo tempo. Equivalentemente, o $mmc(a,b)$ é um inteiro positivo m tal que:*

(i) $a|m$ *e* $b|m$*;*

(ii) Se existir $m'\in\mathbb{Z}$*, tal que* $a|m'$ *e* $b|m'$*, então* $m|m'$*.*

Ainda consideramos o inteiro positivo m o mínimo múltiplo comum dos inteiros $a_1,a_2,a_3,\cdots,a_n$, se m for um múltiplo comum de $a_1,a_2,a_3,\cdots,a_n$ e ainda para todo múltiplo comum m' de $a_1,a_2,a_3,\cdots,a_n$, ocorrer que $m|m'$.

Exemplo 2.42. *Para encontrarmos o $mmc(6,10)$, note que*

$$A = \textit{múltiplos de 6 : } \{0,6,12,18,24,30,36,42,48,\ldots\}$$
$$B = \textit{múltiplos de 10: } \{0,10,20,30,40,50,60,70,\ldots\},$$

e o menor elemento do conjunto interseção $A\cap B$ é 30, logo $mmc(6,10)=30$.

Teorema 2.43. *Sejam a e b dois números inteiros. Então, $mmc(a,b)\cdot mdc(a,b)=|ab|$.*

Demonstração. Consideremos o caso onde a e b são positivos, e assim $|ab|=ab$. Seja $mmc(a,b)=m$ e $mdc(a,b)=d$, então

$$mdc(a,b)=d \Longrightarrow d|a \quad \text{e} \quad d|b \Longrightarrow d|ab \Longrightarrow \frac{ab}{d}=t. \tag{10}$$

Agora basta provar que $t = mmc(a,b) = m$. Para isso, usaremos a Definição 2.41 de mínimo múltiplo comum.

Como $mdc(a,b) = d$, podemos escrever $a = k_1 d$ e $b = k_2 d$, de (10) podemos reescrever $t = k_1 b$ e $t = ak_2$. Segue imediatamente que $a|t$ e $b|t$, satisfazendo a condição *(i)* da definição de mínimo múltiplo comum.

Seja agora $m_1 \in \mathbb{Z}$ um múltiplo comum de a e b, isto é $a|m_1$ e $b|m_1$. Então existe $q \in \mathbb{Z}$ tal que $m_1 = aq$. Substituindo $a = k_1 d$ na ultima igualdade anterior, teremos $m_1 = k_1 dq$. Ainda, $b|m_1$, isto é, $k_2 d|k_1 dq$, logo, $k_2|k_1 q$. Do Lema 2.39, $mdc(k_1,k_2) = 1$, e do Teorema 2.34 podemos concluir que $k_2|q$. Assim $q = k_2 x$, e substituindo na equação de $m_1 = k_1 dq$, temos que $m_1 = k_1 dk_2 x$. Ainda de (10), temos

$$a = k_1 d \quad \text{e} \quad b = k_2 d \Longrightarrow t = \frac{k_1 dk_2 d}{d} = k_1 dk_2. \tag{11}$$

Portanto de (11), obtemos $m_1 = tx$, e segue que $t|m_1$. Assim é verificado a condição *(ii)* da definição de mínimo múltiplo comum. □

A seguir, um exemplo abordado no aplicativo desenvolvido neste trabalho.

Exemplo 2.44. *Seja x um número natural tal que $mmc(20,x) = 140$ e $mdc(20,x) = 5$. Qual é o valor de x?*

Solução. *Usando a Proposição 2.43 e utilizando os dados do enunciado, temos*

$$\begin{aligned} mmc(20,x) \cdot mdc(20,x) &= |20 \cdot x| \\ 140 \cdot 5 &= |20x| \\ 700 &= 20x \\ x &= \frac{700}{20} \\ x &= 35. \end{aligned}$$

2.4 NÚMEROS PRIMOS

Os números primos são objetos de estudo de várias áreas da matemática, e suas aplicações são diversas, como a criptografia.

Definição 2.45. *Seja p um número inteiro maior ou igual a 1. Dizemos que p é primo se tal número possuir apenas dois divisores positivos, a saber, 1 e o próprio número p. Caso contrário, dizemos que o número é composto.*

Exemplo 2.46. *O número 20 é um número composto, já que seus divisores são 1, 2, 4, 5, 10 e o próprio 20. Já o número 13 é considerado primo, pois seus únicos divisores são 1 e o próprio 13.*

Proposição 2.47. *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Suponha que $p|ab$ e $p \nmid a$. Assim, temos que $mdc(p,a) = 1$, e do Teorema de Euclides (Teorema 2.34), podemos concluir que $p|b$. □

Corolário 2.48. *Se $p, p_1, p_2, \cdots, p_n$ são números primos e, se $p|p_1 p_2 \cdots p_n$, então $p = p_i$ para algum $i = 1, 2, \cdots, n$.*

Demonstração. Usando a Proposição 2.47, indução sobre n e o fato de que, se $p|p_i$, então $p = p_i$ para algum $i = 1, 2, \cdots, n$. □

Teorema 2.49 (*Teorema Fundamental da Aritmética*)**.** *Todo inteiro positivo n maior do que 1, pode ser representado de forma única (a menos da ordem) como produto de fatores primos, isto é,*

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_m,$$

onde $m \geq 1$.

Demonstração. Vamos demonstrar este teorema por indução em n. Se $n = 2$ o resultado é válido pois $2 = 2$. Suponhamos que o resultado seja válido para todo número natural menor que n, e vamos provar que é válido para n. Se n for primo o teorema é válido. Suponhamos então que n seja composto. Logo existem $a, b < n$, tais que $n = a \cdot b$, e como a e b são menores que n, por hipótese de indução existem número primos que representam de forma única a e b, como estes primos não são, necessariamente, distintos, n terá sua representação da forma geral:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_m^{e_m},$$

ficando assim demonstrada a existência. Resta mostrar a unicidade. Suponhamos que existam duas decomposições de n em números primos, isto é,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Note que $p_1|q_1 q_2 \cdots q_s$, ou seja, $p_1|q_j$ para algum j. Suponha sem perda de generalidade que $p_1|q_1$. Como ambos são primos, temos que, $p_1 = q_1$, e assim

$$\frac{n}{p_1} = p_2 \cdots p_r = q_2 \cdots q_s,$$

assim teremos que $1 < \frac{n}{p_1} < n$, ou seja, por hipótese de indução as fatorações $p_2 \cdots p_r$ e $q_2 \cdots q_s$ são idênticas, portanto $r = s$, concluindo que os p_i e q_j são iguais aos pares ($p_1 = q_1, \cdots, p_r = q_s$). □

O próximo exemplo também está disponível no aplicativo *Teoria dos Números - Quiz Show*:

Exemplo 2.50. *Analise os itens abaixo e verifique qual deles representa a fatoração em números primos do número 540.*

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

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

c) $2^4 \cdot 3^5 \cdot 5^{10}$

d) $2^1 \cdot 3^1 \cdot 5^0$

Solução. *Fazendo a decomposição em fatores primos do número 540:*

540	*2*	*(divida 540 por 2)*
270	*2*	*(divida 270 por 2)*
135	*3*	*(divida 135 por 3)*
45	*3*	*(divida 45 por 3)*
15	*3*	*(divida 15 por 3)*
5	*5*	*(divida 5 por 5)*
1	$2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5$	

Assim temos que:

$$540 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^3 \cdot 5.$$

Proposição 2.51. *Seja $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ um número natural. Se b é um divisor positivo de a, então*

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n},$$

onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \ldots, r$.

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

Proposição 2.52. *Se* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ *onde* $p_1, p_2, p_3, \cdots p_n$ *são primos que compõem a fatoração de a e b, então*

$$mmc(a,b) = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_n^{max\{\alpha_n,\beta_n\}}.$$

Demonstração. Pela Proposição 2.51, e, seja $m = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_n^{max\{\alpha_n,\beta_n\}}$, m é um múltiplo comum de a e b, já que $a|m$ e $b|m$. Seja m' um múltiplo comum de a e b, então $m' = p_1^{t_1} \cdots p_n^{t_n}$, com $t_i \geq \alpha_i$ e $t_i \geq \beta_i$ com $1 \leq i \leq n$, onde $t_i \geq max\{\alpha_i, \beta_i\}$. Logo, $m|m'$, o que acarreta $m \leq m'$, assim $mmc(a,b) = p_1^{max\{\alpha_1,\beta_1\}} p_2^{max\{\alpha_2,\beta_2\}} \cdots p_n^{max\{\alpha_n,\beta_n\}}$. □

Segue exemplo de questão elaborada para o aplicativo *Teoria dos Números - Quiz Show* que aborda o cálculo do *mmc* através da decomposição em fatores primos.

Exemplo 2.53. *Os carros de corrida sofrem frequentes manutenções pelos mecânicos responsáveis da montadora. Sr. Valdir é o mecânico responsável por dois carros e sua rotina de manutenção é distribuída da seguinte maneira: o carro A deve passar pela manutenção de 15 em 15 dias e o carro B de 16 em 16 dias. Suponha que hoje Valdir fez as devidas manutenções nos carros A e B. Daqui a quanto tempo Valdir voltará a fazer a manutenção no mesmo dia nos carros de sua equipe?*

a) 240 dias

b) 100 dias

c) 300 dias

d) 340 dias

Solução. *Para responder esta questão devemos procurar o mmc (mínimo múltiplo comum) entre os números 15 e 16:*

15,	16	2
15,	8	2
15,	4	2
15,	2	2
15,	1	3
5,	1	5
1,	1	$2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

Assim temos que $mmc(15,16) = 2^4 \cdot 3 \cdot 5 = 240$*, daí decorrerão 240 dias para que Valdir volte a fazer a manutenção dos dois carros de sua equipe no mesmo dia.*

2.5 EQUAÇÕES DIOFANTINAS LINEARES

Apresentaremos agora a teoria básica sobre Equações Diofantinas lineares, com duas incógnitas, do tipo $aX + bY = c$, com $a, b, c \in \mathbb{Z}$. A condição de existência de solução e a forma geral da solução das equações diofantinas são estudadas nesta seção.

Proposição 2.54. *Sejam $a, b, c \in \mathbb{Z}$ com a e b não-nulos e $d = mdc(a,b)$. A equação diofantina $aX + bY = c$ admite uma solução $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ se, e somente se, $d|c$.*

Demonstração. Suponha que a Equação Diofantina tenha solução inteira, digamos (x_0, y_0). Assim, $ax_0 + by_0 = c$. Note que se $d = mdc(a,b)$, temos que $d|a$ e $d|b$, logo pela Proposição 2.31, teremos que d divide as combinações lineares de a e b. Então, $d|(ax_0 + by_0)$, isto é, $d|c$. Reciprocamente se $d|c$, então existe $k \in \mathbb{Z}$ tal que $c = dk$. Como $d = mdc(a,b)$, pela Proposição 2.31, existem $r, s \in \mathbb{Z}$, tais que

$$ar + bs = d.$$

Multiplicando a igualdade acima por k, teremos

$$ark + bsk = dk = c,$$

e fazendo as devidas substituições, encontramos

$$a(rk) + b(sk) = c,$$

onde $rk, sk \in \mathbb{Z}$, mostrando que a equação tem solução. □

O próximo exemplo é uma das questões do tema *EQUAÇÕES DIOFANTINAS* do aplicativo *Teoria dos Números - Quiz Show*.

Exemplo 2.55. *Qual das Equações Diofantinas abaixo possui solução inteira?*

a) $5X + 15Y = 21$

b) $3X + 42Y = 123$

c) $35X + 120Y = 351$

d) $7X + 56Y = 39$

Solução. *Pela Proposição 2.54, analisaremos cada item desta questão:*

a) $mdc(5,15) = 5$*, e* $5 \nmid 21$*, logo esta equação não possui soluções inteiras.*

b) $mdc(3,42) = 3$*, e* $3|123$*, logo esta equação possui soluções inteiras.*

c) $mdc(35,120) = 5$*, e* $5 \nmid 351$*, logo esta equação não possui soluções inteiras.*

d) $mdc(7,56) = 7$*, e* $7 \nmid 39$*, logo esta equação não possui soluções inteiras.*

Portanto, a solução do exercício é a equação $3X + 42Y = 123$.

Proposição 2.56. *Seja* (x_0, y_0) *uma solução para a Equação Diofantina* $aX + bY = c$*, onde* $mdc(a,b) = 1$*. Então, as soluções* $x, y \in \mathbb{Z}$ *da equação são dadas por:*

$$x = x_0 + tb, \qquad y = y_0 - ta; \qquad t \in \mathbb{Z}.$$

Demonstração. Seja (x,y) uma solução da equação $aX + bY = c$, logo podemos representar a seguinte igualdade

$$\begin{aligned} ax_0 + by_0 &= ax + by = c \\ \Rightarrow ax_0 - ax &= by - by_0 \qquad \cdot(-1) \\ \Rightarrow ax - ax_0 &= by_0 - by \\ \Rightarrow a(x - x_0) &= b(y_0 - y). \end{aligned} \tag{12}$$

Como $mdc(a,b) = 1$, temos

$$b|(x - x_0) \Rightarrow x - x_o = tb, \quad t \in \mathbb{Z}. \tag{13}$$

Substitui $x - x_o$ por tb na igualdade (12), obtemos

$$\begin{aligned} atb &= b(y_0 - y) \\ \Rightarrow at &= y_0 - y. \end{aligned} \tag{14}$$

Portanto, de (13) e (14), concluímos que

$$x = x_0 + tb \quad e \quad y = y_0 - ta, \quad t \in \mathbb{Z}.$$

□

Para exemplificar a teoria, exibimos alguns exemplos que se encontram no aplicativo desenvolvido neste trabalho.

Exemplo 2.57. *Encontre a solução geral da equação*

$$3x + 5y = 60.$$

Solução. *Dada a equação* $3x+5y=60$. *Temos que* $mdc(3,5)=1$ *e* $1|60$, *portanto esta equação possui solução.*

Por investigação podemos concluir que uma solução particular é $x_0=0$ *e* $y_0=12$. *Logo a solução geral será da forma*

$$\begin{cases} x = 5t, \\ y = 12-3t, \end{cases}$$

com $t \in \mathbb{Z}$.

Exemplo 2.58. *Valdir trabalha em um estacionamento no centro de sua cidade e certo dia ele percebeu que haviam no total 186 pneus. Sabendo que ao realizar a contagem haviam motos e carros no local, podemos concluir que o máximo de veículos entre carros e motos neste local é:*

a) 1 carro e 91 motos;

b) 91 carros e 1 moto;

c) 30 carros e 61 motos;

d) 32 carros e 17 motos.

Solução. *Primeiramente como não sabemos o número de cada tipo de veículo, denotaremos a quantidade de carros e motos da seguinte maneira:*

x como sendo o número de motos,
y como sendo o número de carros.

Como cada moto possui 2 pneus e cada carro 4 pneus, podemos dizer que $2x$ *representa o número total de pneus das motos e* $4y$ *o número total de pneus dos carros. Logo*

$$2x+4y=186.$$

Note ainda que, como $mdc(2,4)=2$, *podemos dividir toda a equação por 2, e assim obtemos*

$$x+2y=93.$$

Por investigação encontramos $x_0=1$ *e* $y_0=46$, *pois*

$$1+2\cdot 46=93.$$

Assim a solução geral será dada por

$$\begin{cases} x = 1 + 2t \\ y = 46 - t, \end{cases}$$

com $t \in \mathbb{Z}$*. Ainda perceba que o número de veículos deve ser não-negativo, logo* $1 + 2t \geq 0$ *e* $46 - t \geq 0$*, donde temos que* $0 \leq t \leq 46$.

Como o estacionamento deve conter o máximo de veículos, em nossa equação devemos encontrar o máximo de motos e o mínimo de carros, logo a solução geral $y = 46 - t$ *, deve ser a menor possível, já que y representa o número de carros. Isso ocorre para* $t = 45$*, ou seja,*

$$y = 46 - t = 46 - 45 = 1$$

como $t = 45$*, substituindo na solução geral de x*

$$x = 1 + 2t = 1 + 2 \cdot 45 = 1 + 90 = 91$$

Assim, podemos concluir que no estacionamento podem estar estacionados o máximo de veículos, sendo 1 carro e 91 motos.

3 ESTRUTURA E FUNCIONAMENTO DO APLICATIVO TEORIA DOS NÚMEROS - QUIZ SHOW

Neste capítulo apresentaremos o aplicativo desenvolvido para a dissertação, denominado *Teoria dos Números - Quiz Show*, desenvolvido de forma a se tornar uma ferramenta para auxiliar o ensino de matemática na educação básica. Com este intuito, este aplicativo apresenta uma linguagem adequada a crianças e adolescentes sobre o tema Teoria dos Números, tema de suma importância para a formação matemática dos discentes. Na tentativa de cativar os estudantes, este aplicativo propõem um desafio, na forma de *quiz* que será descrito no decorrer deste capítulo. O aplicativo *Teoria dos Números - Quiz Show* foi desenvolvido na plataforma *Android Studio* disponível no site `https://developer.android.com/studio/index.html?hl=pt-br`.

O aplicativo está disponível para celulares com o sistema Android, e poderá ser baixado através da Play Store, bastando digitar o nome do aplicativo *Teoria dos Números - Quiz Show* no local de busca da loja virtual e realizar a instalação.

Figura 1: Aplicativo disponível na loja virtual *Play Store*.

3.1 APRESENTAÇÃO DO APLICATIVO *TEORIA DOS NÚMEROS - QUIZ SHOW*

Ao iniciar o aplicativo, o jogador se deparará com a tela *Splah Screen*, ou seja, a tela de abertura do aplicativo, como mostra a figura abaixo.

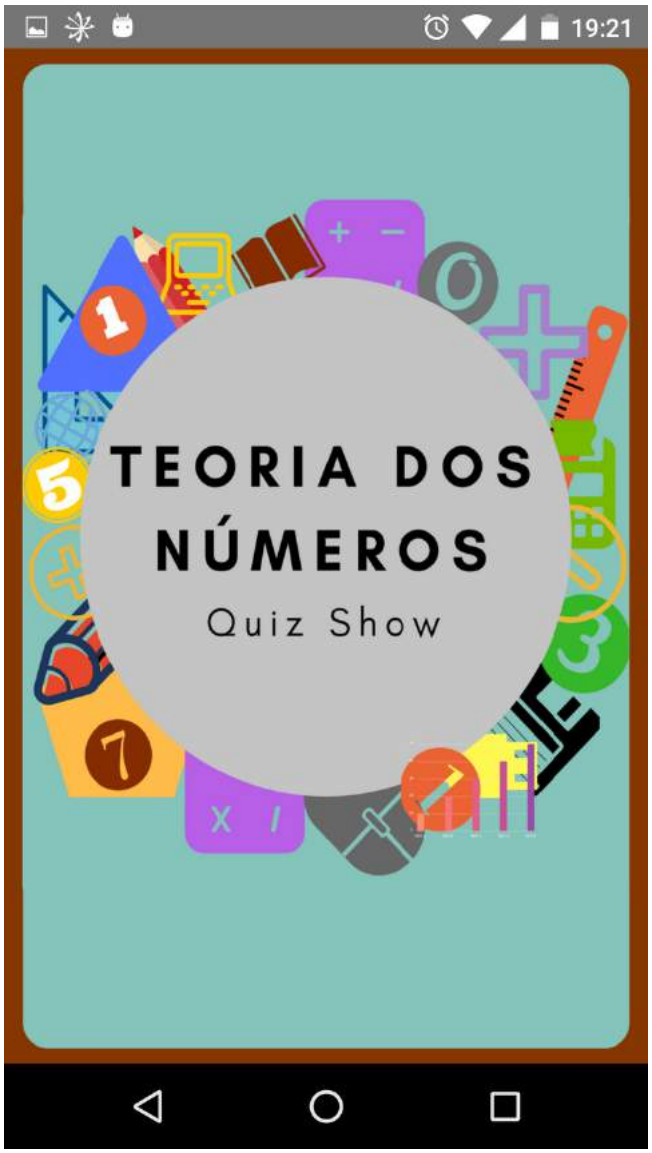


Figura 2: Tela inicial de *Teoria dos Números - Quiz Show*

Automaticamente, após 2 segundos será aberto o menu principal, oferecendo algumas opções ao jogador.

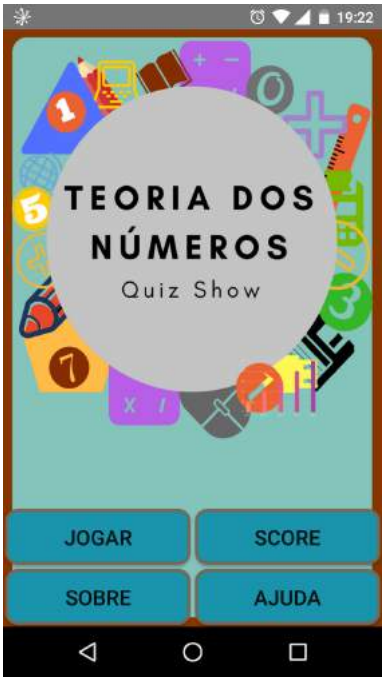


Figura 3: Menu principal de *Teoria dos Números - Quiz Show*.

Ao selecionar a opção *JOGAR*, será aberto um segundo menu, onde estarão presentes os temas referentes à Teoria dos Números direcionados à educação básica.

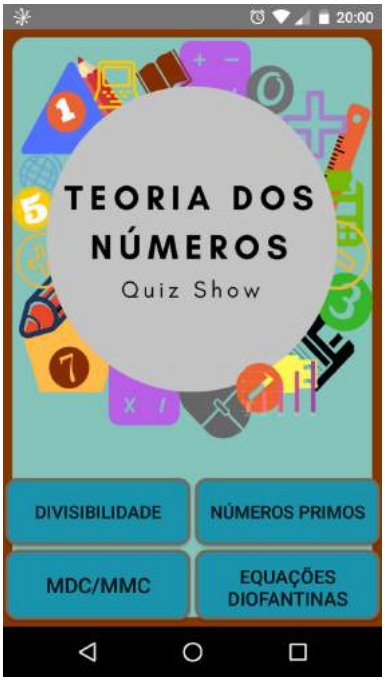


Figura 4: Menu de temas de *Teoria dos Números - Quiz Show*

Para cada tema abordado neste trabalho, foram elaboradas questões a nível de educação básica. Ao iniciar qualquer um dos temas propostos, será iniciada uma rodada com 7 questões

aleatórias sobre o assunto, avaliando o conhecimento do jogador, onde o nível de dificuldade das questões vai aumentando com o desenvolvimento do jogo.

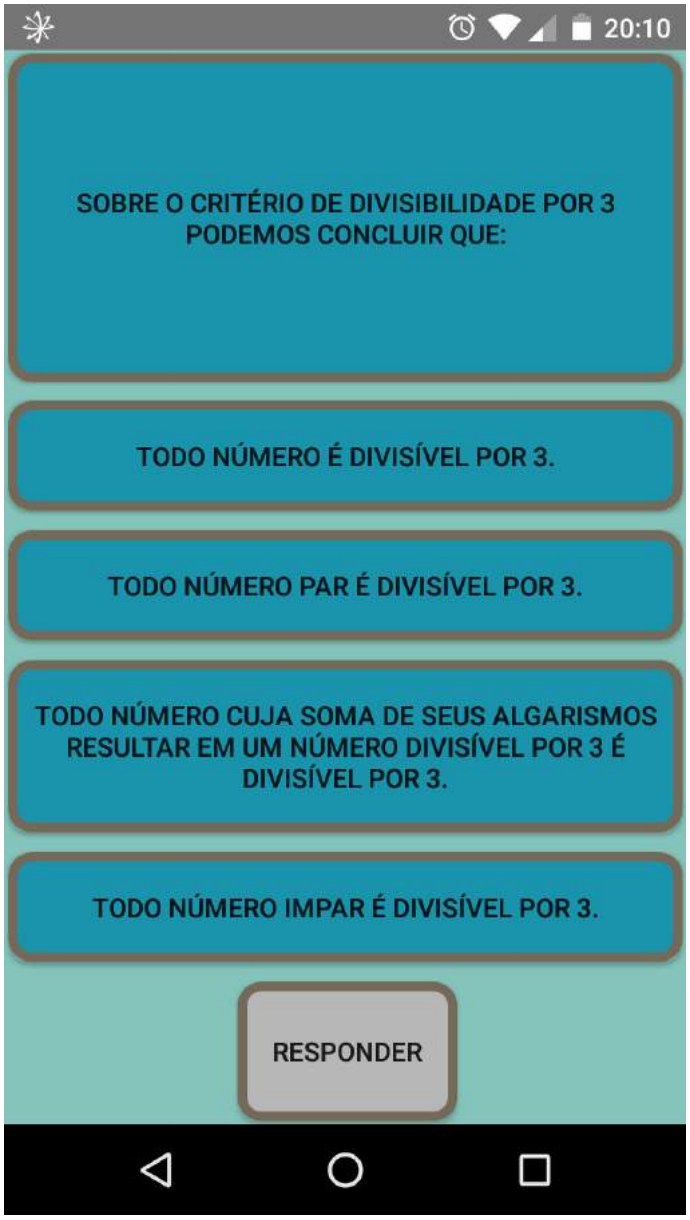


Figura 5: Exemplo de pergunta do tema *DIVISIBILIDADE*

Escolhido um dentre os temas: *Divisibilidade, Números Primos, MDC/MMC* e *Equações Diofantinas*, as perguntas apareceram uma-a-uma. Com a pergunta em tela, o jogador terá sempre quatro alternativas, podendo ser selecionado qualquer uma das alternativas; Ainda, é possível escolher outra opção a qualquer momento, sendo que a resposta só será considerada clicando em *RESPONDER*.

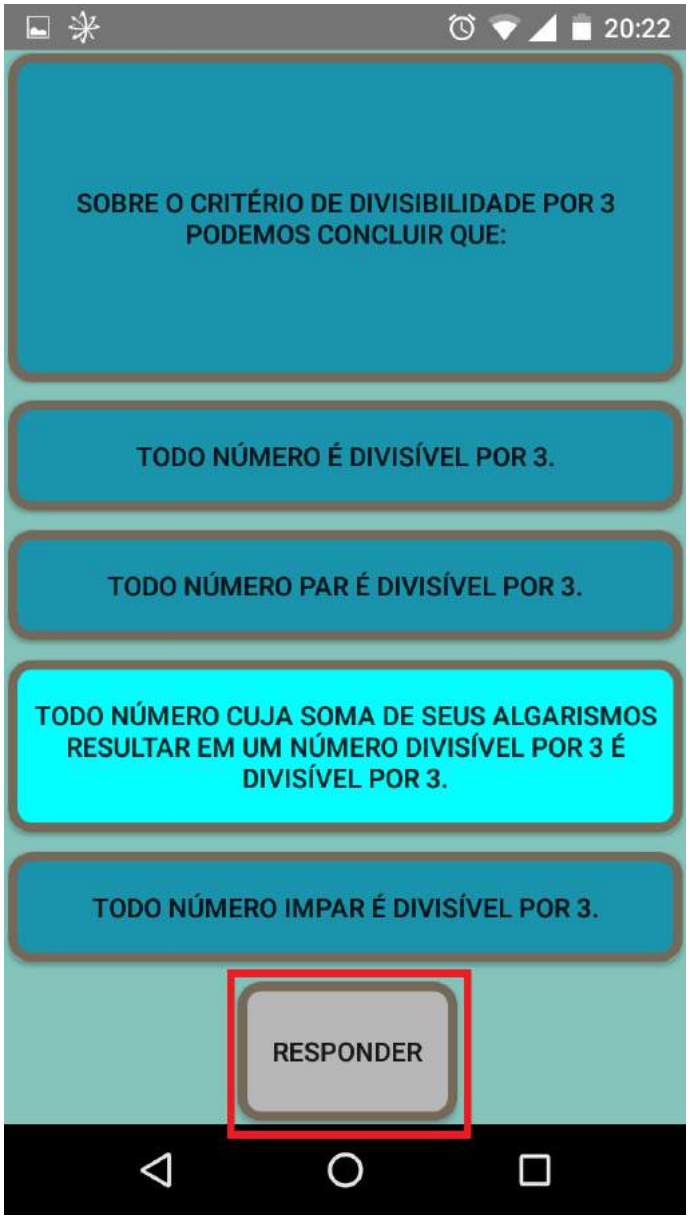


Figura 6: Tela de confirmação da resposta

Após confirmada a escolha, clicando em responder, aparecerá o resultado de acerto ou erro do jogador para a pergunta, e ainda, independente do resultado, lhe é dado um botão com a opção de *SOLUÇÃO*.

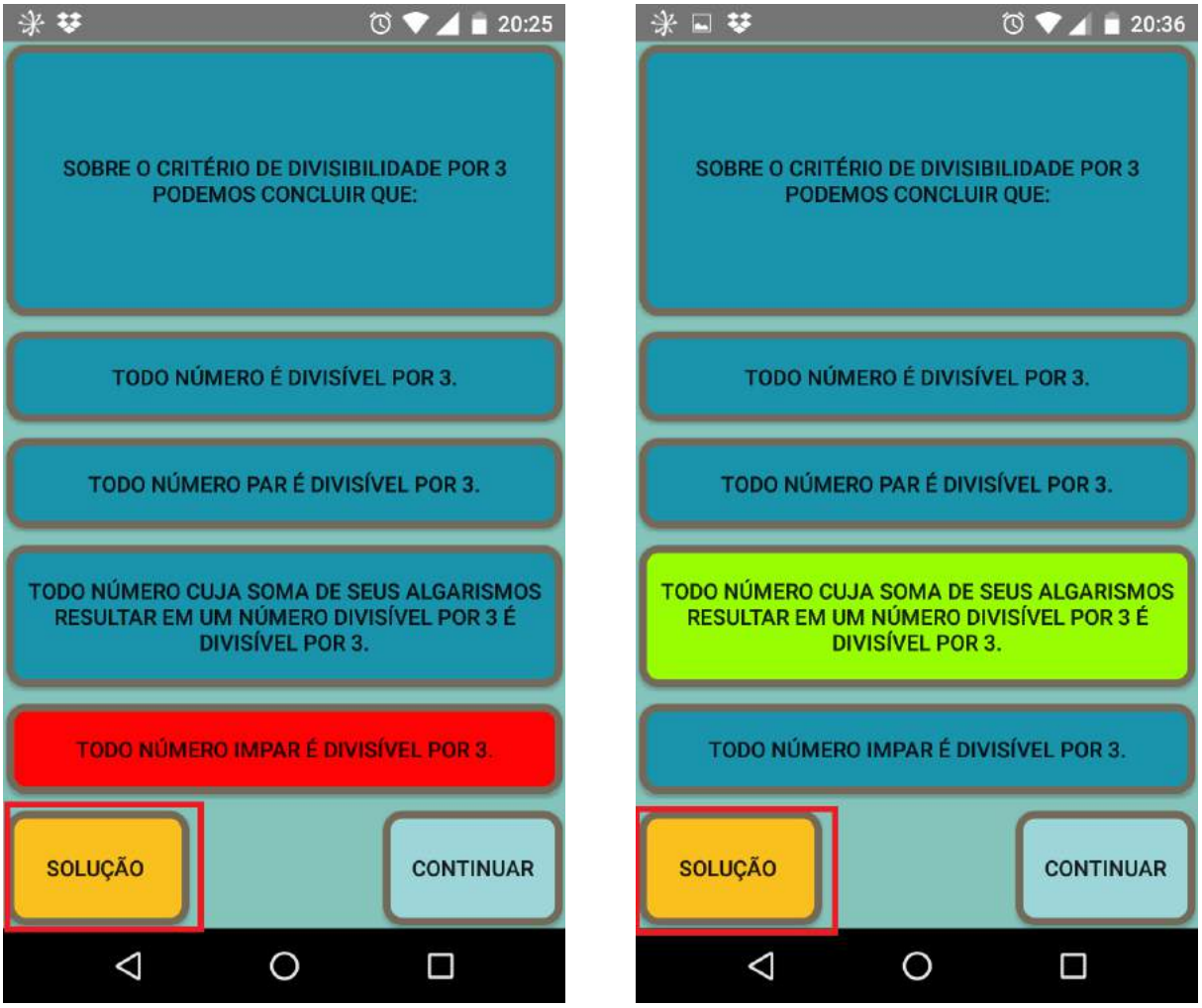


Figura 7: Opção *SOLUÇÃO*

Uma vez selecionada a opção *SOLUÇÃO*, aparecerá uma explicação referente a questão. O botão solução é útil para que o jogador confira se raciocinou a questão de maneira correta ou apenas acertou por uma coincidência. Além disso, esse botão relembra o conteúdo ou simplesmente ajuda o jogador a aprender algo novo, caso ele não possua familiaridade com o assunto, como segue figura abaixo.

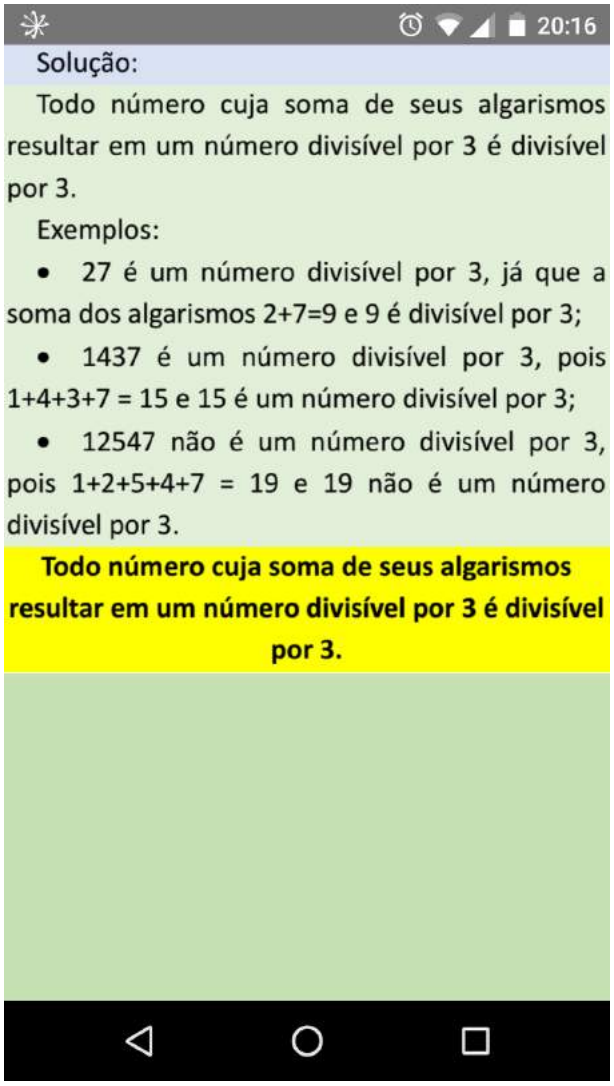


Figura 8: Solução referente a pergunta do aplicativo *Teoria dos Números - Quiz Show*

E assim segue os quatro temas do aplicativo, todos eles possuem rodadas de sete perguntas aleatórias e todas com um solução comentada. Durante toda a rodada de perguntas e respostas, a cada pergunta respondida corretamente, foi implementado um contador de acertos no formato de estrelas, onde cada resposta correta o jogador obtém um estrela, além de mensagens de motivação e de atenção referente ao desempenho no jogo.

Figura 9: Contador de acertos usando estrelas para representar cada ponto conquistado.

Figura 10: Mensagem de motivação para continuação.

Figura 11: Mensagem quando se erra a pergunta no aplicativo *Teoria dos Números - Quiz Show.*

Quando o jogador termina uma rodada, completando as sete questões, lhe será apresentado uma tela com os resultados obtidos, um novo menu contendo algumas opções, como nas figuras a seguir.

Figura 12: Exemplos de telas com resultados satisfatórios

Figura 13: Exemplos de telas com resultados abaixo do esperado

Observe que há algumas diferenças entre as telas onde o jogador obteve resultado satisfatório e as telas em que o jogador obteve o resultado abaixo do esperado. Uma das principais diferenças está no menu, mais precisamente na primeira opção, onde o jogador pode salvar seus resultados. Ao salvar os pontos, o jogador sempre terá duas opções que depende de seus resultados obtidos: se o resultado for satisfatório, salvando seus pontos, ele pode avançar para o próximo tema que já esta programado; Caso o resultado não tenha sido o esperado, ele terá a opção de salvar e voltar para a tela de temas, além das outras opções que são fornecidas independente do resultado, tendo assim a possibilidade de iniciar novamente (o mesmo tema ou outro).

Figura 14: Tela com as opções para salvar os resultados do aplicativo *Teoria dos Números - Quiz Show*

Para visualizar os resultados salvos, deve-se retornar para o menu principal onde se encontra a opção *SCORE*. Selecionando-a, um ambiente com a opção de selecionar o tema desejado para visualização dos pontos salvos, será exibido.

Figura 15: Tela *SCORE*

Para visualizar os pontos do tema que preferir, o jogador deve selecioná-lo na lista *TEMAS* e assim clicar no botão *SELECIONAR TEMA*, como é ilustrado a seguir.

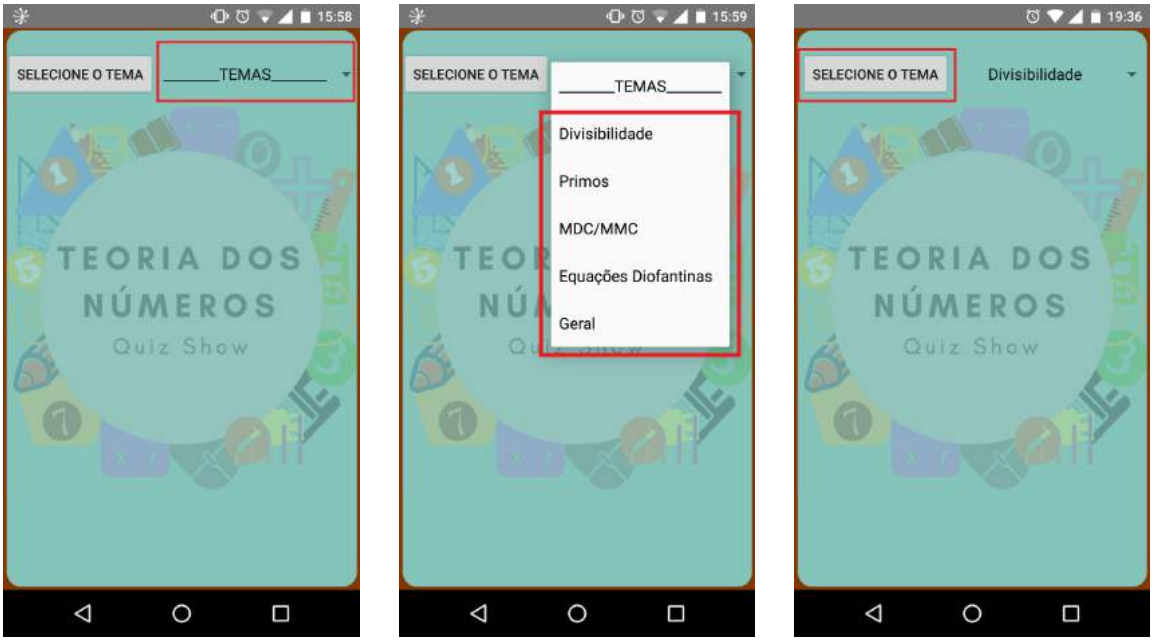


Figura 16: Passos para visualizar os pontos salvos

Voltando ao menu principal do aplicativo podemos encontrar a opção *SOBRE*, que conta com detalhes sobre o desenvolvimento do aplicativo, conforme figura abaixo:

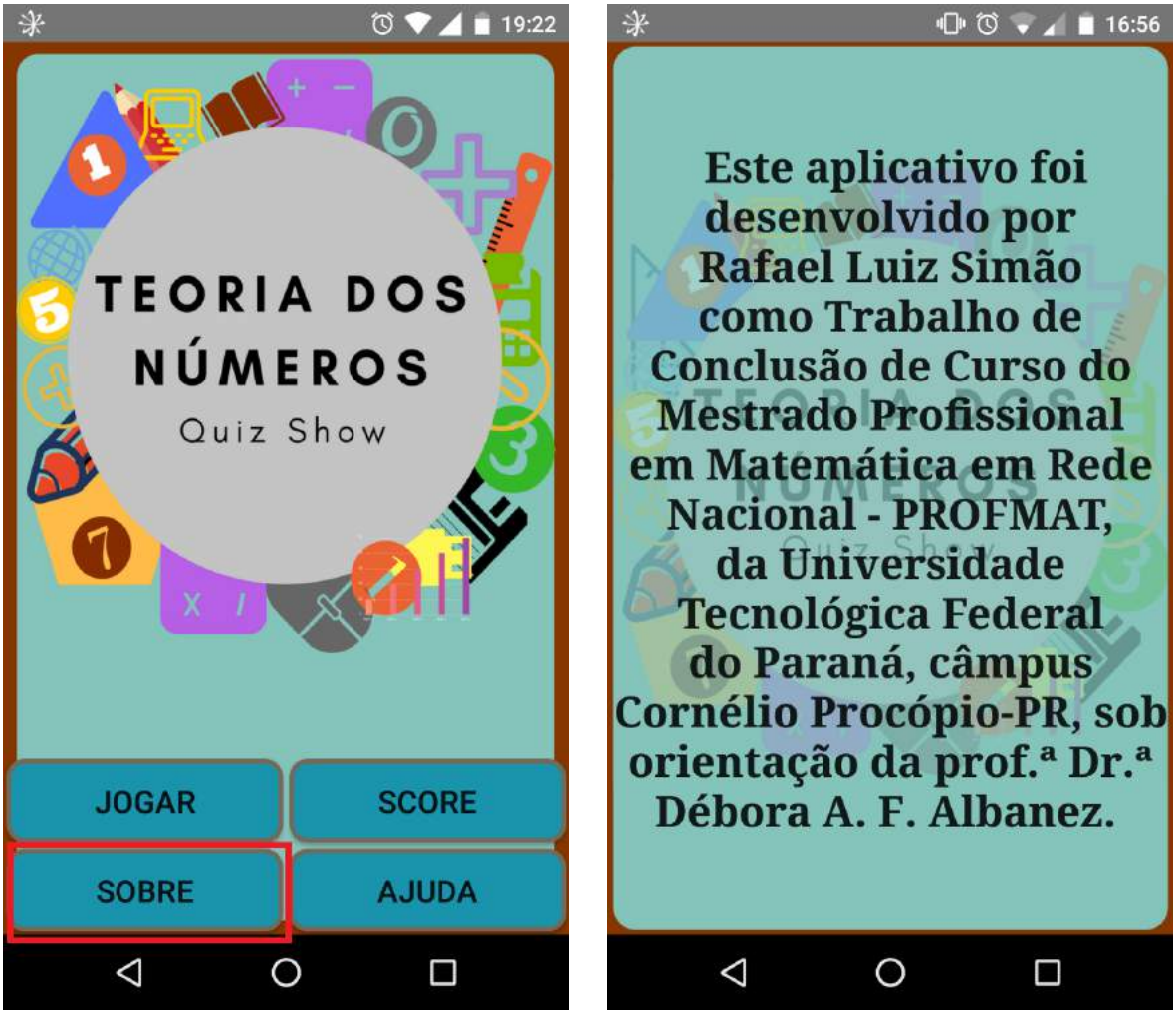


Figura 17: Tela *SOBRE*

4 PROPOSTA DE ATIVIDADE EM SALA DE AULA

A atividade em sala de aula foi desenvolvida com as turmas de 9º ano, da Escola Municipal Prof.ª Vera Lúcia Marcato Paganelli, situada em Ipaussu/SP.

A proposta de atividade em sala de aula foi desenvolvida em quatro etapas/temas, onde foi trabalhado os temas existentes no aplicativo *Teoria dos Números - Quiz Show* e o uso do aplicativo em sala de aula como recurso didático. A seguir, a descrição de cada tema trabalhado.

4.1 *TEORIA DOS NÚMEROS - QUIZ SHOW:* DIVISIBILIDADE

Objetivos Gerais: Identificar e compreender os conceitos e técnicas de divisibilidade e a utilização do aplicativo *Teoria dos Números - Quiz Show* como recurso didático.

Objetivos Específicos:

- Apresentar o que é divisibilidade, revisando a *Divisão Euclidiana*;
- Trabalhar os conceitos de divisibilidade, inicialmente utilizando o próprio material didático do aluno (livro e caderno);
- Utilizar o aplicativo *Teoria dos Números - Quiz Show* como recurso didático, assim mostrar que a tecnologia pode ser empregada na educação como um motivador para os discentes, pois o celular está presente no dia-a-dia dos alunos.

Tempo Estimado: 2 aulas.

Etapas de Desenvolvimento

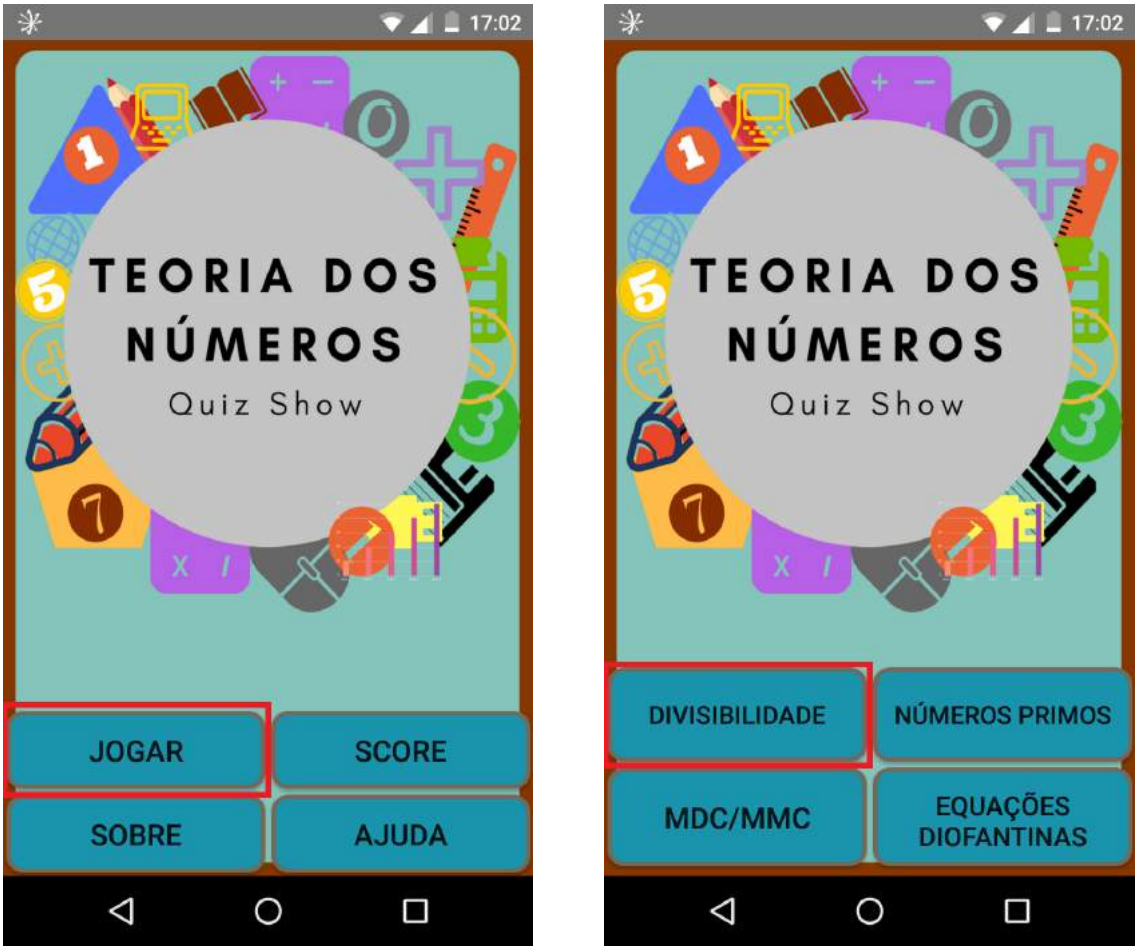
1ª Aula: Apresentação da teoria de divisibilidade.

Nesta primeira aula foi apresentado aos alunos o que é divisibilidade, retomando a *Divisão Euclidiana*, apresentando aos alunos o que é um divisor, dividendo, quociente e resto

de uma divisão. Além disso, lhes foi apresentado o conjunto de divisores de um número inteiro e também alguns critérios de divisibilidade, como a divisão por 2, 3, 4, 5, 6, 9 e 10. Para aplicação desta atividade, o recurso didático utilizado foi o próprio material escolar do aluno, como lápis, caneta, caderno e livro didático.

2ª Aula: Utilizando o aplicativo *Teoria dos Números - Quiz Show* como recurso didático, para o tema divisibilidade.

Após toda a teoria apresentada sobre divisibilidade na primeira aula, a segunda aula foi destinada a utilizar o aplicativo desenvolvido. Foi solicitado, a pedido do professor, que todos os alunos abrissem o aplicativo nos seus aparelhos celulares. Eles selecionaram no menu a opção *"JOGAR"* e depois o tema *"DIVISIBILIDADE"*, como ilustra a Figura 18.



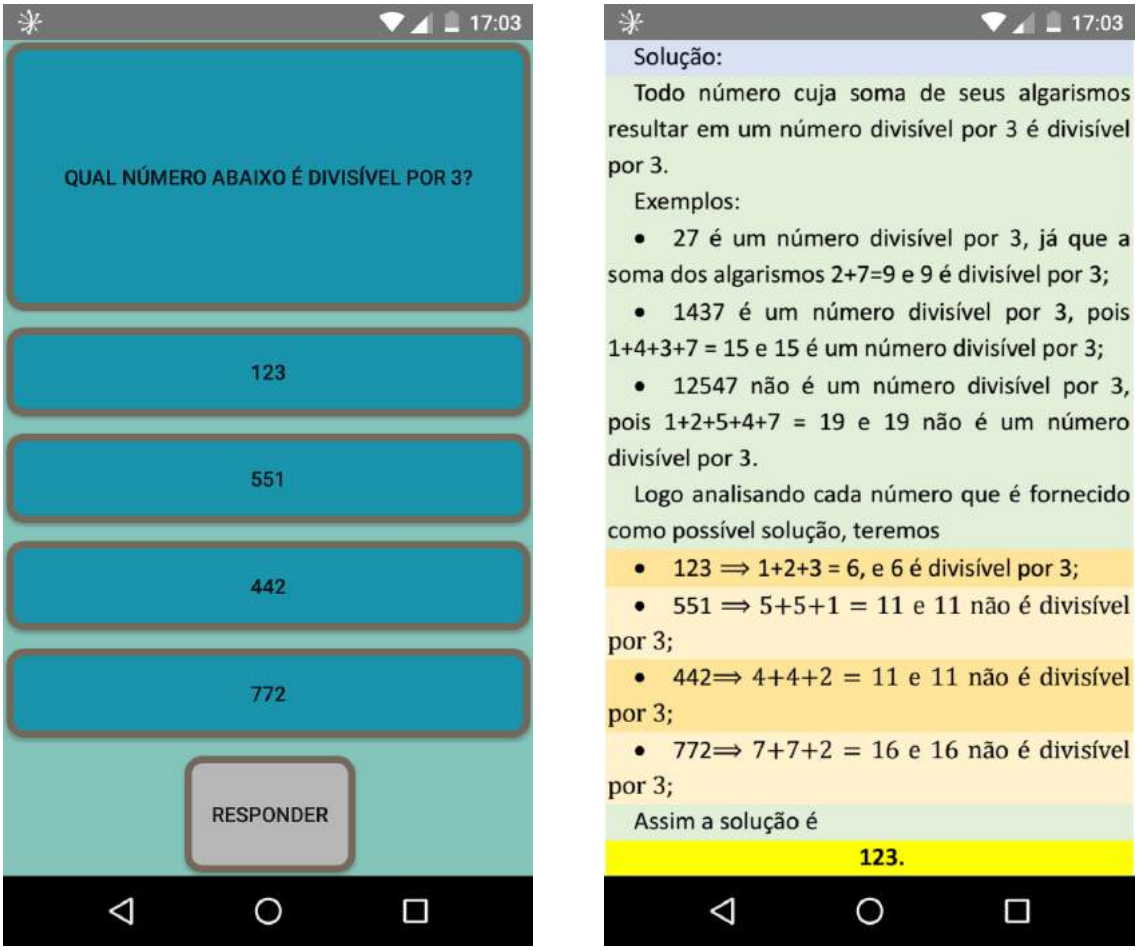
(a) Tela Inicial: o aluno deve selecionar a opção *JOGAR*.

(b) Tela de Temas: o aluno deve selecionar a opção *DIVISIBILIDADE*.

Figura 18: Passos para a 2ª aula de Divisibilidade

Neste momento, foi dado um tempo para que os alunos resolvessem as questões usando todo o conhecimento adquirido na aula anterior. Nesta etapa algumas dúvidas surgiram, princi-

palmente na resolução das perguntas, e as questões mais complexas foram explicadas individualmente e coletivamente. Foi também solicitado que o aluno consultasse o botão *"SOLUÇÃO"* para complementar a explicação, já que todas as questões contém a solução comentada, acertando ou não a questão. Segue exemplo de questão que está no aplicativo e foi resolvida pelos alunos:



(a) Questão do aplicativo referente ao tema. *Divisibilidade*

(b) Solução disponível no aplicativo refrente a questão ao lado.

Figura 19: Exemplo de questão disponível no aplicativo *Teoria dos Números - Quiz Show*.

Observação 4.1. Para acompanhar o desempenho da turma, e também para que o próprio aluno tenha uma autoavaliação, o professor pode pedir para que os alunos salvem seus pontos obtidos. Segue um exemplo de uma situação onde alunos dividiram o mesmo aparelho eletrônico durante a aula (seus nomes foram omitidos):

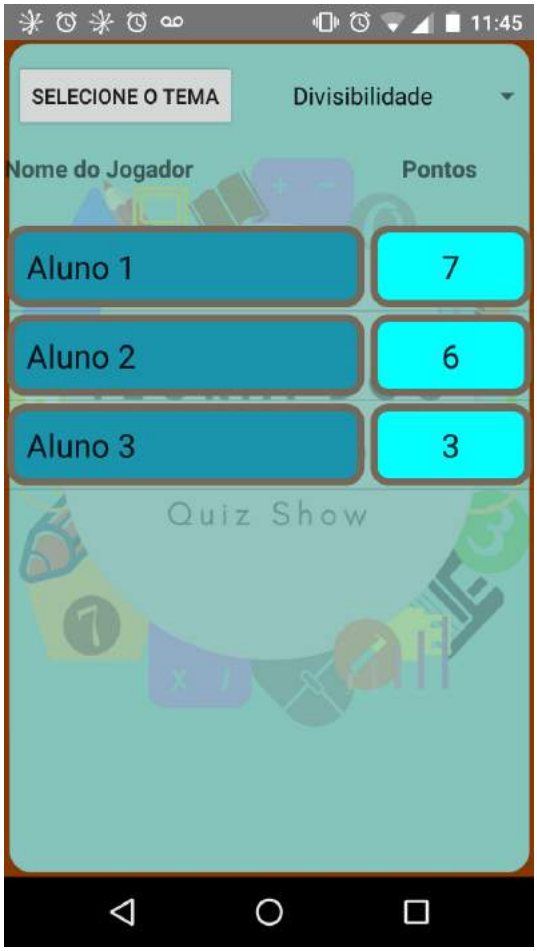


Figura 20: Score dos alunos durante a aula de Divisibilidade.

4.2 *TEORIA DOS NÚMEROS - QUIZ SHOW:* NÚMEROS PRIMOS

Objetivos Gerais: Identificar e compreender os conceitos de números primos e a utilização do aplicativo *Teoria dos Números - Quiz Show* como recurso didático.

Objetivos Específicos:

- Apresentar a definição de números primos;
- Apresentar o Crivo de Eratóstenes como uma "ferramenta" para localizar números primos;
- Trabalhar o Teorema Fundamental da Aritmética.

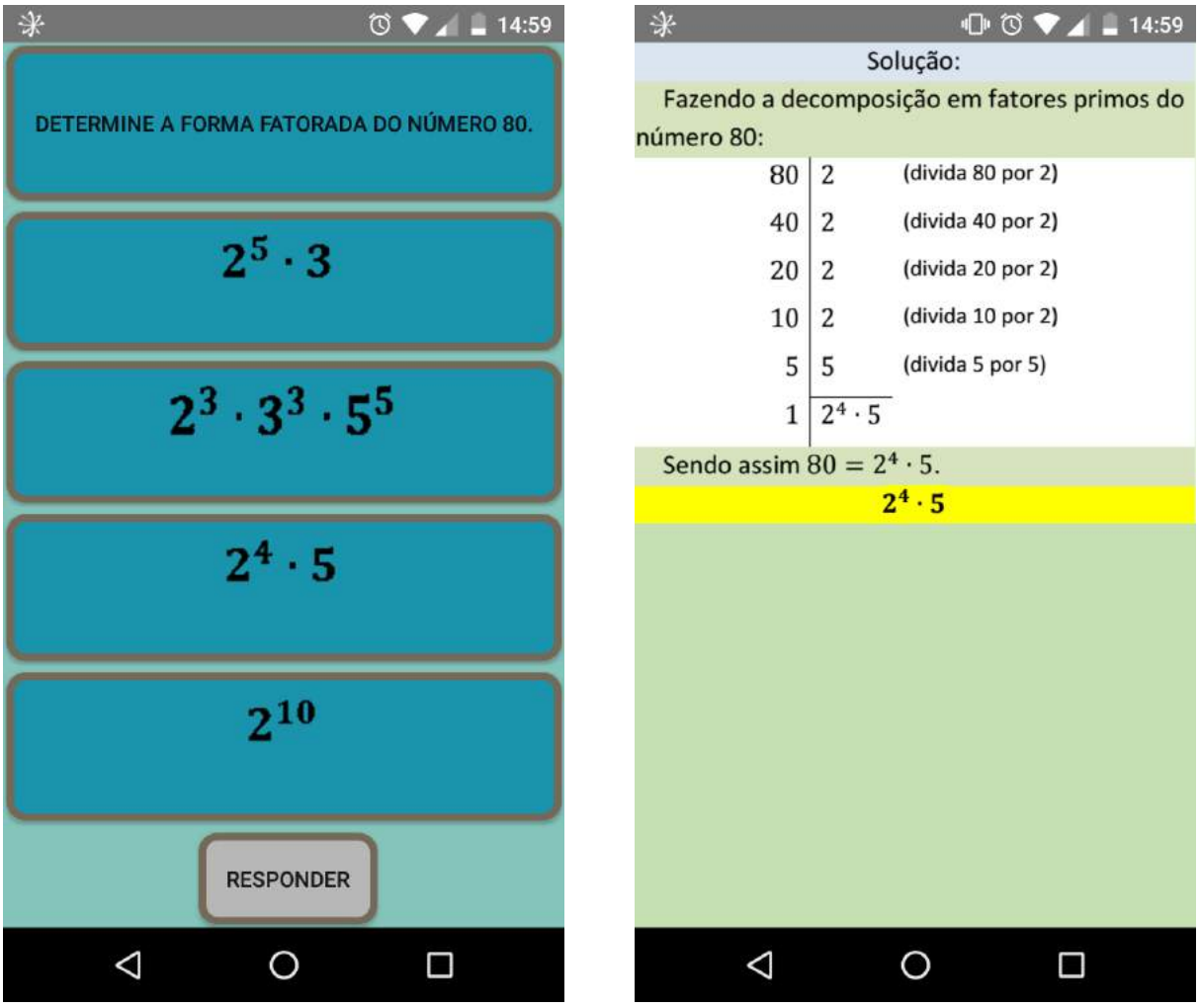
Tempo Estimado: 2 aulas.

Etapas de Desenvolvimento

1ª Aula: Apresentação da teoria dos números primos.

Na primeira aula de números primos, foi trabalhado com os alunos os conceitos de números primos, apresentando o Crivo de Eratóstenes que consiste em um algoritmo prático para se descobrir os números primos até um número dado. E por fim, apresentando o Teorema Fundamental da Aritmética, pois se baseia em uma teoria onde todos os números inteiros positivos maior que 1 podem ser decompostos em fatores primos. O recurso utilizado, foi o próprio material escolar do aluno.

O trabalho em sala de aula para utilização do aplicativo na opção *"NÚMEROS PRIMOS"* se deu de maneira análoga a exposta na Seção 4.1 . Segue questão trabalhada em sala de aula:



(a) Questão do aplicativo referente ao tema *Números Primos*

(b) Solução disponível no aplicativo refrente a questão ao lado.

Figura 21: Exemplo de questão disponível no aplicativo *Teoria dos Números - Quiz Show*.

Figura 22: Aluno utilizando aplicativo *Teoria dos Números - Quiz Show*.

Para acompanhar o desempenho da turma, foi verificado a pontuação de cada aluno neste tema, e os próprios alunos fizeram suas autoavaliações sobre seus conhecimentos do assunto. Foi notável o interesse dos discentes, pois eles queriam ver quem se sairia melhor na pontuação, estimulando uma competição saudável, onde eles se ajudavam entre si quando possuíam dúvidas.

4.3 *TEORIA DOS NÚMEROS - QUIZ SHOW:* MDC/MMC

Objetivos Gerais: Identificar e compreender os conceitos de máximo divisor comum e o mínimo múltiplo comum e a utilização do aplicativo *Teoria dos Números - Quiz Show* como recurso didático.

Objetivos Específicos:

- Apresentar a definição e as propriedades do máximo divisor comum;
- Apresentar a definição e as propriedades do mínimo múltiplo comum;
- Algoritmo de Euclides.

Tempo Estimado: 2 aulas.

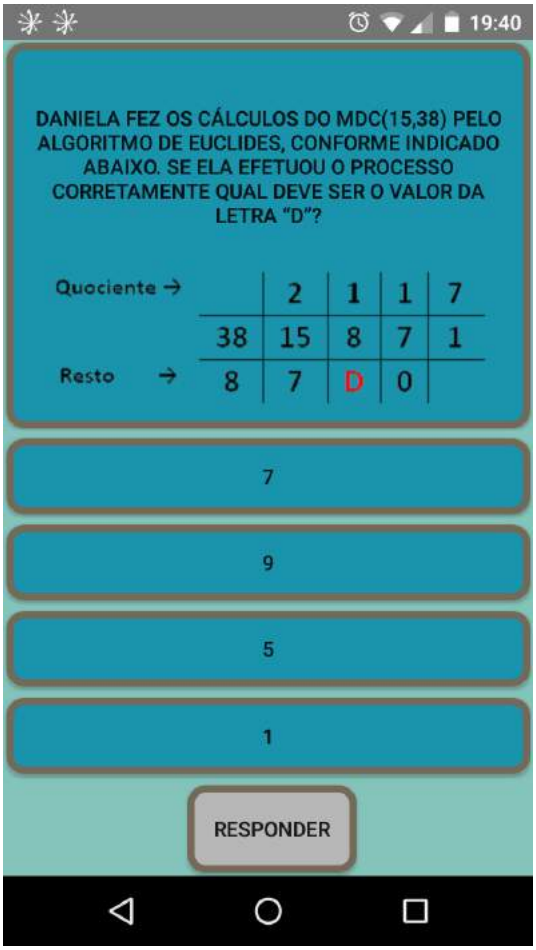
Etapas de Desenvolvimento

1ª Aula: Apresentação da teoria do MDC/MMC.

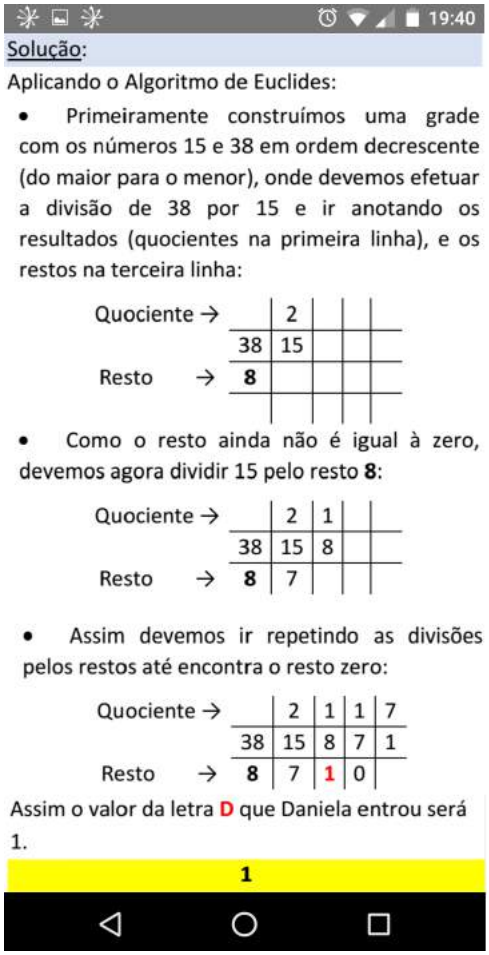
Inicialmente, a teoria apresentada aos alunos foram: máximo divisor comum e o mínimo múltiplo comum, além do Algoritmo de Euclides, útil para obter o máximo divisor comum.

2ª Aula: Utilizando o aplicativo *Teoria dos Números - Quiz Show* como recurso didático para teoria de *MDC/MMC*.

A utilização do aplicativo para teoria de *MDC/MMC* ocorreu de maneira análoga a das seções 4.1 e 4.2.



(a) Questão do aplicativo referente ao tema *MDC/MMC*



(b) Solução disponível no aplicativo refrente a questão ao lado.

Figura 23: Exemplo de questão disponível no aplicativo *Teoria dos Números - Quiz Show*.

Figura 24: Aluno trabalhando as questões do aplicativo *Teoria dos Números - Quiz Show*.

4.4 *TEORIA DOS NÚMEROS - QUIZ SHOW:* EQUAÇÕES DIOFANTINAS

Objetivos Gerais: Identificar e compreender os conceitos de Equações Diofantinas e a utilização do aplicativo *Teoria dos Números - Quiz Show* como recurso didático.

Objetivos Específicos:

- Apresentar a definição de Equação Diofantina;
- Modelar uma situação problema que envolva Equações Diofantinas;
- Identificar a existência de solução;
- Identificar uma solução particular de uma Equação Diofantina;
- Identificar a solução geral de uma Equação Diofantina.

Tempo Estimado: 2 aulas.

Etapas de Desenvolvimento

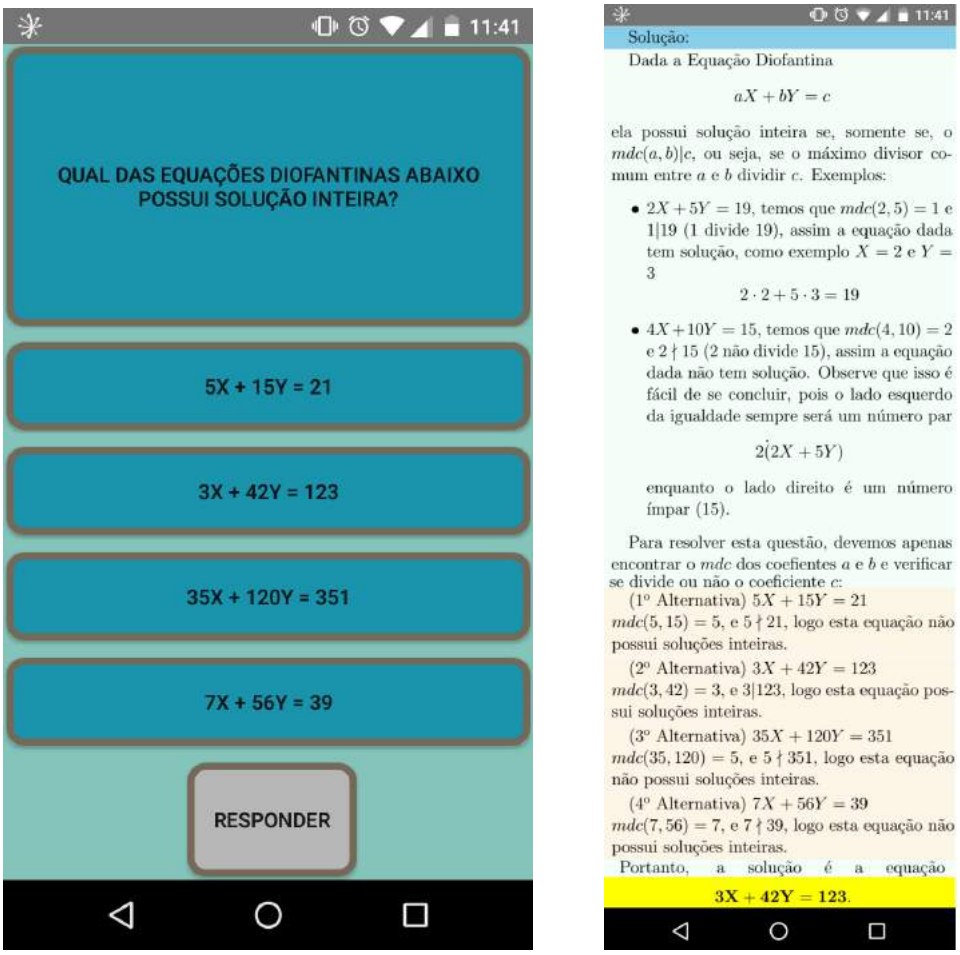
1ª Aula: Apresentação da teoria de Equações Diofantinas.

Para iniciar o tema, foi apresentado o que é uma Equação Diofantina da forma $ax + by = c$ com $a, b, c, x, y \in \mathbb{Z}$, as condições de existência de solução, onde afirmamos aos alunos que existe solução para uma Equação Diofantina se $mdc(a,b)|c$. Ainda foi apresentado para os alunos a solução particular e a solução geral de uma Equação Diofantina dada por $x = x_0 + bt$,

$y = y_0 - at$ com $t \in \mathbb{Z}$. Os recursos didáticos utilizados foram os materiais do aluno e a lousa para expor o conteúdo.

2ª Aula: Utilizando o aplicativo *Teoria dos Números - Quiz Show* como recurso didático para o aprendizado de Equações Diofantinas.

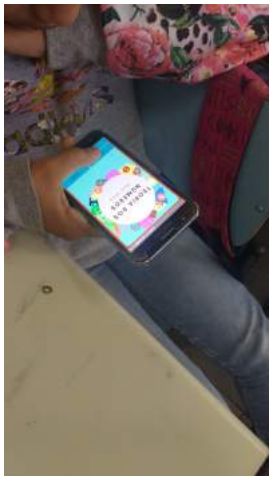
Com o jogo iniciado para esse tema, os alunos tiveram a mesma experiência dos temas anteriores, como rodadas de perguntas referente ao tema e ao final a opção de salvar seus resultados para acompanhamento do rendimento, segue a Figura 25 como exemplo de questão trabalhada em sala de aula.



(a) Questão do aplicativo referente ao tema *EQUAÇÕES DIOFANTINAS*

(b) Solução disponível no aplicativo refrente a questão ao lado.

Figura 25: Exemplo de questão disponível no aplicativo *Teoria dos Números - Quiz Show*, relacionada à equações diofantinas.



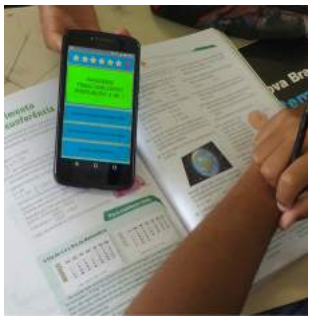


Figura 26: Alunos usando o aplicativo *Teoria dos Números - Quiz Show* como recurso didático.

Ao final deste último tema trabalhado, foi verificado o *"SCORE"* dos alunos na opção GERAL, onde todos os resultados salvos ficam registados.

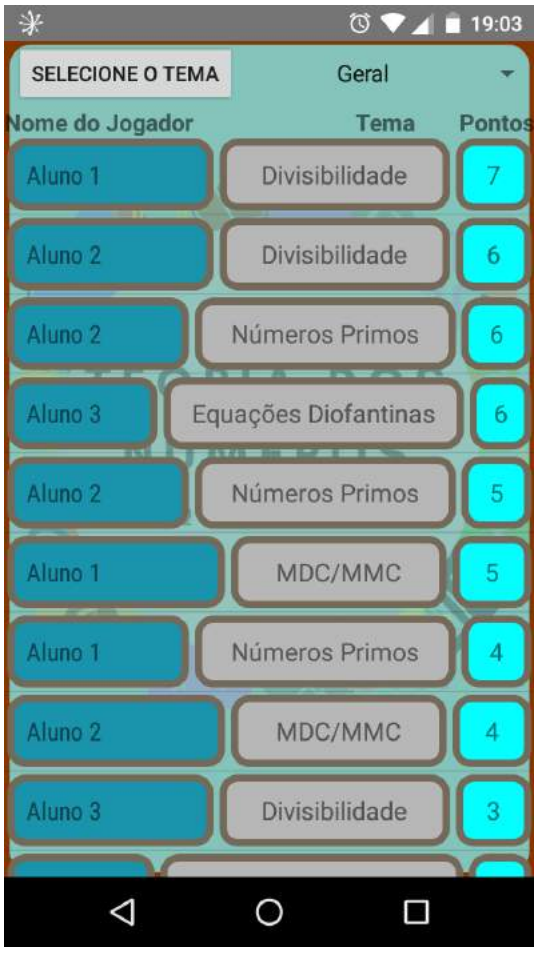


Figura 27: SCORE com opção Geral, registra todos os resultados obtidos pelo jogador do aplicativo.

5 CONCLUSÃO

É consenso entre educadores de todas as áreas que os professores vem encontrando novos desafios dentro da sala de aula, entre eles a falta de interesse dos discentes pelos conteúdos ensinados apenas de maneira tradicional. No caso da matemática, vários alunos consideram a disciplina difícil e durante a aula, muitos optam pelo uso incorreto (talvez em muitos casos, pela falta de orientação), dos aparelhos eletrônicos, atrapalhando ainda mais o processo de aprendizagem.

Desenvolvemos um aplicativo para aparelhos móveis em Teoria dos Números elementar por considerar este tema de fundamental importância para os estudos matemáticos iniciais. Ao trazermos o aplicativo *Teoria dos Números - Quiz Show*, para sala de aula com os alunos da rede pública, dando as orientações adequadas para sua utilização como ferramenta de aprendizagem, pudemos perceber que este despertou a curiosidade dos alunos para este tema, além de estimular uma competição saudável entre eles, disputando quem acertava mais questões e fazia mais pontos. E assim notamos que de fato a tecnologia de aplicativos móveis pode ser utilizada em prol da educação.

Por fim, esperamos que esta proposta de ensino utilizando o aplicativo *Teoria dos Números - Quiz Show*, ou outro aplicativo educacional disponível nos lojas virtuais, sirva de inspiração a professores de ensino fundamental e médio, estudantes ou amantes da matemática. Destacamos também a necessidade da continuação das pesquisas em educação relacionadas ao uso de aplicativos para dispositivos móveis em sala de aula, já que esta tecnologia está em contínuo desenvolvimento. Ansiamos que o leitor/professor se interesse também pelo desenvolvimento de novos aplicativos, contribuindo para a melhoria da educação matemática.

REFERÊNCIAS

EDUCAÇÃO, M. da. **Parâmetros curriculares nacionais: Matemática/Secretária de Educação Fundamental**. Brasília: MEC/SEF, 1998.

HEATH, T. L. **Euclid - The thirteen books of elements**. 1. ed. United States: Courier Corporation, 1956.

HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro, RJ: SBM, 2014.

KENSKI, V. M. **Educação e Tecnologias o Novo Ritmo Da Informação**. 8. ed. Campinas, SP: PAPIRUS, 2011.

MILIES, C. P.; COELHO, S. P. **Números: Uma Introdução Matemática**. 3. ed. São Paulo, SP: Edusp, 2013.

MOREIRA, C. G. T. de A.; MARTÍNEZ, F. E. B.; SALDANHA, N. C. **Tópicos de Teoria dos Números**. 1. ed. Rio de Janeiro, RJ: SBM, 2012.

SANTOS, J. P. de O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro, RJ: IMPA, 2017.