UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO - UFRPE
MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT

Teoria dos Números no Ensino Básico: Um estudo de caso no 2º ano do Ensino Médio

Josemar Claudino Barbosa

Recife, 2017

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO - UFRPE
MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT

Teoria dos Números no Ensino Básico: Um estudo de caso no 2º ano do Ensino Médio

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática - PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO - UFRPE, como requisito parcial para obtenção do Grau de Mestre em Matemática.

Área de Concentração: Matemática

Orientador: Drª. Bárbara Costa da Silva
Coorientador: Drª. Isis Gabriella de Arruda Quinteiro Silva

Recife, 2017

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

B238t Barbosa, Josemar Claudino
Teoria dos números no ensino básico: um estudo de caso no 2º ano do ensino médio / Josemar Claudino Barbosa. – 2017.
118 f.: il.

Orientadora: Bárbara Costa da Silva.
Coorientadora: Isis Gabriella de Arruda Quinteiro Silva.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação Profissional em Matemática, Recife, BR-PE, 2017.
Inclui referências, anexo(s) e apêndice(s).

1. Teorema dos números 2. Congruência modular 3. Sequência didática I. Silva, Bárbara Costa da, orient. II. Silva, Isis Gabriella de Arruda Quinteiro, coorient. III. Título

CDD 510

JOSEMAR CLAUDINO BARBOSA

Teoria dos Números no Ensino Básico: Um estudo de caso no 2º ano do Ensino Médio

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em ____ /____/_____

BANCA EXAMINADORA

_____

Profª Drª Bárbara Costa da Silva (Orientador(a))– UFRPE

_____

Profª Drª Isis Gabriella de A. Quinteiro Silva (Coorientador(a))– UFRPE

_____

Prof. Dr. Jorge Nicolás Caro Montoya – DMAT-UFPE

_____

Profª. Drª. Karla Ferreira de Arruda Duque– PROFMAT/UFRPE

Dedico este trabalho aos meus pais.

Agradecimentos

Agradeço a Deus a oportunidade de concluir esse curso de mestrado que infelizmente teve que ser interrompido já na reta final, no ano de 2014, por motivo de doença que me acometeu e na família. Não foi fácil erguer-se novamente e lutar para concluí-lo. Mas a Bíblia diz que Deus faz um caminho no deserto. Não é fácil passar pelos desertos da vida. Mas lá, Ele me sustentou. À Ele toda a Glória.

Agradeço aos meus pais, e aos meus familiares pela presença amiga e fraterna.

Agradeço à minha querida esposa pela compreensão e apoio. Seu sorriso foi, por muitas vezes, o motivo de continuar lutando.

Agradeço à Direção Geral e à Direção de Ensino do Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - IFPE, campus Caruaru, pelo apoio dado.

Agradeço aos alunos da turma do 2º ano do ensino médio do curso técnico integrado de edificações do IFPE, campus Caruaru, participantes do curso básico de Teoria dos Números.

Agradeço também aos amigos da turma de 2012, em especial Emerson Dantas, Danilo Campos, José Roberto, Marcio Rodrigo, José Ferreira e Carlos Eduardo pelos momentos agradáveis de estudo.

Agradeço também aos colegas da turma de 2015, em especial Ribamar Neves, Bruno Lopes, Murilo, José Igor, Eudes e Michelangelo pelo incnetivo durante o curso.

Agradeço ao amigo Wagner Santos, egresso do PROFMAT-UFRPE, que muito contribuiu no manuseio do programa LATEX.

Agradeço também à SBM e à CAPES pela singular oportunidade dada para cursar o PROFMAT.

Agradeço também à Professora Doutora Isis Gabriella, por sua sempre paciente e gentil orientação.

Por fim, quero agradecer à Professora Doutora Barbara Costa, que é um exemplo de docente a ser seguido, por sua singeleza nas orientações.

"Não temas, porque eu sou contigo; não te assombres, porque eu sou teu Deus; eu te fortaleço, e te ajudo, e te sustento com a destra da minha justiça.".
(Isaías 41:10)

Resumo

Apresentamos neste trabalho uma proposta de inclusão de conceitos básicos da Teoria dos Números no currículo do ensino médio. A Teoria dos Números é uma área da matemática de extrema importância, que possui inúmeras aplicações, como por exemplo a criptografia, e que pode ser útil na resolução de problemas que, sem o uso das ferramentas matemáticas estudadas nessa teoria, teriam uma solução bastante complexa. Este trabalho teve origem considerando a necessidade de tornar o processo de ensino-aprendizagem da matemática mais proveitoso a partir da resolução de problemas desafiadores que despertem o interesse dos alunos por essa ciência e propiciem, nos mesmos, o desenvolvimento do raciocínio lógico, pensamento crítico e a compreensão de ideias conceituais, que seria o ponto chave da aprendizagem da matemática. Nesse contexto, trabalhar alguns conceitos da teoria dos números seria uma forma de gerar tais resultados. Portanto, neste trabalho será apresentada uma proposta de sequência didática onde serão trabalhados, sem abrir mão do rigor matemático, mas ao mesmo tempo respeitando o nível de aprendizado dos alunos, conceitos matemáticos como Divisibildade, "máximo divisor comum" (MDC) e "mínimo múltiplo comum" (MMC), propriedade fundamental da aritmética, Aritmética Modular e Equações Diofantinas. No contexto atual da educação brasileira, onde os resultados das avaliações do nível de aprendizagem dos estudantes em relação à matemática são pífios, é necessário repensarmos a prática pedagógica vigente em que apenas a memorização de fórmulas tem sido priorizada no ensino de matemática. Sendo assim, esse trabalho consistiu em desenvolver um curso básico de Teoria dos Números com alunos de uma turma do 2º ano do ensino médio no Instituto Federal de Educação e Ciência de Pernambuco - IFPE, Campus Caruaru. Antes do curso, os alunos foram submetidos a um teste inicial, denominado "Teste 1" e, ao término do curso, realizaram um novo teste, denominado, "Teste 2" para que fossem mensurados os possíves avanços dos alunos. Durante o curso foram trabalhados vários temas do estudo da teoria dos números, bem como suas aplicações, seja na própria matemática ou em algumas situações do cotidiano, e que servirão de instrumentos de motivação para o desenvolvimento das aulas.

Palavras-chave: Teoria dos Números, Congruência Modular, Sequência Didática.

Abstract

We present in this project a proposal to include basic concepts of number theory in the secondary school curriculum. Numbers theory is an area of mathematics of great importance, which has numerous applications, such as cryptography, and which can be useful in solving problems that would have a rather complex solution without the mathematical tools studied in this theory . This work originated considering the need to make the teaching-learning process of mathematics more profitable by solving challenging problems that arouse students' interest in this science and foster, in them, the development of logical reasoning, critical thinking and the understanding of conceptual ideals, which would be the key point in learning mathematics. In this context, working on some concepts of Numbers Theory would be one way of generating such results. Therefore, in this work will be presented a proposal of a didactic sequence where they will be worked, without abandoning mathematical rigor, but at the same time respecting the level of the student's learning process, mathematical concepts such as divisibility, GCD and LCM, fundamental arithmetic property, modular arithmetic, and diophantine equations. In the current context of Brazilian education, where the results of assessments of students' learning level in relation to mathematics are poor, it is necessary to rethink the current pedagogical practice in which only the memorization of formulas has been prioritized in mathematics teaching. Thus, this work consisted of developing a basic course in Numbers Theory with students of a 2nd grade high school class at the Federal Institute of Education and Science of Pernambuco - IFPE, Campus Caruaru. Before the course, the students underwent an initial test, called "Test 1" and, at the end of the course, they performed a new test, called "Test 2" to measure the students' possible progress. During the course, several themes of the study of Number Theory as well as their application of Numbers Theory were worked on, either in mathematics itself or in some everyday situations, and which will serve as motivational tools for the development of classes.

Keywords: Numbers Theory, Modular Congruence, Didactic Sequence.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

O ensino de matemática no Brasil vem sendo alvo de estudos e discussões por parte de especialistas da área, em busca de melhorar os índices que medem o ensino dessa disciplina no Brasil. Um dos temas que vem sendo discutido é a inclusão de alguns tópicos básicos de teoria dos números, que seriam uma ferramenta eficaz para uma prática de ensino que evidencie a resolução de problemas. Conforme os PCN's de Matemática para o Ensino Médio em [4, p. 40]:

> É preciso que o aluno perceba a matemática como um sistema de códigos e regras que a tornam uma linguagem de comunicação de idéias e permite modelar a realidade e interpretá- la.

Ainda de acordo com os PCN's, em [4, p. 40]:

> A matemática no ensino médio não possui apenas o caráter formativo ou instrumental, mas também deve ser vista como ciência, com suas características estruturais específicas. É importante que o aluno perceba que as definições, demonstrações e encadeamentos conceituais e lógicos têm a função de construir novos conceitos e estruturas a partir de outros e que servem para validar intuições e dar sentido às técnicas aplicadas.

Além disso, dentre os objetivos do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) destacamos o de estimular a melhoria do ensino de matemática em todos os níveis e o de incentivar uma postura crítica acerca das aulas de matemática nos níveis do ensino fundamental e médio, que enfatize o papel central do conhecimento de matemática frente às exigências da sociedade moderna.

Nesse sentido, mais uma vez verifica-se a importância do ensino da teoria dos números.

Diante disso e ciente que o desafio é grande no que se refere à melhora do rendimento do processo de ensino aprendizagem de matemática, apresentaremos neste trabalho uma proposta de sequência didática que possibilite o aprendizado de alguns tópicos da teoria dos números, em especial a aritmética modular e as equações diofantinas, com alunos de uma turma do $2^{\underline{o}}$ ano do ensino médio. Para tanto, foram ministradas aulas, ao longo de 10 encontros, abordando alguns tópicos de teoria de números. No início e no final do curso foram aplicados testes com o objetivo de avaliar a aprendizagem dos alunos, fundamentando, através desses resultados, a viabilidade do ensino de tais conteúdos.

Nesta caminhada, buscamos incentivar, na medida em que as aulas forem desenvolvidas, que os estudantes usassem estratégias para resolver os problemas que surgiram durante o percurso das atividades.

Ao final deste curso, o estudante deverá ter a capacidade de compreender tópicos básicos da teoria dos números, bem como suas aplicações, e utilizá-las como ferramentas para resolução de variados problemas e aplicá-los em algumas situações do cotidiano, como por exemplo a criptografia. Esse trabalho foi aplicado em uma turma da segunda série do ensino médio do Instituto Federal de Ciência e Tecnologia de Pernambuco - IFPE, Campus Caruaru, entre os meses de outubro e novembro, no horário contrário ao turno de aula dos respectivos alunos. Esta atividade foi essencialmente prática, intercalada por alguns momentos de demonstração dos teoremas que fundamentaram o desenvolvimento das aulas e com bastante resolução de exercícios tirados, principalmente, de provas das "Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP)". Durante o curso, utilizamos vídeos sobre alguns temas estudados, bem como vários jogos matemáticos.

A realização da pesquisa se deu da seguinte forma:

- Aplicação de um teste, que intitulamos de "Teste 1", para verificar os conhecimentos dos discentes bem como as estratégias de resolução utilizadas pelos mesmos para a resolução das questões presentes no teste. Os conteúdos abordados nas questões do Teste 1 foram: Congruência Modular (Questão 1), Lema dos Restos (Questões 5 e 13), Divisibilidade (Questões 2, 7 e 9), Equações Diofantinas (Questões 3 e 6), Algoritmo da Divisão (Questões 4, 8 e 11), Paridade (Questão 12), MDC (Questão 14), Números Primos (Questão 10). Após a realização do mesmo, foi realizada a correção e a análise das respostas dadas pelos alunos e a mesma foi apresentada no Capítulo 1 desta dissertação.

- Realização de um curso intitulado "Tópicos Básicos de Teoria dos Números". Tal curso foi realizado ao longo de 10 aulas através das quais foram ministrados os seguintes temas: Aula 01 - Divisibilidade, Aula 02 - Divisão Euclidiana, Aula 03 - Paridade de Inteiros, Aula 04 - Números primos, Aula 05 - MDC, Aula 06 - MMC, Aula 07 - Equações Diofantinas, Aula 08 - Congruência Modular, Aula 09 - Teorema de Euler e Teorema de Fermat, Aula 10 - Criptografia método RSA. Nas aulas, as estratégicas didáticas utilizadas foram aplicações de jogos, exibição de vídeos, exposição oral dos temas e resolução de muitos exercícios. Os planos de aulas podem ser encontrados no capítulo 2 desse trabalho e os materiais extras utilizados nas aulas podem ser vistos no apêndice A dessa dissertação.

- Aplicação de um segundo teste, intitulado de "Teste 2", com 14 questões, através do qual buscou-se constatar os possíveis avanços obtidos no aprendizado dos participantes do curso ministrado. Nesse segundo teste, a estrutura foi a seguinte: Divisibilidade (Questão 7), Algoritmo da Divisão (Questão 2), Paridade de Inteiros (Questões 11 e 12), Números Primos (Questões 4 e 9), MDC (Questão 14), Equação Diofantina (Questão 3), Congruências, Teorema de Euler e Fermat (Questões 1, 6 e

10), Lema dos Restos (Questões 8, 5 e 13). Após a realização do mesmo, foi feito a correção e a análise das respostas dadas pelos discentes, a qual está apresentada no Capítulo 3 desse trabalho.

1 Teste 1 e análise dos resultados

O Teste 1 foi aplicado para 18 alunos do 4º período do curso Técnico em Edificações Integrado ao Ensino Médio do Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - IFPE, Campus Caruaru. O objetivo da aplicação desse teste foi verificar o nível de conhecimento e as estratégias utilizadas para a resolução das questões por parte dos alunos participantes do curso, visto que para resolver de maneira prática muitas das questões, seriam necessários alguns conhecimentos da teoria dos números que não são estudados no ensino básico. Abaixo, exibimos a análise das respostas dos discentes em cada questão e depois uma análise mais geral dos resultados obtidos.

1.1 Análise das questões

Questão 1

Qual é o resto da divisão de 3^{20} por 8?

(a) 1 (b) 3 (c) 2 (d) 4 (e)5

Alternativa correta: A

A tabela abaixo mostra o percentual de alunos (de um total de 18 participantes conforme foi especificado acima) que assinalaram cada alternativa da questão 1.

Tabela 1 – Questão 1T1

Alternativa	Percentual de alunos
a	16,7
b	5,5
c	11,1
d	16,7
e	0
n.a. (não assinalou)	50

O objetivo dessa questão era verificar quais seriam as estratégias para resolução da mesma. Como já era de se esperar, muitos tentaram desenvolver a potência 3^{20} e, após achar o valor dessa potência, dividí-lo por 8 e verificar qual é o resto dessa divisão. Como é um valor alto, é bastante comum errar os cálculos e, consequentemente, apenas 16,7% dos alunos acertaram essa questão. No entanto, tendo conhecimento, por exemplo, do Lema dos Restos (**Lema 2.2.1**), que será abordado posteriormente nesse trabalho, facilmente essa questão é resolvida. E isso foi constatado durante as aulas quando os alunos ficaram

surpresos com a resolução dessa questão: "Era só isso mesmo, professor?", indagaram. Diante disso, acreditamos que seja possível inserir modelos de questões nesse formato no ensino básico para que, através de desafios como esses, as aulas fiquem mais motivadas e interessantes.

Questão 2

Quantos múltiplos de 7 existem entre 14 e 7000, inclusive?

(a) 995 (b) 996 (c) 997 (d) 998 (e) 999

Alternativa correta: E

A tabela abaixo mostra o percentual de alunos que assinalou cada alternativa da questão 2.

Tabela 2 – Questão 2T1

Alternativa	Percentual de alunos
a	5,5
b	0
c	16,7
d	11,1
e	38,9
n.a. (não assinalou)	27,8

O objetivo dessa questão era verficar o nível de conhecimento dos alunos no que tange ao conceito de múltiplos e divisores. Como se pode observar, é uma questão bastante simples. A **Tabela 2** mostra que 38,9% dos avaliados acertaram essa questão. Vemos também que 11,1% dos alunos assinalaram a alternativa D. Na correção do teste aplicado, foi verificado que tais alunos subtraíram 14 de 7000 e o resultado dessa diferença dividiram por 7, encontrando 998. Provavelmente, não interpretaram bem o termo inclusive.

Questão 3

Se um macaco sobe uma escada de dois em dois degraus, sobra um degrau; se ele sobe de três em três degraus, sobram dois degraus. Quantos degraus a escada possui, sabendo que o número de degraus é múltiplo de sete e está compreendido entre 40 e 100?

(a) 63 (b) 70 (c) 77 (d) 84 (e) 91

Alternativa correta: C

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 3.

Tabela 3 – Questão 3T1

Alternativa	Percentual de alunos
a	0
b	0
c	77,7
d	11,1
e	38,9
n.a. (não assinalou)	11,1

O objetivo dessa questão era verificar se os alunos tentariam resolver a questão através de um modelo algébrico e, sem perceber, encontrar uma equação diofantina ou através de substituições. Bem, todas as tentativas de resolução foram realizadas por meio de substuições dos valores a fim de verificar qual seria a solução do problema. Analisando a **Tabela 3** apresentada acima, observa-se que 77,7% conseguiram resolver essa questão uitilizando a estratégia citada acima. No entanto, durante a ministração da aula cujo tema foi Equações Diofantinas, frizamos para os alunos a necessidade de apropriar-se desse modelo matemático pois nem sempre a estratégia utilizada pelos mesmos seria suficiente para resolver problemas nesse formato.

Questão 4

Quantas semanas formam 280 dias?

(a) 40 (b) 50 (c) 60 (d) 70 (e)80

Alternativa correta: A

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 4.

Tabela 4 – Questão 4T1

Alternativa	Percentual de alunos
a	94,4
b	0
c	0
d	5,5
e	0

O objetivo dessa questão foi analisar o conceito de Divisão Euclidiana, uma vez que para resolvê-la, seria necessário analisar o quociente da divisão de 280 por 7. Os alunos estavam bem apropriados da resolução desse modelo de questão com a **Tabela 4** mostrando claramente isso.

Questão 5

O resto da divisão por 4 do número $1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots + 2^9 + 2^{10}$ é:

(a) 1 (b) 2 (c) 3 (d) 4 (e)5

Alternativa correta: C

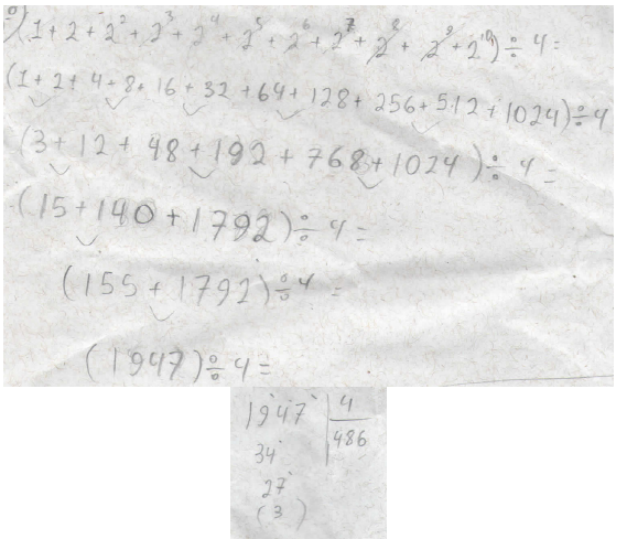
A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 5.

Tabela 5 – Questão 5T1

Alternativa	Percentual de alunos
a	5,5
b	0
c	55,6
d	0
e	5,5
n.a. (não assinalou)	33,3

Para resolver tal questão, bastava utilizar o Lema dos Restos (**Lema 2.2.1**), que é um conhecimento que praticamente não se aborda no ensino básico. A partir da análise da **Tabela 5**, vemos que 55,6% dos alunos acertaram essa questão, mas, para isso, segundo a análise das respostas, resolveram o valor de cada potência, somaram cada valor encontrado e, em seguida, dividiram o valor da soma encontrada por 4, verificando o resto. Mais uma vez, durante as aulas, na ministração do tema Lema dos Restos e, posteriormente, com a resolução de várias questões utilizando esse lema, muitos falaram que não imaginavam que através, dessa simples ideia, facilmente resolveriam inúmeras questões. A figura abaixo mostra a estratégia de um determinado aluno na resolução da questão 5 do Teste 1.

Figura 1 – Resposta de um aluno - 1



Questão 6

Numa loja são vendidos selos no valor de R$ 5,00 e R$ 7,00. De quantas maneiras podemos comprar esses selos de modo a gastar exatamente R$ 100,00?

(a) 2 (b) 3 (c) 4 (d) 5 (e)6

Alternativa correta: B

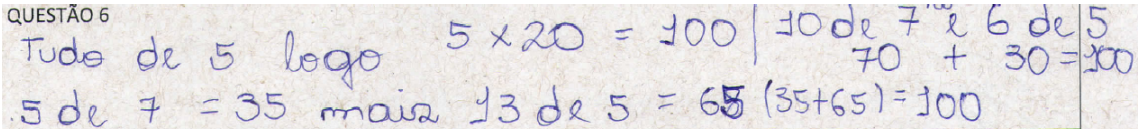
A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 6.

Tabela 6 – Questão 6T1

Alternativa	Percentual de alunos
a	5,5
b	66,7
c	5,5
d	0
e	0
n.a. (não assinalou)	22,2

Observando a **Tabela 6** verifica-se que 66,7 %, conseguiram resolver corretamente a questão. No entanto, para obterem a resposta correta, utilizaram o método de tentativa e erro a partir da alternativas oferecidas pela questão. No entanto, o objetivo era observar se eles iriam utilizar um modelo algébrico para a resolução desse problema, chegando a uma equação diofantina. Obviamente, pelo fato de não terem estudado esse assunto na educação básica, possivelmente, não resolveriam essa questão utilizando as ferramentas estudadas e fornecidas no estudo das equações diofantinas. Durante a abordagem desse assunto na ministração do curso, os alunos mostraram-se bastante motivados com as possibilidades de resolução de problemas a partir desse estudo. A seguir, segue imagem escaneada da resolução de um dos discentes participante do Teste 1.

Figura 2 – Resposta de um aluno - 2



Questão 7

No número $6a78b$, a denota o algarismo da unidade de milhar e b denota o algarismo da unidade. Se $6a78b$ for divisível por 45, então o valor de $a + b$ é:

(a) 2 (b) 3 (c) 4 (d) 5 (e)6

Alternativa correta: E

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 7.

Tabela 7 – Questão 7T1

Alternativa	Percentual de alunos
a	0
b	11,1
c	0
d	5,5
e	5,5
n.a. (não assinalou)	77,8

Essa questão aplicada é de nível básico e bastava ter o conhecimento das regras de divisibilidade por 5 e 9 para resolver tal questão, já que $(5, 9) = 1$, e portanto um número é múltiplo de 5 e 9 se, e somente se, for múltiplo de $5 \cdot 9 = 45$. No entanto, ao analisarmos a **Tabela 7**, nota-se que apenas um dos alunos assinalou a alternativa correta. Nessa questão, a maoria dos alunos $(77, 8\%)$ não assinalaram alternativa, possivelmente pelo fato de achar engenhoso substituir as letras a e b por valores que fizessem com que o número $6a78b$ se tornasse divisível por 45. Mais uma vez, ao abordarmos e demonstrarmos durante as aulas as regras de divisibilidade, os alunos mostraram-se bastante entusiasmados com as aplicações dessas regras na resolução de alguns exercícios desafiantes.

Questão 8

O dobro de um número dividido por 5 deixa resto 1. Qual é o resto da divisão desse número por 5?

(a) 2 (b) 3 (c) 4 (d) 5 (e) 6

Alternativa correta: B

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 8.

Tabela 8 – Questão 8T1

Alternativa	Percentual de alunos
a	0
b	22,2
c	0
d	11,1
e	11,1
n.a. (não assinalou)	55,6

Conhecimentos básicos de divisão euclidiana e do lema do resto seriam suficientes para resolver essa questão. Ao corrigirmos as respostas dos que acertaram essa questão, percebemos que os mesmos utilizaram a estratégia de considerar algum número cujo dobro ao ser dividido por 5 deixa resto 1 e, em seguida, analisaram a divisão desse número por 5. Os que acertaram essa questão, utilizaram o método de tentativa e erro para encontar o resto da divisão.

Questão 9

Se a e b são dois números naturais e $2a + b$ é divisível por 13, então qual dos números a seguir é múltiplo de 13?

(a) $91a + b$ (b) $92a + b$ (c) $93a + b$ (d) $94a + b$ (e) $95a + b$

Alternativa correta: C

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 9.

Tabela 9 – Questão 9T1

Alternativa	Percentual de alunos
a	16,7
b	0
c	11,1
d	0
e	0
n.a. (não assinalou)	72,2

Além do conhecimento de divisibilidade, para resolver essa questão necessitava-se de conhecimentos algébricos, a saber, soma de monômios. No entanto, os 11,1% dos alunos que conseguiram resolver esssa questão atribuíram valores para a e b de forma que $2a + b$ fosse um múltiplo de 13. Daí, ao encontrarem esses valores para a e b, substituíram os mesmos nas alternativas a fim de encontrar qual delas apresentava um múltiplo de 13.

Questão 10

Sejam p_1 e p_2 números primos positivos distintos que dividem n e $n^2 + 35$. Então, o valor de $p_1 + p_2$ é:

(a) 5 (b) 11 (c) 12 (d) 13 (e) 15

Alternativa correta: C

Por intermédio da tabela abaixo pode-se ver o percentual de alunos que assinalaram cada alternativa da questão 10.

Tabela 10 – Questão 10T1

Alternativa	Percentual de alunos
a	5,5
b	0
c	5,5
d	5,5
e	0
n.a. (não assinalou)	83,3

Nessa questão, o objetivo era saber o nível de conhecimento dos alunos no que tange aos números primos. Apenas um aluno constatou que, como os primos p_1 e p_2 dividem n, então, obviamente, dividem n^2. Daí, bastava analisar, por meio da decomposição em fatores primos, quais são os fatores primos de 35. Claramente, observa-se a limitação de conhecimento a respeito desse tema pois, de acordo com a **Tabela 10**, 83,3% dos alunos não tinham ideia de como fazer tal questão.

Questão 11

O ano de 2013 começou em uma terça-feira. Em que dia da semana cairá o último dia do ano?

(a) segunda-feira (b) terça-feira (c) quarta-feira (d) quinta-feira (e) sexta-feira

Alternativa correta: B

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 11.

Tabela 11 – Questão 11T1

Alternativa	Percentual de alunos
a	5,5
b	44,4
c	22,2
d	0
e	0
n.a. (não assinalou)	27,8

Observando a **Tabela 11** verifica-se que 44,4% dos discentes assinalaram a alternativa correta. Obviamente, pelo fato de ser uma questão de nível simples, a porcentagem

tão baixa de acertos, deixou-nos surpresos. Durante as aulas, tratamos de resolver bastantes exercícios com esse modelo de questão.

Questão 12

O valor da soma $1 + 2 + 3 + \cdots + 2014$ é um número:

(a) par (b) ímpar

Alternativa correta: B

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 12.

Tabela 12 – Questão 12T1

Alternativa	Percentual de alunos
a	22,2
b	55,5
n.a. (não assinalou)	22,2

Como era de se esperar, os alunos tentaram fazer essa questão realizando a soma de todas essas parcelas. É claro que tal cálculo é engenhoso, e porque não dizer, pedante. Portanto, apenas 55,5% dos alunos conseguiu achar a resposta correta.

Questão 13

Na divisão de 106 e 197 por 6 obtemos, respectivamente, restos 4 e 5. Qual é o resto da divisão de $106 \cdot 197$ por 6?

(a) 1 (b) 2 (c) 3 (d) 4 (e)5

Alternativa correta: B

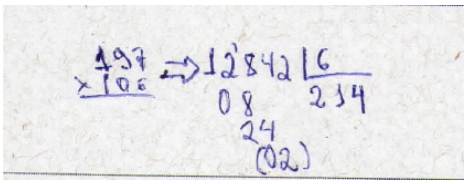
A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 13.

Tabela 13 – Questão 13T1

Alternativa	Percentual de alunos
a	5,5
b	77,8
c	5,5
d	0
e	5,5
n.a. (não assinalou)	5,5

Para resolver essa questão, bastava analisar os restos e, aplicando o Lema dos Restos, facilmente ela seria resolvida. O alto índice de acertos, $77,8\%$, conforme a **Tabela 13**, foi fruto da estratégia de multiplicar 106 por 197 e analisar o resto da divisão desse produto por 6. Provavelmente, os que erraram tal questão cometeram algum equívoco no produto de 106 por 197. É claro que com o Lema do Resto, facilmente essa questão seria resolvida. Deixamos bem claro para os alunos, durante o curso, que essa estratégia não seria suficiente em determinadas situações. A figura abaixo mostra tal estratégia realizada por um dos alunos.

Figura 3 – Resposta de um aluno - 3



Questão 14

Dois rolos de arame, um de 210 metros e outro de 330 metros, devem ser cortados em pedaços de mesmo comprimento. Quantos pedaços podem ser obtidos se desejamos que cada um destes pedaços tenha o maior comprimento possível?

(a) 18 (b) 19 (c) 20 (d) 25 (e)30

Alternativa correta: A

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 14.

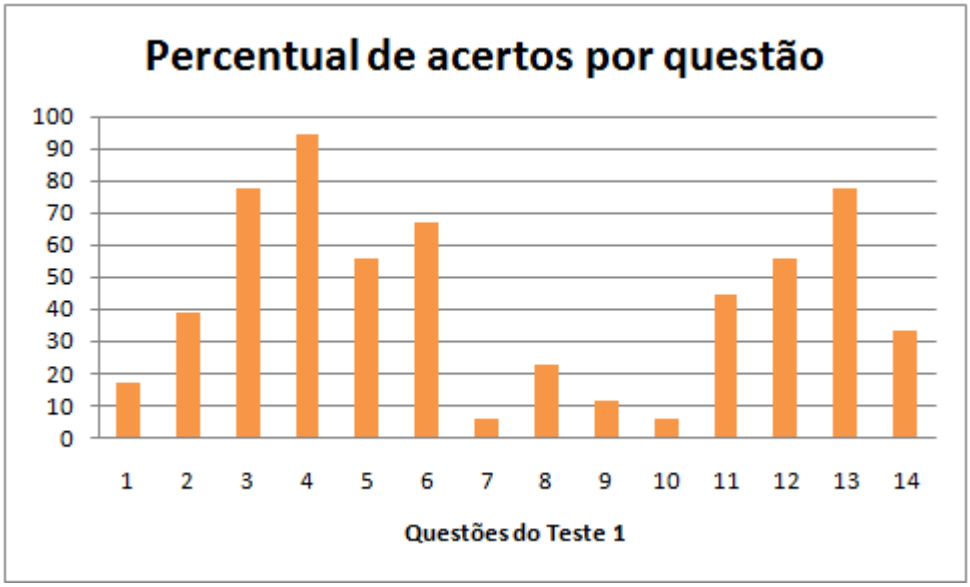
Tabela 14 – Questão 14T1

Alternativa	Percentual de alunos
a	33,4
b	11,1
c	11,1
d	22,2
e	0
n.a. (não assinalou)	22,2

É fácil ver que conhecimentos básicos do cálculo do MDC seriam suficientes para resolver essa questão. Nessa questão, apenas $33,4\%$ dos alunos assinalaram a alternativa correta.

1.2 Análise dos resultados

O gráfico abaixo mostra o percentual de alunos (de um total de 18 participantes) que acertaram cada questão do Teste 1. O percentual médio de acertos por questão foi de aproximadamente 43,24%.



O gráfico acima é uma síntese dos resultados do Teste 1. Nota-se que a questão 4, cujo nível é simples e aborda uma aplicação da divisão euclidiana, teve um maior percentual de acerto. Por outro lado, oberva-se que nas questões 7 e 10, que envolvem conhecimentos um pouco mais aprofundados da Teoria dos Números, os alunos avaliados tiveram uma maior dificuldade de obter sucesso. Ao analisarmos esse gráfico, vemos que, apesar do ensino de alguns conceitos básicos da teoria dos números fazerem parte do currículo obrigatório do ensino básico, tais conceitos não são vistos de forma aprofundada neste nível de ensino. Além disso, alguns outros temas como congruências, equações diofantinas, etc; não fazem parte do currículo obrigatório. Uma consequência dessa situação é que uma ótima oportunidade de desenvolver nos alunos o gosto pela matemática através de desafios interessantes é perdida. Mais ainda, tais conceitos possibilitam o desenvolvimento de várias habilidades nos alunos desse nível de ensino.

Segundo Resende em [17, p. 209]:

> [...] A Teoria dos Números, ao ter como foco o estudo dos números inteiros, é um campo propício para o desenvolvimento de atividades investigativas, pois a exploração de padrões e de relações numéricas, o uso da recursão e da indução matemática, envolvendo os inteiros, a divisibilidade e números primos estiveram e estão presentes na matemática e podem ser exploradas nas atividades escolares, em qualquer nível.

No entanto, a Teoria dos Números não tem sido explorada de forma adequada na educação básica. Muitas situações-problema podem ser exploradas ao estudarmos os conteúdos

dessa teoria e que possibilitariam aos estudantes do ensino básico um excelente desenvolvimento das habilidades matemáticas propostas pelos PCN's. Uma delas, segundo os PCN's em [4, p. 42] é:

> Desenvolver as capacidades de raciocínio e resolução de problemas, de comunicação, bem como o espírito crítico e criativo.

Nesse sentido, sugerimos que tais temas sejam abordados como uma ferramenta facilitadora da aproximação dos alunos com a matemática visto que dentre as várias habilidades que podem ser construídas pelos alunos, destacamos a questão do desenvolvimento do raciocínio generalizador, que é fundamental no estudo da matemática. Essa nossa sugestão é, em parte, sugerida também pela proposta de currículo de matemática para o ensino médio elaborada em 2014 pela SBM (Sociedade Brasileira de Matemática) em conjunto com professores universitários e professores atuantes na educação básica. A proposta foi elaborada para o Ensino Médio, Ensino Fundamental 1, Ensino Fundamental 2 e Ensino Superior. Iremos destacar, no entanto, a sugestão de proposta para o Ensino Médio visto que foi para alunos nessa fase de ensino que realizamos os Testes 1 e 2, bem como o curso básico. A figura seguir é um recorte de tal proposta para a 1ª série do Ensino Médio no eixo Aritmética:

Figura 4 – Proposta de Currículo para a 1ª série do Ensino Médio sugerida pela SBM no eixo Aritmética

1ª Série - Área: Matemática Discreta

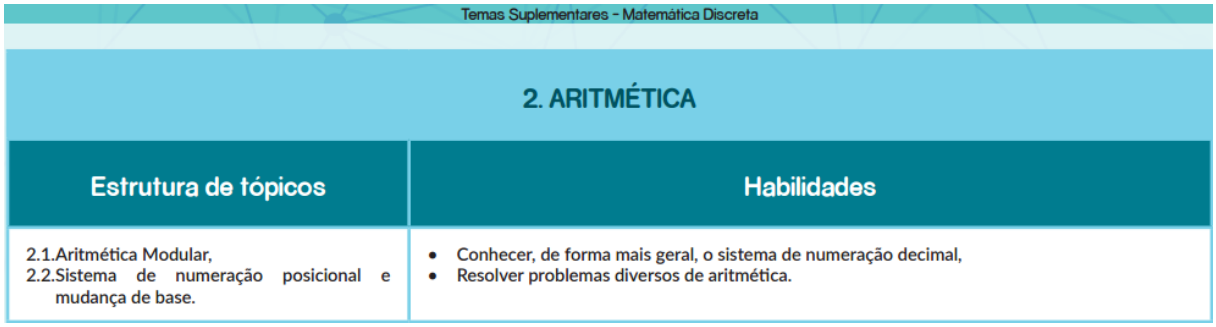
2. ARITMÉTICA

Estrutura de tópicos	Habilidades
2.1. Divisão Euclidiana, discussão sobre diferentes algoritmos e procedimentos e suas relações com a estrutura do sistema posicional de numeração. 2.2. Divisibilidade e Resto: aritmética dos restos, múltiplos e divisores, números primos, fatoração e critérios de divisibilidade; 2.3. Máximo Divisor Comum; 2.4. Mínimo Múltiplo Comum.	• Valorizar os números naturais, em suas aplicações, como um dos conceitos mais antigos concebidos pelo ser humano; • Compreender o Algoritmo de Euclides; • Reconhecer proposições e propriedades dos múltiplos e divisores de um número, fatorar e saber usar os critérios de divisibilidade; • Demonstrar propriedades do Máximo Divisor Comum e do Mínimo Múltiplo comum de dois números; • Conhecer aplicações em torno do estudo da aritmética, favorecendo a relação teoria-prática no contexto de mundo.

Fonte: Sociedade Brasileira de Matemática

Nessa mesma proposta curricular sugerida pela SBM, existe a sugestão da inclusão de outros temas da Teoria dos Números, no entanto, como temas complementares. A figura a seguir é um recorte dessa sugestão:

Figura 5 – Proposta de Currículo para o Ensino Médio sugerida pela SBM no eixo Aritmética - Temas Suplementares



Temas Suplementares - Matemática Discreta

2. ARITMÉTICA

Estrutura de tópicos	Habilidades
2.1.Aritmética Modular, 2.2.Sistema de numeração posicional e mudança de base.	• Conhecer, de forma mais geral, o sistema de numeração decimal, • Resolver problemas diversos de aritmética.

Fonte: Sociedade Brasileira de Matemática

Tal proposta visa contribuir com uma discussão que, no nosso entendimento, deve ser contínua na busca de encontrar sempre um currículo de matemática, para a Educação Básica no Brasil, que consiga proporcionar uma significativa melhora na aprendizagem dos alunos e desconstruir alguns mitos no que tange à disciplina de matemática, como por exemplo a ideia de que a matemática é um disciplina acessível apenas para alguns. Ideias como essa distanciam cada vez mais os alunos da matemática e contribuem fortemente para um desempenho ruim dos mesmos na disciplina.

2 A parte prática do trabalho

Neste capítulo apresentamos o material didático que foi desenvolvido para o Curso Básico de Teoria dos Números bem como os planos de aula elaborados para cada tema proposto nesse curso, além de um breve relatório de cada aula. As aulas foram ministradas numa turma do 4º período do curso técnico de Edificações equivalente ao 2º ano do ensino médio de uma turma do ensino médio regular. As aulas ocorreram nas segundas e terça-feiras e cada aula teve duração de 45 minutos. A tabela abaixo indica a quantidade de aulas nas quais foram abordados os respectivos conteúdos dos planos de aula. A proposta inicial era de 10 encontros, sendo cada encotro de duas aulas. No entanto, foram necessários mais de 10 encontros para concluirmos o curso.

Tabela 15 – Quantidade de aulas por tema

Plano	Total de aulas
1	2
2	2
3	2
4	2
5	4
6	2
7	3
8	3
9	2
10	2

2.1 Divisibilidade

Plano de Aula

Tema: Divisibilidade

Objetivos:
Levar o(a) aluno(a) a:

- Estudar o conceito de divisibilidade e suas propriedades;
- Reconhecer quando um número inteiro divide outro inteiro;
- Usar as propriedades básicas da divisão de inteiros na resolução de problemas.

Conteúdos:
Divisibilidade e suas propriedades; Conjunto dos divisores de um número inteiro.

Metodologia:
Iniciaremos a aula com um vídeo sobre múltiplos e divisores do Telecurso 2000, problematizando o tema a ser estudado. Após o vídeo, iniciaremos uma discussão sobre as condições para que um número inteiro seja divisível por outro inteiro. Em seguida, formalizaremos a definição de divisibilidade, mostraremos e demonstraremos as propriedades da divisibilidade e, por fim, resolveremos alguns exercícios propostos no texto da aula.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila.

Referências:

- Bracher, Daniele. **IV EIEMAR Escola de Inverno de Educação Matemática**. UFPel. Disponível em `http://w3.ufsm.br/ceem/eiemat/Anais/arquivos/ed_4/RE/RE_Bracher_Daniele.pdf`. Acesso em 12/09/2016.
- Dias, Cristina Helena Bovo Batista.**Numeros primos e divisibilidade: Um estudo de propriedades**. 2013.49f. Dissertação (Mestrado Profissional em Matemática). Universidade Estadual Paulista, São Paulo.
- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Moreira, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª**. 1ª ed. Rio de Janeiro: SBM, 2003.

Texto didático

> "A matemática é a rainha das ciências e a teoria dos números é a rainha da matemática".
>
> Carl Friedrich Gauss

A Teoria dos Números é o ramo da matemática pura que estuda propriedades dos números inteiros, bem como a larga classe de problemas que surge no seu estudo. O estudo de tais propriedades vem, ao longo dos anos, causando grande fascínio entre grandes matemáticos, tais como Euclides (390 a.C), Pitágoras (569-500 a.C), Eratóstenes (276-196 a.C), Leonhard Euler (1707-1783) , Pierre de Fermat (1601-1665), entre outros. O termo aritmética (arithmetiké) vem do idioma grego e literalmente significa "ciência dos números", e é também usado para referir-se a Teoria dos Números. Nesse curso, vamos estudar vários temas como o conceito de Divisibilidade e suas propriedades , a Teoria das Congruências (também chamada de aritmética dos restos), Equações Diofantinas, dentre outros. Vale ressaltar que o objetivo desse curso não é um longo aprofundamento dessa teoria que, como foi dito antes, é muito vasta. O foco é estudar alguns conceitos básicos e utilizá-los como facilitador na resolução de vários problemas cuja solução seria bastante engenhosa sem uso de tal teoria. Desta forma, abriremos mão de algumas demonstrações. No entanto, tal procedimento não comprometerá o desenvolvimento do trabalho. Vamos lá e bons estudos!

Para início de conversa, vamos falar de um conceito muito importante no estudo da teoria dos números. Esse conceito é chamado de divisibilidade. Mas, do que trata tal conceito? Vejamos a seguir.

Na Teoria dos Números, é imprescindível o estudo do conceito de divisibilidade de inteiros e suas propriedades. Tal estudo possibilitará, de uma maneira bastante prática, a resolução de exercícios bastante interessantes.

Por volta de 300 a.c, o matemático Euclides deu importantes contribuições para o desenvolvimento desse conceito, através da sua obra intitulada de "Os Elementos". Inicialmente, vamos estudar a definição de divisibilidade e suas principais propriedades e, em seguida, analisaremos alguns exemplos resolvidos e tentaremos resolver alguns exercícios bem desafiantes.

Definição 2.1.1. *Sejam a e b inteiros com $a \neq 0$. Dizemos que a é um divisor de b ou que b um múltiplo de a, se existir um inteiro c tal que $b = ac$. Isto será denotado por $a \mid b$ e o caso contrário será denotado por $a \nmid b$.*

Por exemplo, $8 \mid 24$ pois $24 = 3.8$. Verifique se $9 \mid 54$ e se $5 \mid 64$.

É fácil ver que $1 \mid a$ para todo a inteiro, $a \mid a$ e $a \mid 0$ para todo $a \neq 0$, $a \in \mathbb{Z}$. De fato, temos que $a = 1 \cdot a$, para todo $a \in \mathbb{Z}$ e que $0 = a \cdot 0$, para todo inteiro a, $a \neq 0$.

As propriedades que serão vistas a seguir serão de fundamental importância pois se revelarão bastante úteis na resolução de vários exercícios. A princípio, tente verificar através de alguns exemplos numéricos a veracidade de cada afirmação abaixo.

1. Sejam a, b e c inteiros, $a \neq 0$, $b \neq 0$. Se $a \mid b$ e $b \mid c$, então $a \mid c$.
2. Sejam a, b, c, e d inteiros, $a \neq 0$, $c \neq 0$. Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.
3. Sejam a, m e n inteiros, com $a \neq 0$ e $n \neq 0$. Se $an \mid am$, então $n \mid m$.
4. Sejam a, b e c inteiros, com $a \neq 0$. Se $a \mid (b + c)$, então $a \mid b$ se, e somente se, $a \mid c$.
5. Sejam a, b e c inteiros, com $a \neq 0$. Se $a \mid (b - c)$, então $a \mid b$ se, e somente se, $a \mid c$.
6. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|b$ e $a|c$, então $a \mid (bx \pm cy)$ para quaisquer x, y inteiros.
7. Dados os inteiros positivos a e b. Temos que se $a \mid b$, então $b \geq a$.

Vejamos agora as demonstrações de cada propriedade.

Demonstrações:

1. Se $a \mid b$, então podemos escrever $b = am$, para algum $m \in \mathbb{Z}$. Por outro lado, como $b \mid c$, então podemos escrever $c = bn$, para algum $n \in \mathbb{Z}$. Portanto, teremos que $c = bn = a(mn)$, o que mostra que $a \mid c$.
2. Se $a \mid b$ então podemos escrever $b = am$ para algum $m \in \mathbb{Z}$. Por outro lado, se $c \mid d$ então $d = cn$, para algum $n \in \mathbb{Z}$. Dái, temos que $b \cdot d = (ac)(mn)$, o que mostra que $ac \mid bd$.
3. De fato, como $an \mid m$, temos que existe k inteiro tal que $am = (an)k$. Ora, como $a \neq 0$, podemos dividir ambos os membros por a, o que vai resultar $m = nk$, o que mostra que $n \mid m$.
4. Como $a \mid (b + c)$, existe $k \in \mathbb{Z}$ tal que $b + c = ak$. Mais ainda, como $a|b$, temos que existe $r \in \mathbb{Z}$ tal que $b = ar$. A partir das duas igualdades, concluímos que

$$ar + c = ak,$$

Logo, temos que

$$c = ak - ar = a(k - r),$$

o que implica que $a \mid c$. Ficará como exercício para o leitor a demonstração da outra implicação.

5. A demonstração dessa propriedade também fica a cargo do leitor pois tem uma demonstração análoga à da propriedade anterior.

6. De fato, como $a \mid b$ e $a \mid c$, então existem inteiros m e n tais que $b = am$ e $c = an$. Daí, temos que

$$bx \pm cy = (am)x \pm (an)y = a(mx) \pm a(ny) = a(mx \pm ny), \text{ para todo } x, y \in \mathbb{Z},$$

donde concluí-se que $a \mid (bx \pm cy)$.

7. Com efeito, como $a \mid b$, então existe um inteiro k, positivo, tal que $b = ak$. Daí, é fácil ver que $a \leq b$, pois como $a > 0$ e $k > 0$, temos que $a \leq ak = b$.

Observe um interessante exemplo que trata do tema divisibilidade: prove que o número $N = 5^{45362} - 7$ não é divisível por 5. Para provarmos essa afirmação, utilizaremos um método matemático chamado de redução ao absurdo. Suponhamos que esse número fosse divisível por 5. Sendo assim, teríamos $5^{45362} - 7 = 5r$, para algum $r \in \mathbb{Z}$. Daí, teríamos $7 = 5^{45632} - 5r$. É claro que o número 5^{45632} é um múltiplo de 5, consequentemente, para algum inteiro $q \in \mathbb{Z}$, teríamos também $7 = 5q - 5r = 5\underbrace{(q - r)}_{\in\mathbb{Z}}$, o que é um absurdo pois 7 não é múltiplo de 5. É possível também resolvermos esse problema utilizando as propriedades vistas anteriormente. Utilizaremos a propriedade 6. Para isso, observemos que como $5 \mid 5^{45362}$, pela propriedade 5 temos que se $5 \mid 5^{45362} - 7$, então $5 \mid 7$, o que não é verdade, mostrando assim que $5 \nmid 5^{45362} - 7$.

Outro exemplo bastante interessante, é resolvermos o seguinte problema: Se a e b são dois números naturais e $2a+b$ é divisível por 13, podemos afirmar que $93a+b$ também é múltiplo de 13? A resposta é sim!

De fato, temos que $93a+b = 91a+(2a+b)$. Ora, como $13 \mid 91a$, pois $91a = 13 \cdot (7a)$ e, por hipótese, $13 \mid 2a + b$, concluímos que $13 \mid 93a + b$.

Definição 2.1.2. *Chamamos de conjunto dos divisores naturais de um natural n dado, e indicamos por $D(n)$, os naturais de quem n é múltiplo.*

Por exemplo, sendo $n = 20$, temos $D(20) = \{1, 2, 4, 5, 10, 20\}$.

Se $D(n)$ tem exatamente dois elementos, isto é, $D(n) = \{1, n\}$, dizemos que n é um número primo. Por exemplo, o número 7 possui apenas dois divisores, 1 e 7.

Números como esse serão objeto de estudo numa outra seção, onde abordaremos com mais detalhes as propriedades dos números primos. Tais propriedades servirão, inclusive, para determinarmos a quantidade de divisores inteiros de um número inteiro dado.

Vejamos agora as aplicações das propriedades estudadas nos exercícios propostos a seguir.

Exercícios

Questão 1. *(OBMEP 2011 - N2Q3 - 2a fase) O múltiplo irado de um número natural é o menor múltiplo do número formado apenas pelos algarismos 0 e 1. Por exemplo, o múltiplo irado de 2, bem como de 5, é 10; já o múltiplo irado de 3 é 111 e o de 110 é ele mesmo.*

a) Qual é o múltiplo irado de 20?

b) Qual é o múltiplo irado de 9?

c) Qual é o múltiplo irado de 45?

d) Qual é o menor número natural cujo múltiplo irado é 1110?

Questão 2. *Verifique que 3 divide 228 e que 5 divide 725, mas 15 não divide 228 nem 725. Por que isso acontece?*

Questão 3. *Usando as propriedades vistas anteriormente, prove que* $3 \mid (12m+21n)$ *para todos os inteiros* m *e* n*.*

Questão 4. *Verifique se a soma de três múltiplos de 5 também será um múltiplo de 5.*

Questão 5. *Explique porque um divisor comum de 105 e 60 tem de ser um divisor comum de 45.*

Questão 6. *Encontre todos os divisores de 30.*

Questão 7. *Para quais valores de* $a \in \mathbb{Z}$ *vale*

1. $a-2 \mid a^3+4$*?*
2. $a+3 \mid a^3-3$*?*

Questão 8. *(DESAFIO - IMO) - Mostre que a fração* $\dfrac{21n+4}{14n+3}$ *é irredutível para todo* n *natural.*

Questão 9. *(PROFMAT) Sejam* x *e* y *números inteiros tais que* $10x+y$ *seja um múltiplo de* 7*. Assinale a alternativa correta.*

a) $x-2y$ *será certamente um múltiplo de* 7*.*

b) $2x+y$ *será certamente um múltiplo de* 7*.*

c) $x - y$ *será certamente um múltiplo de 7.*

d) $2x - y$ *será certamente um múltiplo de* 7.

Questão 10. *(COLÉGIO NAVAL - 1984) O resto da divisão* $1211^{20} + 9119^{32} \cdot 343^{26}$ *por 11 é:*

a) 0

b) 1

c) 2

d) 3

e) 4

Relatório

Na primeira aula, cujo objetivo era estudar o conceito de divisibilidade, antes de iniciarmos o conteúdo, discutimos um pouco sobre o Teste 1 aplicado. Os alunos falaram que acharam as questões, na sua maioria, muito difíceis. No entanto, falei que os conteúdos que iríamos estudar no curso seriam uma ferramenta bastante útil na resolução dos mesmos e que a medida que eles fossem adquirindo os conhecimentos trabalhados nas aulas, eles iriam ter um novo olhar sobre cada questão. Em seguida, foi passado um vídeo sobre múltiplos e divisores do Telecurso 2000 que mostrou, de maneira bem dinâmica e criativa, segundo os alunos, o conceito de divisibilidade. Em seguida, tratamos do tema de uma maneira mais formal.

Ainda nessa primeira aula, ficou notório o quanto os alunos não estavam acostumados com o conceito de divisibilidade bem como com a linguagem algébrica fundamental para a demonstração das propriedades que seriam estudadas. Sendo assim, utilizei bastante exemplos para somente depois, fazer as demonstrações das propriedades da divisibilidade. Enfatizei muito o fato de na matemática, não podermos fazer generalizações a partir de alguns exemplos que foram válidos em alguns casos estudados. Para generalizar é preciso fazer as devidas demonstrações não abrindo mão do rigor matemático e, para isso, seria necessário eles se acostumarem com esse tipo de abordagem matemática. Obviamente, na resolução dos exercícios ficou claro o quanto eles não estavam acostumados com esses tipos de exercícios, mas aos poucos, eles começaram a entender as ideias. Inclusive, resolvemos algumas questões que foram abordadas no Teste 1 e um novo olhar sobre as questões foi se concretizando.

2.2 Divisão Euclidiana

Plano de Aula

Tema: Divisão Euclidiana

Objetivos:
Levar o(a) aluno(a) a:

- Estudar e compreender o desenvolvimento do Algoritmo da Divisão;
- Verificar as aplicabilidades do Algoritmo da Divisão no estudo da Teoria dos Números;
- Fazer uso do algoritmo da divisão na solução de problemas envolvendo números inteiros;
- Expressar um número inteiro de forma única a partir da sua divisão por outro número inteiro.

Conteúdos:
Algoritmo da divisão e suas propriedades.

Metodologia:
Iniciaremos a aula com um jogo chamado de Jogo do Resto. Nesse jogo, trabalharemos situações em que a divisão de um inteiro por outro não é exata introduzindo de maneira formal o conceito de dividendo, divisor, quociente e resto. Em seguida, trabalharemos as propriedades do algoritmo da divisão e as usaremos para a resolução de alguns exercícios.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, notebook, data-show e apostila.

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- MOREIRA, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Moreira, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª**. 1ª ed. Rio de Janeiro: SBM, 2003.
- Oliveira, Krerley Irraciel Martins. **Iniciação à Matemática: um curso com problemas e soluções**. 2ª ed. Rio de Janeiro: SBM, 2010.
- Tao, Terence. **Como resolver problemas matemáticos - Uma perspectiva pessoal**. Rio de Janeiro: SBM, 2013.
- Zeni, José Ricardo de Rezende. **Três Jogos para o Ensino e Aprendizagem de Números e Operações no Ensino Fundamental**. Universidade Estadual Paulista (UNESP). Disponível em `http://www.feg.unesp.br/ jrzeni/pesquisa/2007/3Jogos/3Jogos-Zeni.pdf`. Acesso em 12/09/2016.

Texto didático

No estudo da divisibilidade nos inteiros, vimos que dados os inteiros a, b, com $a \neq 0$, o inteiro a é um divisor do inteiro b se existir outro inteiro c tal que $b = ac$ e indicamos por $a \mid b$. No entanto, quando isso não ocorre, dizemos que a não divide b e indicamos $a \nmid b$.

A seguir, estudaremos um algoritmo que, apesar de simples, é uma das ferramentas mais poderosas no estudo da Teoria dos Números e que inclui este último caso, ou seja, quando $a \nmid b$. Esse algoritmo é chamado de Algoritmo da Divisão. Tal algoritmo foi apresentado pelo matemático Euclides e é bastante útil na resolução de diversos problemas interessantes.

Teorema 2.2.1 (Algoritmo da divisão)**.** *Dados dois inteiros b e a, com $a \neq 0$, existem dois únicos inteiros q e r, tais que*

$$b = a \cdot q + r, \quad com \quad 0 \leq r < |a|,$$

Neste caso o número b é chamado de dividendo, a é chamado de divisor, q é chamado de quociente e r é chamado de resto da divisão.

Por exemplo, $13 = 5 \cdot 2 + 3$ e isto significa dizer que ao dividirmos 13 por 5, o quociente é 2 e o resto dessa divisão é 3. Vejamos também que $4 = 5 \cdot 0 + 4$, ou seja, na divisão de 4 por 5, o quociente é 0 e o resto é 4. Logo abaixo, veremos a demonstração desse algoritmo.

Demonstração . *Considere o número inteiro a, com $a > 0$ (para $a < 0$, o procedimento é análogo). Podemos escrever o conjunto dos números inteiros da seguinte forma:*

$$\mathbb{Z} = ... \cup \big[-2a, -a\big) \cup \big[-a, 0\big) \cup \big[0, a\big) \cup \big[a, 2a\big) \cup \big[2a, 3a\big) \cup ... \cup \big[qa, (q+1)a\big) \cup ...$$

Os subconjuntos descritos acima são disjuntos dois a dois, ou seja, sendo b um inteiro qualquer, temos que b pertence a apenas um desses subconjuntos, sendo portanto único. Mais ainda, podemos escrever:

$$qa \leq b < (q+1)a = qa + a \Rightarrow 0 \leq \underbrace{b - qa}_{r} < a.$$

Desta forma, r é únicamente determinado e

$$b = qa + r, \text{ com } 0 \leq r < a.$$

■

Por exemplo, ao dividirmos 19 por 5, temos que $q = 3$ e $r = 4$. Por outro lado, ao dividirmos -19 por 5, obteremos $q = -4$ e $r = 1$.

Uma das importantes consequências do Algoritmo da Divisão é saber que ao dividirmos um inteiro b por um inteiro a, $a \neq 0$, o resto r dessa divisão pertence ao conjunto $\{0, 1, 2, 3, ..., a-1\}$. Estudando o caso em que $a = 2$, temos que o resto r da divisão de b por a será 0 ou 1. Se $r = 0$, temos que $b = 2 \cdot q$, com q inteiro e, nesse caso, dizemos que b é um número par. Se $r = 1$, escrevemos $b = 2 \cdot q + 1$, com q inteiro e, nesse caso, dizemos que b é um número ímpar. Tal análise, permite-nos generalizar e dizer que todo inteiro b pode ser expresso na forma $2 \cdot q$ ou $2 \cdot q + 1$, com $q \in \mathbb{Z}$. Analogamente, no caso em que $a = 3$, temos que b será da forma $3 \cdot q$, $3 \cdot q + 1$ ou $3 \cdot q + 2$, com q inteiro.

A seguir, estudaremos um importante resultado conhecido como Lema dos Restos.

Lema 2.2.1 (Lema dos Restos)**.** *A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, respectivamente, na divisão por um inteiro a, $a \neq 0$.*

Demonstração . *Sejam n_1 e $n_2 \in \mathbb{Z}$. Ao fazermos a divisão com resto desses dois números por a, teremos*

$$n_1 = aq_1 + r_1 \text{ e } n_2 = aq_2 + r_2,$$

onde $0 \leq r_1, r_2 < a$. *Daí, teremos*

$$\begin{aligned} n_1 n_2 &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 \\ &= aq + r_1 r_2 \end{aligned} \tag{2.1}$$

onde vamos considerar $q \in \mathbb{Z}$ *e* $q = aq_1 q_2 + q_1 r_2 + q_2 r_1$. *Mais ainda, ao dividirmos* $r_1 r_2$ *por* a, *teremos*

$$r_1 r_2 = ap + r, \quad p \in \mathbb{Z}, \quad 0 \leq r < a, \tag{2.2}$$

daí, de (2.1) *e* (2.2), *concluí-se que*

$$n_1 n_2 = aq + ap + r = a(p + q) + r,\ 0 \leq r < a.$$

■

A demonstração para a soma é muito simples e tem procedimento anàlogo ao anterior, ficando portanto como exercício.

Por exemplo, ao dividirmos 18 e 17 por 5, os restos dessas duas divisões serão 3 e 2, respectivamente. De fato, temos

$$18 = 5 \cdot 3 + 3 \quad \text{e} \quad 17 = 5 \cdot 3 + 2.$$

Pelo lema dos restos, o resto da divisão de $18 + 17$ por 5 será igual ao resto da divisão $3 + 2 = 5$ por 5, ou seja, será 0.

Por outro lado, o resto da divisão de $18 \cdot 17$ por 5 será, pelo lema dos restos, igual ao resto da divisão de $3 \cdot 2 = 6$ por 5, e portanto igual a 1.

É claro que os exemplos vistos anteriormente são bastante simples, mas servem como um ponto de partida para análise de casos mais interessantes, como o que segue. Qual é o resto da divisão de 3^{250} por 4? À primeira vista, parece praticamente impossível descobrirmos qual é o resto dessa divisão. Nesse caso, como o lema dos restos pode contribuir? Vejamos!

Note que, ao dividirmos $3^2 = 9$ por 4, o resto dessa divisão é igual a 1. Como $3^{250} = (3^2)^{125}$, temos, pelo lema dos restos, que o resto da divisão de 3^{250} por 4 será igual ao resto da divisão do produto $\underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdots \cdot 1}_{125 fatores} = 1$ por 4, ou seja, o resto será 1.

Para finalizarmos, vejamos um outro exemplo. Qual é o resto da divisão de $3^{100}+5^{45}$ por 2? Inicialmente, note que o resto da divisão de 3 por 2, é 1. Portanto, pelo lema dos restos, temos que o resto da divisão de 3^{100} por 2 será igual ao resto da divisão de $1^{100} = 1$ por 2, ou seja, igual a 1. Por outro lado, o resto da divisão de 5 por 2 também é igual a 1, sendo assim, o resto da divisão de 5^{45} por 2 será igual ao resto da divisão de $1^{45} = 1$ por 2, consequentemente, esse resto será igual a 1. Sendo assim, o resto da divisão de $3^{100} + 5^{45}$ por 2 será o resto da divisão $1 + 1 = 2$ por 2, sendo, portanto igual a 0.

Observemos então como o Lema dos Restos é uma ferramenta poderosa para resolvermos vários problemas que, aparentemente, seriam bastante difíceis.

Logo abaixo, indicamos alguns exercícios bastante desafiantes a respeito dos conteúdos que estudamos nessa seção.

Exercícios

Questão 11. *Encontre o quociente e o resto na divisão de*

a) 227 *por* 143

b) 1479 *por* 272

c) 2378 *por* 1769

Questão 12. *Quantos naturais entre* 100 *e* 200 *deixam resto* 5 *quando divididos por* 7*?*

Questão 13. *Encontre o resto da divisão de*

a) 2^{2009} *por* 3

b) 15^{2008} *por* 7

Questão 14. *O resto da divisão de um número inteiro n por* 15 *é* 5*. Qual é o resto da divisão de n por* 7*?*

Questão 15. *(OBM) Mostre que se n é um inteiro ímpar, então* $n^2 - 1$ *é divisível por* 8*.*

Questão 16. *Os números inteiros positivos são arrumados em* 7 *colunas conforme a disposição a seguir:*
Qual é a linha e coluna em que se encontra o número 1500*?*

Questão 17. *Joãozinho exagerou na bagunça na sala de aula e o professor, como forma de castigo, mandou que ele resolvesse o seguinte problema: "Encontre um número natural, maior do que* 100*, cujo quadrado ao ser dividido por* 3 *deixa resto* 2*". Sabendo-se que Joãozinho respondeu corretamente, qual foi uma possível resposta de Joãozinho?*

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
...	...	...	...	...	...	...
...	...	...	...	...	...	...

Questão 18. *Mostre que o produto de dois números naturais consecutivos é sempre divisível por* 2.

Questão 19. *Seja n um inteiro. Prove que a divisão de* n^2 *por 6, nunca deixa resto 2.*

Questão 20. *(ENC - 2002) o resto da divisão do inteiro N por* 20 *é* 8. *Qual é o resto da divisão de N por* 5*?*

Questão 21. *Na divisão euclidiana de a por b o quociente é* 6 *e o resto, o menor possível. Ache a e b nos seguintes casos:*

a) $a - b = 525$

b) $a + b = 234$

Questão 22. *(UFMG) Na divisão de dois números inteiros, o quociente é 16 e o resto é o maior possível. Sabendo que a soma do dividendo e do divisor é 125, descubra qual é o resto dessa divisão.*

Questão 23. *(OBMEP) A professora de Emília comprou 96 balas para repartir igualmente entre seus alunos, sem que sobrassem balas. No dia da distribuição todos os alunos foram à escola, exceto Emília. A professora distribuiu igualmente as balas entre os alunos presentes, mas sobraram 5 balas. Quantos alunos tem a turma de Emília?*

Relatório

Na aula do algoritmo da divisão, o que chamou muito a atenção foi o fato dos alunos ficaram surpresos com a demonstração desse referido algoritmo. Um fato curioso, foi os alunos não saberem que, ao dividirmos, por exemplo, 5 por 7, o quociente é 0 e o resto é 5. De fato, tal situação foi inicialmente observada quando fizemos a aplicação do jogo do resto. A aplicação desse jogo durou aproximadamente 20 minutos. No desenrolar da partida fiz algumas intervenções no início em relação às regras, mas logo os alunos entenderam o jogo, que foi uma forma de prepará-los para as definições que estavam por vir.

Um outro caso bastante interessante e que causou bastante euforia entre os alunos foi o Lema dos Restos e o quanto ele é fundamental na resolução de exercícios interes-

santíssimos. Resolvemos exercícios que, aparentemente, pareciam muito difíceis já nos preparando para o estudo da aritmética modular.

Figura 6 – Alunos jogando o Jogo do Resto

Fonte: Foto tirada pelo autor

2.3 Paridade de inteiros

Plano de Aula

Tema: Paridade de Inteiros

Objetivos:
Levar o(a) aluno(a) a:

- Estudar a aplicabilidade da paridade de inteiros na resolução de várias situações problemas;
- Resolver problemas que envolvam a paridade de inteiros;
- Compreender o sistema binário;
- Compreender e identificar os diversos padrões na resolução de problemas que envolvem a paridade de inteiros.

Conteúdos:
Paridade de Inteiros; Propriedades da Paridade de Inteiros.

Metodologia:
Iniciaremos a aula discutindo quais as estratégias utilizadas pelos alunos para resolver a questão 12 do Teste 1. Em seguida, falaremos sobre o conceito de paridade e as suas respectivas propriedades. A partir daí, resolveremos alguns problemas contextualizados envolvendo o tema. Por fim, falaremos sobre o sistema binário e iremos propor um desafio chamado de "mágica dos números" que trabalhará os temas paridade e sistema binário.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Fonseca, Rubens.**Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Sampaio, João C.V. **Mágica com os números**. Revista do Professor de Matemática - RPM, Edição Especial, SBM, São Paulo, 2009.

Texto didático

Dando continuidade ao assunto, vamos tentar resolver esse interessante desafio: Em um quartel existem 100 soldados e, todas as noites, três deles são escolhidos para trabalhar na sentinela. É possível que após certo tempo um dos soldados tenha trabalhado com cada um de todos os outros exatamente uma vez?

Para responder essa pergunta, vamos estudar um conceito que embora pareça bastante trivial, é uma ferramenta extremamente poderosa na resolução de problemas matemáticos envolvendo os números inteiros. Esse conceito é chamado de paridade.

Definição 2.3.1. - *Dizemos que um inteiro n é par se ele puder ser expresso na forma $2k$,com k inteiro. Por outro lado, dizemos que um inteiro n é ímpar, se for expresso na $2k+1$, para algum inteiro k.*

Temos como exemplos de números pares, os inteiros 34, 58 *e* -18. *E, como exemplos de números ímpares, os inteiros* 3, 55 *e* -15.

Teorema 2.3.1. - *Todo número inteiro ou é par ou é ímpar.*

Demonstração . *De fato, pelo algoritmo da divisão, o resto da divisão de um número inteiro n por 2 poderá ser 0 ou 1. Se o resto for 0, $n = 2k$ para algum inteiro k e nesse caso n é dito par. Se o resto for 1, $n = 2k+1$, com k inteiro.*

■

Definição 2.3.2. *Dois inteiros possuem a mesma paridade quando ambos forem pares ou ímpares.*

Paridade da soma de dois inteiros - Analisaremos o que acontece quando somamos dois inteiros quaisquer.

Proposição 2.3.1. *A soma de dois inteiros pares resulta em um número par.*

Demonstração . *Sejam a e b dois inteiros pares. Logo, podemos escrever $a = 2k$ e $b = 2k'$, com k, $k' \in \mathbb{Z}$. Daí, temos que,*

$$a + b = 2\underbrace{(k + k')}_{\in\mathbb{Z}} = 2r,$$

o que mostra que a soma de dois inteiros pares é par.

■

Proposição 2.3.2. *A soma de um inteiro par com um inteiro ímpar, resulta em um inteiro ímpar.*

Demonstração . *Com efeito, sejam a e b inteiros par e ímpar, respectivamente. Podemos escrever então $a = 2k$ e $b = 2k' + 1$. Portanto, temos*

$$a + b = 2k + 2k' + 1 = 2\underbrace{(k + k')}_{\in\mathbb{Z}} + 1 = 2r + 1,$$

o que mostra que a soma de um inteiro par com um inteiro ímpar resulta em um inteiro ímpar.

■

Proposição 2.3.3. *A soma de dois inteiros ímpares resulta em um inteiro par.*

Demonstração . *De fato, sejam a e b dois inteiros ímpares. Logo, podemos escrever $a = 2k + 1$ e $b = 2k' + 1$, com k, $k' \in \mathbb{Z}$. Daí, temos que,*

$$a + b = 2k + 1 + 2k' + 1 = 2\underbrace{(k + k' + 1)}_{\in\mathbb{Z}} = 2r',$$

o que mostra que a soma de dois inteiros ímpares resulta em um número par.

■

Resumidamente, temos

- par + par = par
- par + ímpar = ímpar
- ímpar + ímpar = par

Podemos agora generalizar e afirmar que:

Proposição 2.3.4. *A soma de vários inteiros pares também será um inteiro par.*

Proposição 2.3.5. *Se somarmos uma quantidade par de inteiros ímpares, tal soma resultará em um inteiro par.*

Proposição 2.3.6. *Se somarmos uma quantidade ímpar de inteiros ímpares, o resultado será um inteiro ímpar.*

Proposição 2.3.7. *Se somarmos uma "mistura" de inteiros pares e ímpares , o resultado dessa soma será um inteiro que tem a mesma paridade que a quantidade de parcelas ímpares que foram somadas.*

As demonstrações das três primeiras proposições são bastante simples, portanto fica a cargo do leitor. Para realizá-las são usadas as mesmas ideias dos casos anteriores. A proposição **2.3.7** iremos demonstrar a seguir.

Demonstração . *Com efeito, pela **proposição 2.3.4**, ao somarmos vários inteiros pares, o resultado será um inteiro par. Se nessa "mistura" há uma quantidade par de números ímpares, teremos então um resultado cujo inteiro é par, conforme **proposição 2.3.5**. Daí,*

teremos então a soma de dois inteiros pares, cujo resultado também será um inteiro par que é a paridade da quantidade de inteiros ímpares. Por outro lado, se a quantidade de inteiros ímpares nessa "mistura" for ímpar, conforme a ***proposição 2.3.6*** *o resultado da soma desses inteiros será um inteiro ímpar. Nesse caso, teremos a soma de um inteiro par com um inteiro ímpar, cujo resultado é um inteiro ímpar, que é paridade da quantidade de inteiros ímpares.*

■

Paridade do produto de dois inteiros - Analisaremos o que acontece com o produto de dois inteiros quaisquer:

Proposição 2.3.8. *O produto de dois inteiros pares resulta em um inteiro par.*

Demonstração . *Com efeito, sejam a e b dois inteiros pares. Logo, podemos escrever $a = 2k$ e $b = 2k'$, com k, $k' \in \mathbb{Z}$. Daí, temos que,*

$$ab = 2\underbrace{(2k \cdot k')}_{\in\mathbb{Z}} = 2r,$$

o que mostra que produto de dois inteiros pares também é par.

■

Proposição 2.3.9. *O produto de um inteiro par por um inteiro ímpar resulta em um inteiro par.*

Demonstração . *De fato, sejam a e b inteiros par e ímpar, respectivamente. Podemos escrever então $a = 2k$ e $b = 2k + 1$. Portanto, temos*

$$ab = 2k(2k' + 1) = 2\underbrace{(2kk' + k)}_{\in\mathbb{Z}} = 2s,$$

o que mostra que produto de um inteiro par com um inteiro ímpar resulta em um inteiro par.

■

Proposição 2.3.10. *O produto de dois inteiros ímpares resulta em um inteiro ímpar.*

Demonstração . *Com efeito, sejam a e b dois inteiros ímpares. Logo, podemos escrever $a = 2k + 1$ e $b = 2k' + 1$, com k, $k' \in \mathbb{Z}$. Daí, temos que,*

$$ab = (2k+1)(2k'+1) = 2\underbrace{(2kk'+k+k')}_{\in\mathbb{Z}}+1 = 2r'+1,$$

o que mostra que a produto de dois inteiros ímpares resulta em um número ímpar.

■

Resumidamente, temos

1. par · par = par
2. par · ímpar = par
3. ímpar · ímpar = ímpar

Podemos agora generalizar e afirmar que:

Proposição 2.3.11. *O produto de vários inteiros pares também será um inteiro par.*

Proposição 2.3.12. *Se multiplicarmos uma quantidade qualquer de inteiros ímpares, tal produto resultará em um inteiro ímpar.*

Proposição 2.3.13. *Se multiplicarmos uma "mistura" de inteiros pares e ímpares , o resultado desse produto será um inteiro par.*

As demonstrações dessas proposições ficam a cargo do leitor pois são bastante simples e para realizá-las basta usar ideias análogas às anteriores.

Para finalizar, vamos resolver o problema proposto no início da seção. O problema era o seguinte:

- Em um quartel existem 100 soldados e, todas as noites, três deles são escolhidos para trabalhar de sentinela. É possível que após certo tempo um dos soldados tenha trabalhado com cada um dos outros exatamente uma vez?

A resposta é não. Para justificar essa resposta, vamos fixar um desses soldados: o soldado X. Para cada noite em que vai trabalhar, o soldado X deverá ter a companhia de mais dois soldados. Portanto, será necessário agruparmos de dois em dois os demais 99 soldados. Mas, como 99 é um número ímpar, é fácil concluir que não é possível formarmos pares de soldados distintos para trabalharem com o soldado X.

Exercícios

Questão 24. *Escrevemos abaixo os números naturais de 1 a 10.*

1 2 3 4 5 6 7 8 9 10

Antes de cada um deles, coloque sinais "+" (positivo) ou "−" (negativo) de forma que a soma de todos seja zero.

Questão 25. *Escrevemos abaixo os números naturais de 1 a 11.*

1 2 3 4 5 6 7 8 9 10 11

Antes de cada um deles, coloque sinais "+" (positivo) ou "−" (negativo) de forma que a soma de todos seja zero.

Questão 26. *Pedro comprou um caderno com* 96 *folhas, com páginas numeradas de* 1 *a* 192*, em ordem crescente. Vitor arrancou aleatoriamente* 25 *folhas do caderno e somou todos os* 50 *números escritos nestas folhas. É possível que essa soma seja* 1990*?*

Questão 27. *É possível escrever o número 45 como soma de 10 parcelas, de modo que cada parcela seja 1 ou 3 ou 5?*

Questão 28. *(UFJF-2009-VESTIBULAR) De quantas maneiras podemos escolher 3 números naturais distintos dentre os inteiros de 1 a 20, de modo que a soma dos números escolhidos seja ímpar?*

a) 100

b) 360

c) 570

d) 720

e) 1140

Questão 29. *É possível trocar uma nota de* 25 *rublos em* 10 *notas com valores* 1, 3 *ou* 5*?*

Questão 30. *Se n é um número inteiro qualquer, qual dos números abaixo é ímpar?*

a) $n^2 - n + 2$

b) $n^2 + n + 2$

c) $n^2 + n + 1$

d) $n^2 + 5$

e) $n^3 + 5$

Questão 31. *Mostre que se a e b são inteiros ímpares, então $a^2 - b^2$ é divisível por 8.*

Questão 32. *Um fazendeiro deseja abater 30 porcos em 5 dias de modo que em cada dia sejam abatidos somente um número ímpar de porcos. Caso isso seja possível, determine como. Caso seja impossível, explique o motivo.*

Questão 33. *Todas as alternativas sobre números inteiros dadas abaixo estão corretas, exceto:*

a) Todo número par pode ser escrito como $2n$, onde n é um número inteiro.

b) Todo número ímpar pode ser escrito como $2n + 7$, onde n é um número inteiro.

c) A soma de dois números inteiros ímpares é sempre um número inteiro par.

d) Todo número inteiro ou é par ou é ímpar.

e) Todo número inteiro par pode ser escrito como $n^2 + 2$.

Relatório

Tivemos na aula de Paridade de Inteiros uma celeridade maior na explanação dos conteúdos pois os alunos começaram a desenvolver uma maturidade maior na linguagem matemática trabalhada na Teoria dos Números. Trabalhamos a definição de paridade, mostramos a peculiaridade de todo número inteiro ser par ou ser ímpar, não havendo outra possibilidade. Mostramos tambéms as implicações no que tange à soma, e multiplicação de inteiros. As propriedades trabalhadas foram assimiladas de uma maneira muito satisfatória, de forma que conseguimos fazer bastante exercícios.

Foi muito interessante perceber o quanto os alunos conseguiram desenvolver bem as idéias presentes no estudo da paridade de inteiros e suas aplicações na resolução dos exercícios. Mais uma vez, voltamos a resolver algumas questões propostas no Teste 1 e questões do material didático, sendo inclusive algumas das olimpíadas de matemática. Por conta da limitação do tempo, não conseguimos trabalhar o conceito de sistema binário e consequentemente não conseguimos aplicar o desafio proposto no plano de aula, chamado de "Mágica do Números". No entanto, percebemos que tal situação não comprometeu a assimilação por parte dos alunos do conteúdo Paridade de Inteiros.

2.4 Números Primos

Plano de Aula

Tema: Números Primos

Objetivos:
Levar o(a) aluno(a) a:

- Estudar a importância dos números primos na Teoria dos Números;
- Identificar um número primo;
- Identificar um número composto;
- Encontrar o número de divisores inteiros de um número natural;
- Construir e aplicar o Crivo de Eratóstenes.

Conteúdos:
Números Primos e Compostos

Metodologia:
Iniciaremos a aula com a exibição do documentário "A História dos Números" até o minuto 10 e, em seguida, falaremos da definição de um número primo. Posteriormente, falaremos do "Crivo de Eratóstenes", um método bastante útil para encontrar números primos. Por fim, resolveremos alguns exercícios.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, notebook, data-show e apostila.

Referências:

- Boyer, Carl B.**História da Matemática**. 3ª ed. Rio de Janeiro: SBM, 2011.
- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Moreira, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª.**. 1ª ed. Rio de Janeiro: SBM, 2003.

Texto didático

> "Na verdade, os números primos, que desempenham um papel importante em vários ramos na Matemática, são como o hidrogênio e o oxigênio do mundo dos números, eles são os átomos da Matemática".
>
> Marcus du Saltoy

Agora, vamos estudar um tema que há bastante tempo tem sido objeto de estudo de vários matemáticos. Estudaremos sobre os números primos.

Definição 2.4.1. *Um número inteiro $p > 1$ é dito primo se possui apenas dois divisores positivos:* 1 *e* p*. São exemplos de números primos, os números* 5*,* 17*,* 19*,* 71*, etc. Quando um número inteiro positivo não é primo, ele é chamado de número composto.*

Os números primos têm encantado muitos matemáticos ao redor do mundo. Esse encanto não é de hoje. Vários matemáticos, ao longo dos séculos, tais como Fibonacci (1170-1250), Leonard Euler (1707-1783) e Pierre de Fermat (1601-1665), dentre outros, debruçaram-se em compreender a dinâmica dos números primos, e criar modelos matemáticos que pudessem proporcionar a descoberta de algum novo número primo ou simplesmente verificar se algum inteiro dado era ou não primo.

A aplicabilidade dos números primos no nosso cotidiano é vasta. Por exemplo, podemos citar o método de criptografia (conjunto de regras que visa codificar informações) RSA que é um sistema criado pelos matemáticos Ron Rivest, Adi Shamir e Leonard Adleman na década de 70, que permite, por exemplo, a segurança no uso de cartões de crédito e no envio mensagens de emails, criando números primos de até 100 dígitos. Hoje

em dia, já são usados números primos com 600 dígitos, objetivando uma maior segurança. Falaremos melhor sobre a criptografia RSA mais adiante.

Abaixo, veremos um importante teorema que tem importância crucial na teoria dos números.

Teorema 2.4.1 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou pode ser escrito de forma única, como produto de números primos.*

Os exemplos a seguir servem para ilustrar esse resultado.

a) $18 = 3 \cdot 3 \cdot 2 = 3^2 \cdot 2$

b) $40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$

c) $800 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 2^4 \cdot 3 \cdot 5^2 \cdot 7$

Demonstração . *Seja n um número inteiro tal que $n > 1$. Mais ainda, seja p_1 o menor entre os divisores de n diferentes de 1. Temos assim que p_1 é primo ou composto. Suponhamos que p_1 seja composto. Daí, vai existir um inteiro d, $1 < d < p_1$, de forma que $d \mid p_1$. Ora, como $d \mid p_1$ e $p_1 \mid n$, concluímos, pela propriedade 1, estudada na seção de divisibilidade, que $d \mid n$. No entanto, essa conclusão vai contradizer a escolha de p_1. Logo, p_1 é primo. Mas, como $p_1 \mid n$, existe $m_1 \in \mathbb{N}$, tal que $n = p_1 \cdot m_1$. Daí,*

- *Se $m_1 = 1$, temos $n = p_1$, portanto, n é primo.*
- *Se $m_1 > 1$, então podemos fazer o mesmo procedimento que fizemos para o valor de n, ou seja, teremos $m_1 = p_2 \cdot m_2$, com p_2 primo e, consequentemente, podemos escrever $n = p_1 \cdot p_2 \cdot m_2$, com $1 \leq m_2 < m_1$ e p_1, p_2 primos.*
- *Se tivermos $m_2 = 1$, teremos $n = p_1 \cdot p_2$ e assim terminaríamos a prova.*
- *Se $m_2 > 1$, de maneira análoga, podemos decompor m_2 assim como fizemos com m_1.*

Dando continuidade a esse procedimento, vamos obter números primos $p_1, p_2, p_3, ..., p_i$ e uma seqência de números naturais $m_1 > m_2 > m_3 > ... > m_i \geq 1$, de forma que sempre que $m_i > 1$, podemos continuar a decomposição de n. Ora, como entre 1 e n existe uma quantidade finita de números naturais, haverá, na decomposição de n, um último passo, onde no qual teremos $m_j = 1$ e portanto teremos

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_j, \text{ com } p_1, p_2, p_3, ..., p_j \text{ primos.}$$

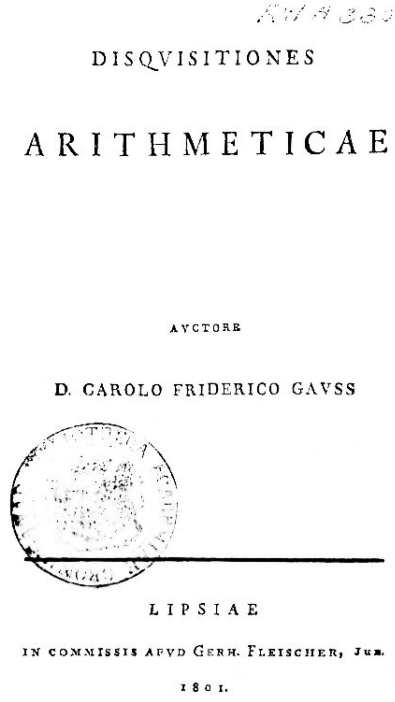
■

Esse teorema já aparece publicado no famoso livro *Elementos* do matemático Euclides. No entanto, a primeira demonstração completa e correta foi realizada e publicada, em 1081, pelo matemático Carl Friedrich Gauss no livro *Disquisitiones Arithmeticae*.

Figura 7 – Carl Friedrich Gauss (1777-1855)

Fonte: google

Figura 8 – Disquisitiones Arithmeticae



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

Fonte: google

Vejamos agora a proposição seguinte.

Proposição 2.4.1. *Seja n um inteiro positivo tal que $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Se $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$ é um divisor de n, então $0 \leq \beta_i \leq \alpha_i$, com $i = 1, 2, \ldots, r$.*

Demonstração . *De fato, como $d \mid n$, existe algum p^{β}, da decomposição em fatores primos de d, que divide algum $p_i^{\alpha_i}$ pois p^{β} e os demais $p_j^{\alpha_j}$ são primos entre si. Sendo assim, $p = p_i$ e, consequentemente, $\beta \leq \alpha_i$.*

■

A partir do Teorema Fundamental da Aritmética e da **Proposição 2.4.1** vista, podemos enunciar a seguinte propriedade.

Propriedade (1)**.** *Seja n um número natural maior que 1. Sendo $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde $p_1, p_2, \cdots, p_k$ são números primos distintos e $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$ e representando por $d(n)$ o número de divisores positivos de n, então*

$$d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Demonstração . *De fato, todos os divisores de n serão da forma $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, com $r_1 \in \{0, 1, ..., \alpha_1\}$, que é um conjunto que possui obviamente $\alpha_1 + 1$ elementos. Por outro lado, temos que $r_2 \in \{0, 1, ..., \alpha_2\}$, que por sua vez, possui $\alpha_2 + 1$ elementos e assim por diante. Portanto, é fácil ver, pelo Princípio Multiplicativo, que o número de divisores positivos, $d(n)$, do natural n será dado pela expressão vista anteriormente.*

■

Por exemplo, vamos encontrar o número de divisores positivos do número 80. Temos que $80 = 2^4 \cdot 5$. Daí, $d(80) = (4 + 1) \cdot (1 + 1) = 5 \cdot 2 = 10$. Portanto, 80 possui 10 divisores positivos.

Uma questão que surge naturalmente é: quantos são os números primos? Veremos a seguir que o conjunto dos números primos é infinito e essa propriedade é uma das singularidades dos números primos. Pelo fato de ser um conjunto infinito, é possível encontrarmos números primos muito grandes. Mas aí, surgem alguns problemas interessantíssimos: como encontrá-los? como eles são distribuídos?. Esses problemas estão até hoje em aberto e vários matemáticos já tentaram solucioná-los. A seguir, provaremos a infinidade dos números primos.

Teorema 2.4.2. *O conjunto dos números primos é infinito.*

Demonstração . *Suponha que existem apenas n números primos, digamos $p_1 < p_2 < \cdots < p_n$. Seja $m \in \mathbb{N}$ tal que $m = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$. Como $m > 1$, pelo Teorema*

Fundamental da Aritmética, existe pelo menos algum números primo p, tal que $p|m$. No entanto, como $p_1, p_2, p_3, p_4, ..., p_n$ são, por hipótese, os únicos números primos, concluímos que $p|p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_n$. Daí, pela propriedade 4 vista na seção de divisibilidade, temos que $p|1$, o que é absurdo, pois o único inteiro positivo divisor de 1 é ele mesmo. Portanto, qualquer que seja o número primo p_n, vai existir sempre um outro número primo p_k tal que $p_k > p_n$, donde concluímos que a quantidade de números primos é infinita.

■

Dando prosseguimento, veremos uma proposição que servirá para estudarmos um importante procedimento, conhecido como Crivo de Eratóstenes, procedimento esse utilizado para descobrir se um número inteiro positivo é primo.

Proposição 2.4.2. *Seja n um número natural maior do que 1. Se n é um número composto, então o menor divisor, diferente de 1, de n, é menor do que ou igual a $\sqrt{n}$, isto é, se n não possui divisores positivos, diferentes de 1 e menores do que $\sqrt{n}$ então n é número primo.*

Demonstração . *Seja n um número composto e seja p o menor divisor de n, diferente de 1. Temos então que $n = pq$, com $q \geq p$. Se multiplicarmos cada membro da desigualdade por p, o resultado será*

$$n = pq \geq p^2,$$

donde segue que $\sqrt{n} \geq p$.

■

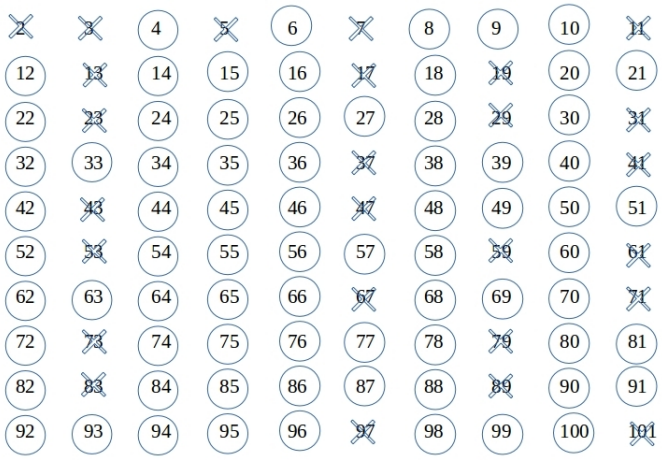
O crivo de Eratóstenes - Trata-se de um algoritmo criado pelo matemático grego Eratóstenes (285-194 a.C) cujo objetivo é encontrar, até determinado número n inteiro positivo dado, quais são os números primos menores ou iguais a ele. De acordo com esse algoritmo, inicialmente lista-se numa tabela todos os inteiros positivos ordenadamente, a partir de 2, até o n, isto é,

$$2, 3, 4, 5, 6, 7, 8, 9, ..., n$$

Após isso, marca-se com um `X` o primeiro número primo da tabela, no caso o 2 e em seguida circula-se todos os múltiplos de 2 da tabela por serem todos eles compostos. O primeiro número que não foi circulado, após o 2, foi o 3, que é próximo número primo da tabela. Daí, o procedimento segue-se , ou seja, marca-se com um `X` o número 3 e circula-se todos os múltiplos de 3 da tabela. O processo será repetido até que o primeiro número

não circulado na tabela seja maior que $\sqrt{n}$, pois devido à **proposição 2.4.1**, a partir daí, todos os números restantes são os primos menores ou iguais que n. A tabela abaixo mostra o caso de $n = 101$.

Figura 9 – Crivo de Eratóstenes

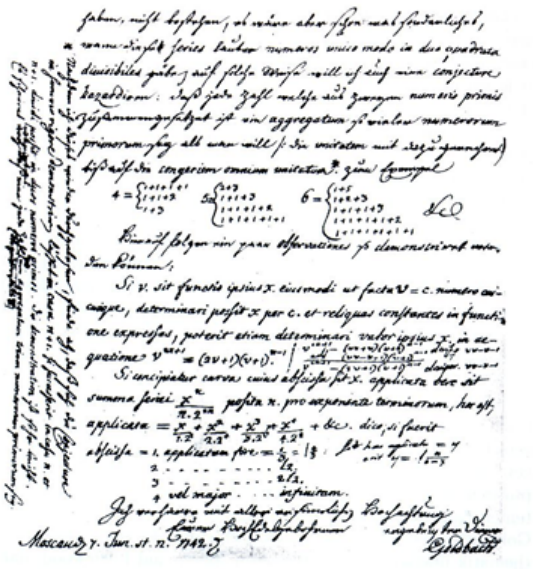


Fonte: google

Até hoje, vários questionamentos a respeito dos números primos não foram respondidos, como por exemplo, com qual frequência aparecem dentro dos conjuntos dos números inteiros. No entanto, um dos problemas mais famosos relacionados aos números primos e que ainda não foi provado, sendo portanto ainda uma conjectura, é chamado de Conjectura de Goldbach. Em 1742, o matemático Christian Goldbach enviou uma carta para o matemático Leonhard Euler. Nessa carta, Goldbach afirmava que todo número natural par, maior do que ou igual que 4, podia ser expresso como a soma de dois números primos. Vejamos alguns exemplos:

$$4 = 2 + 2,\ 22 = 19 + 3,\ 70 = 59 + 11.$$

Figura 10 – Carta de Goldbach a Euler



Fonte: google

Obviamente, o rigor matemático exige que apenas alguns exemplos não podem sustentar uma afirmação. Portanto, tal conjectura está em aberto até hoje, sendo objeto de admiração de inúmeros matemáticos até os dias atuais.
Outro importante matemático, Pierre de Fermat ($1601 - 1665$), fascinado pela beleza dos números primos, tentou criar uma fórmula através da qual pudéssemos encontrar qualquer que seja o número primo. Tal busca levou Fermat a conjecturar que são números primos todos os números F_n, da forma

$$F_n = 2^{2^n} + 1,$$

sendo n um inteiro não-negativo.

Figura 11 – Pierre de Fermat (1601-1655)

Fonte: google

Fermat conseguiu verificar a veracidade de tal conjectura para os seguintes casos:

$n = 0 \Rightarrow F_o = 2^{2^0} + 1 = 3$
$n = 1 \Rightarrow F_1 = 2^{2^1} + 1 = 5$
$n = 2 \Rightarrow F_2 = 2^{2^2} + 1 = 17$
$n = 3 \Rightarrow F_3 = 2^{2^3} + 1 = 257$
$n = 4 \Rightarrow F_4 = 2^{2^4} + 1 = 65537$

O números acima são chamados de Primos de Fermat. O problema é que a partir de $n \geq 5$, Fermat conjecturou que todos os próximos números seriam primos. Porém, Leonard Euler mostrou que para o caso $n = 5$, o número obtido é composto. De fato,

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641.6700417,$$

que é, consequentemente, um número composto. Até hoje, os únicos primos de Fermat conhecidos são os casos vistos anteriormente. Eis aí uma oportunidade de colocar o nome na história e tentar achar mais um primo de Fermat!

Exercícios

Questão 34. *Encontre todos os números primos até* 50.

Questão 35. *Mostre que o número* $n = 2^{20} - 25^4$ *é composto.*

Questão 36. *Achar os cinco menores números primos da forma* $n^2 - 2$.

Questão 37. *Ache três números primos ímpares, cuja soma seja*

a) 81

b) 125

Questão 38. *Achar todos os pares de números primos* p *e* q*, tais que* $p - q = 3$.

Questão 39. *Determinar todos os inteiros positivos* n *tais que* n, $n+2$ *e* $n+4$ *são todos primos.*

Questão 40. *Mostar que a soma de inteiros positivos ímpares e consecutivos é sempre um inteiro composto.*

Questão 41. *Demonstrar que todo número primo, exceto* 2 *e* 3 *é da forma* $6k - 1$ *ou* $6k + 1$*, onde* k *é um inteiro positivo.*

Questão 42. *Achar todos os números primos que são divisores de* 50!.

Questão 43. *Demonstrar que todo número primo ímpar é da forma* $4k + 1$ *ou* $4k - 1$*, onde* k *é um inteiro positivo.*

Questão 44. *Determine o número de divisores positivos dos números abaixo.*

a) 40

b) 120

c) 65

d) 300

Questão 45. *A soma de 3 números é 100, dois são números primos e um é a soma dos outros dois.*

- *Qual é o maior dos 3 números?*
- *Dê um exemplo desses 3 números.*
- *Quantas soluções existem para esse problema?*

Questão 46. *(EPCAR - 2004) O número* $y = 2^a \cdot 3^b \cdot c^2$ *é divisor de* $N = 15 \cdot 20 \cdot 6$. *Sabendo-se que* y *admite exatamente* 36 *divisores, é correto que*

a) $ab = c$.

b) $a + b = c$.

c) $a < b < c$.

d) $a - b = -1$.

Questão 47. *(EPCAR - 2004) Se* a *e* b *são dois números inteiros não nulos tais que* $4a + b = 2b - (3a - b)$, *então, necessariamente, ocorre que*

a) a *é par e* b *é múltiplo de* 7

b) a *é par e* b *é ímpar*

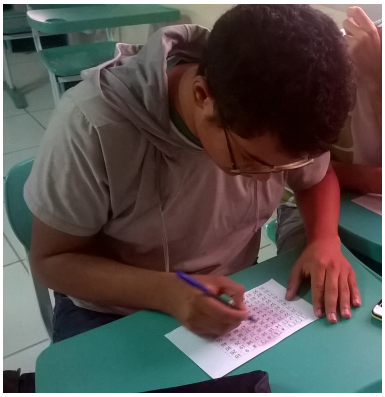
c) a *e* b *são numeros primos*

d) a *é divisor de* 2 *e* b *é divisor de* 7

Relatório

Na aula cujo tema foi "Números Primos" iniciamos com um vídeo produzido pela rede BBC que narra sobre a história dos números primos e a sua importância na matemática. Por conta do tempo, o vídeo, apesar de ter duração de mais de 1 hora, foi assistido até o minuto 10. No entanto, alguns tópicos foram abordados como a importância dos números primos na sociedade moderna atual, em especial na Criptografia (estudo de codificação de mensagens). Estudamos um teorema muito especial na Teoria dos Números que é o Teorema Fundamental da Aritmética e, como consequência, estudamos como é possível descobrir o número de divisores de um número inteiro positivo. Os alunos ficaram bastante motivados com o método do Crivo de Eratóstenes para descobrir números primos. Nesse momento da aula, cada aluno recebeu uma tabela com números de 1 até 100 para, através do Crivo de Eratóstenes, verificar quais desses eram primos. Foi um momento bastante divertido e o vencedor seria aquele que mais rapidamente entregasse a tabela com os primos corretos. Encerramos a aula falando que muitos matemáticos desejaram descobrir uma fórmula que possibilitasse a descoberta de quaisquer que fossem os números primos. Um deles que foi tratado na aula foi Fermat, que conjecturou uma fórmula, mas que anos depois foi desfeita por outro grande matemático, Leonhard Euler. Tratamos ainda da Conjectura de Goldbach. Foi bastante proveitoso observar o quanto essas informações deixaram os alunos bastante entusiasmados e curiosos a respeito desses temas que, aos poucos iam sendo revelados a eles. Muitos dos alunos questionaram o porquê esses temas não serem tratados no ensino médio, fazendo parte da grade curricular.

Figura 12 – Aluno utilizando o Crivo de Eratóstenes



Fonte: Foto tirada pelo autor

2.5 Máximo Divisor Comum - MDC

Plano de Aula

Tema: Máximo Divisor Comum - MDC

Objetivos:
Levar o(a) aluno(a) a:

- Compreender o conceito do MDC;
- Resolver problemas que envolvam o conceito de MDC;
- Compreender e aplicar as propriedades do MDC.

Conteúdos:
MDC e suas propriedades; Divisibilidade; Teorema de Bezout.

Metodologia:
Retomaremos, no início da aula, o conceito de divisibilidade e o conjunto dos divisores de um número para em seguida falarmos do conceito do MDC. Resolveremos alguns exercícios desafiantes e terminaremos a aula com a aplicação do "Jogo Baralho do MDC".

Avaliação:
Cada discente será avaliado através da participação nas discussões e nos jogos.

Recursos Didáticos:
Quadro branco, pincel, notebook, data-show e apostila.

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Fonseca, Rubens.**Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Maurício, Eufélix Monteiro.**Uma propsta de Sequência Didática para o Ensino de MDC e MMC na Educação Básica**. 2014.46f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Espírito Santo, Vitória.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.

Texto didático

Dando continuidade ao curso, falaremos de um conceito importantíssimo que servirá de base para o estudo, por exemplo, das chamadas equações diofantinas, que também será um tema trabalhado nessas notas. Esse conceito é chamado de MDC (máximo divisor comum).

Considere, por exemplo, todos os divisores positivos dos números 36 e 42:

$$D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\} \text{ e } D(42) = \{1, 2, 3, 6, 7, 14, 21, 42\}$$

Note que o maior número que é divisor de 36 e 42, ao mesmo tempo, é 6. Dizemos que 6 é o máximo divisor comum de 36 e 42 e escrevemos $(32, 42) = 6$.

Definição 2.5.1. *Sejam $a, b \in \mathbb{Z}$ com pelo menos um deles diferente de zero. O máximo divisor comum de a e b (MDC) é um inteiro positivo d tal que d é o maior dentre os divisores positivos comuns de a e b. Escrevemos $(a, b) = d$. Se $(a, b) = 1$, dizemos que a e b são primos entre si.*

É fácil ver que sendo $a \in \mathbb{Z}$, temos que $(a, 0) = |a|$,$(a, 1) = 1$ e que $(a, a) = |a|$. As proposições a seguir são de grande importância na teoria dos números, em especial para o cálculo do MDC de números inteiros.

Proposição 2.5.1. *Sejam a e b dois inteiros, com pelo menos um deles diferente de zero. As seguintes afirmações são válidas:*

(i) Se a é múltiplo de b, então $(a, b) = |b|, b \neq 0$.

(ii) Se $a = bq + c$, então o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e c e temos, em particular, que $(a, b) = (b, c)$.

Por exemplo, sejam $a = 15$ e $b = 5$. De (i), temos que $(15, 5) = 5$. Mais ainda, sendo agora $a = 28$ e $b = 8$, temos $28 = 3 \cdot 8 + 4$. Logo, por (ii), concluímos que $(28, 8) = (8, 4) = 4$.

Vejamos agora as demonstrações dessas afirmações.

Demonstração . *Inicialmente, demonstraremos (i). De fato, se um inteiro pertence ao conjunto dos divisores de b, como $b \mid a$, então, também pertence ao conjunto dos divisores de a. Daí, o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores de b. No entanto, como o maior inteiro que divide b é o $|b|$, concluímos que $(a, b) = |b|$.*

Para provarmos (ii), utilizaremos a propriedade 4 estudada na seção sobre divisibilidade. Baseados nela, temos que todo divisor comum de a e b também é divisor de c e, portanto, divisor de b e c. Por outro lado, todo divisor comum de b e c também é divisor de a e, assim, também é um divisor de a. Logo, os divisores comuns dos inteiros a e b também são os mesmos que os divisores comuns dos inteiros b e c o que resulta que $(a, b) = (b, c)$.

■

A proposição acima demonstrada será proveitosa para estudarmos um importante teorema dentro da teoria dos números, conhecido como Algoritmo de Euclides.

Teorema 2.5.1 (**Algoritmo de Euclides**)**.** *Dados dois inteiros positivos a e b, considere as divisões sucessivas*

$$\begin{array}{rcccl} a &=& bq &+ r_0, & 0<r_0<b \\ b &=& r_0q_1 &+ r_1, & 0<r_1<r_0 \\ r_0 &=& r_1q_2 &+ r_2, & 0<r_2<r_1 \\ r_1 &=& r_2q_3 &+ r_3, & 0<r_3<r_2 \\ \vdots & \vdots & \vdots & \vdots \quad \vdots & \vdots \\ r_k &=& r_{k+1}q_{k+2} &+ r_{k+2}, & 0<r_{k+2}<r_{k+1} \\ r_{k+1} &=& r_{k+2}q_{k+3} & & \end{array}$$

até algum r_{k+2} dividir r_{k+1}. Assim, temos que $(a, b) = r_{k+2}$, que é o último resto não-nulo das divisões sucessivas anteriores.

Demonstração . *É fácil ver que processo de divisões sucessivas descritos acima é finito. De fato, pelo algoritmo da divisão, temos que $b > r_0 > r_1 > r_2 > ... \geq 0$. Como a quantidade de números entre b e 0 é finita, então o processo é finito. Mais ainda, analisando as*

igualdades de cima para baixo, como também utilizando a ***proposição 2.5.1****, concluímos que*

$$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{k+1}, r_{k+2}) = r_{k+2}$$

■

Por exemplo, vamos calcular $(1320, 35)$. Baseados no Algoritmo de Euclides, tal cálculo será realizado da seguinte forma:

Figura 13 – Divisões sucessivas

1320 | 35	35 | 25	25 | 10	10 | 5
25 37	10 1	5 2	0 2

Fonte: Produzido pelo autor

Ou seja,

$$\begin{aligned} 1320 &= 35 \cdot 37 + 25 \\ 35 &= 25 \cdot 1 + 10 \\ 25 &= 10 \cdot 2 + 5 \\ 10 &= 5 \cdot 2 + 0 \end{aligned}$$

A partir dos resultados acima, temos que $(1320, 35) = (35, 25) = (25, 10) = (10, 5) = (5, 0) = 5$. Daí, $(1320, 35) = 5$. Esse método é chamado de divisões sucessivas.

Uma forma de representarmos as divisões sucessivas, é usando uma grade conforme ilustrada abaixo para o cálculo de $(1320, 35)$.

Figura 14 – Grade de divisões sucessivas

	37	1	2	2
1320	35	25	10	5
25	10	5	0	

Fonte: Produzido pelo autor

Utilizando esse mecanismo, $(1320, 35)$ será o último resto não nulo, no caso, igual a 5. Através desse método, o cálculo do MDC de números inteiros fica bastante simples.

Vejamos outro exemplo. Vamos calcular $(60, 42)$. Utilizando o método descrito acima, temos

Figura 15 – Grade de divisões sucessivas

	1	2	3
60	42	18	6
18	6	0	

Fonte: Produzido pelo autor

Portanto, $(60, 42) = 6$. Note que a partir desses dados, podemos escrever

$$18 = 60 - 42 \cdot 1 \tag{2.1}$$
$$6 = 42 - 18 \cdot 2 \tag{2.2}$$

Substituindo (2.1) em $(2, 2)$, teremos

$$\begin{aligned} 6 &= 42 - (60 - 42 \cdot 1) \cdot 2 \\ 6 &= 42 - 60 \cdot 2 + 42 \cdot 2 \\ 6 &= 42 \cdot 3 - 60 \cdot 2 \\ 6 &= 60 \cdot (-2) + 42 \cdot 3. \end{aligned}$$

Vemos então que encontramos dois inteiros, a saber -2 e 3, de forma que podemos escrever $(60, 42) = 60 \cdot (-2) + 42 \cdot 3$. Mas, será que é sempre possível isso? O teorema a seguir irá responder a esse questionamento. Mais ainda, veremos na seção que trata das chamadas equações diofantinas que existem infinitos inteiros x e y de forma que $6 = (60, 42) = 60x + 42y$.

Teorema 2.5.2 (**Teorema de Bachet-Bézout**). *Considere dois inteiros não simultaneamente nulos, a e b e seja $d = (a, b)$. Então, existem inteiros x e y de forma que*

$$d = ax + by.$$

Demonstração . *Com efeito, considere o conjunto $C = \{ax + by, com\, x, y \in \mathbb{Z}\}$ e $n = ax_0 + by_0$ o menor elemento positivo de C. Suponhamos, por absurdo, que $n \nmid a$. Pelo algoritmo da divisão, temos que $a = nq + r$, com $0 < r < n$. Daí, $r = a - nq$. Substituindo o valor de n nessa última equação, teremos $r = a - (ax_0 + by_0)q = a - ax_0q - by_0q = a(1 - x_0q) + b(-y_0q)$, ou seja, $r \in C$. Mas, como $0 < r < n$, esse fato contraria a hipótese de n ser o menor elemento positivo de C. Portanto, $n \mid a$. De forma análoga, podemos provar que $n \mid b$. Sendo assim, n é divisor comum de a e b. Agora, resta-nos mostrar que $n = d$. De fato, como $d \mid a$ e $d \mid b$, podemos escrever $a = dq_1$ e $b = dq_2$. Como $n = ax_0 + by_0$, temos então, $n = (dq_1)x_0 + (dq_2)y_0$, mais ainda, $n = d(q_1x_0 + q_2y_0)$, donde concluímos que $d \mid n$, ou seja, pela propriedade 7 estudada na seção de divisibilidade, temos $n \geq d$ e segue que $d = n$ é o maior divisor comum de a e b.*

■

Uma consequência importante desse Teorema é a propriedade abaixo.

Propriedade (1). *Dados a, b inteiros com pelo menos um deles diferente de zero, se existirem inteiros r, s tais que $1 = ra + sb$, então $(a, b) = 1$.*

Demonstração . *De fato, sendo $d = (a, b)$, temos que $d \mid ra$ e $d \mid sb$, portanto $d \mid ra + sb$. Daí, temos que $d \mid 1$. Logo, $d = 1$.*

■

Antes de estudarmos a próxima propriedade, vejamos a seguinte definição:

Definição 2.5.2. *Um número inteiro positivo d será chamado de MDC dos números inteiros $a_1, a_2, ..., a_n$, com pelo menos um diferente de zero, se tiver as seguintes propriedades:*

i d é um divisor comum da lista de inteiros $a_1, a_2, ..., a_n$;

ii Se c é um divisor comum de $a_1, a_2, ..., a_n$, então $c \mid d$.

Propriedade (2). *Dados a, b e c inteiros não nulos, então $(a, b, c) = \big((a, b), c\big)$.*

Demonstração . *Com efeito, sejam $(a, b) = d$, $(a, b, c) = d_1$, $\big((a, b), c\big) = d_2$. Daí, temos que $d_2 \mid c$ e $d_2 \mid d$. Mas, como $d \mid a$ e $d \mid b$, concluímos que d_2 divide a, b e c. Portanto, $d_2 \leq d_1$. No entanto, como d_1 divide a, b e c, temos que, em particular, $d_1 \mid a$ e $d_1 \mid b$, logo $d_1 \mid d$. Daí, segue que d_1 divide d e c. Ora, pelo Teorema de Bézout, existem x_0 e y_0, tais que*

$$(a, b)x_0 + cy_0 = d_2 \Rightarrow dx_0 + cy_0 = d_2$$

mas como d_1 divide d e c, segue, pela propriedade 4 estudada na seção de divisibilidade, que $d_1 \mid d_2$ e, portanto, $d_1 \leq d_2$. Enfim, $d_1 = d_2$, como queríamos mostrar.

■

Como exemplo, vamos calcular o seguinte problema.

- Pedrinho possui 24 bolas de gude azuis, 18 amarelas e 12 verdes. Ele deseja organizá-las em grupos de mesma quantidade de bolas, independemente da cor, de forma que cada grupo possua o maior número de bolas de gude possível. Quantas bolas de gude terá cada grupo?

Para resolvermos o problema acima proposto, é necessário calcularmos $(24, 18, 12)$. Inicialmente, calculemos $(24, 18)$.

Figura 16 – Grade de divisões sucessivas

	1	3
24	18	6
6	0	

Fonte: Produzido pelo autor

Pela grade de divisões sucessivas da Figura 16, temos que $(24, 18) = 6$.

Por outro lado, pela grade de divisões sucessivas da Figura 17, temos $(12, 6) = 6$.

Figura 17 – Grade de divisões sucessivas

	2
12	6
0	

Fonte: Produzido pelo autor

Portanto, $(24, 18, 12) = 6$. Sendo assim, cada grupo terá 6 bolas.

Uma outra forma de calcularmos o MDC entre dois inteiros com pelo menos um diferente de zero, é pela decomposição em fatores primos.

Para isso, vejamos antes a seguinte propriedade.

Propriedade (3). *Sejam os inteiros positivos* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_n}$ *e* $b = p_1^{\beta 1} \cdot p_2^{\beta 2} \cdots p_r^{\beta_n}$. *O MDC de* a *e* b *será o produto de todas as potências* p^s, *tal que* p *pertence ao conjunto de todos os primos que dividem simultaneamente* a *e* b, *onde* s *é o menor expoente de* p.

Demonstração . *Com efeito, seja* $d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_r^{\gamma_n}$, *com* $\gamma_i = min\ \{\alpha_i, \beta_i\}$. *É claro que, pela* ***Proposição 2.4.1*** *estudada na seção de Números Primos,* d *é divisor comum de* a *e* b. *Seja* c *um divisor comum de* a *e* b, *então tem-se* $c = p_1^{\theta_1} \cdot p_2^{\theta_2} \cdots p_r^{\theta_n}$, *mais ainda,* $\theta \leq \{\alpha_i, \beta_i\}$, *ou seja,* $d \geq c$, *donde concluímos que* $(a, b) = d$.

■

Vamos, por exemplo, calcular mais uma vez $(24, 18, 12)$ utilizando esse método apresentado. Temos, então

- $24 = 2^3 \cdot 3$
- $18 = 2 \cdot 3^2$
- $6 = 2 \cdot 3$

Note que os primos 2 e 3 dividem simultanemente 24, 18 e 6. Mais ainda, o menor expoente de tanto do 2 quanto do 3, é 1. Portanto, $(24, 18, 6) = 2^1 \cdot 3^1 = 6$.

Por fim, vamos ver mais uma propriedade que será bastante útil nas seções seguintes.

Propriedade (4)**.** *Sejam a e b inteiros não nulos. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração . *De fato, pela propriedade 1, podemos escrever $ra + sb = 1$, com r, s inteiros. Multiplicando cada membro dessa igualdade por c, teremos*

$$a(rc) + s(bc) = c$$

Como $a \mid a(rc)$ e $a \mid s(bc)$, segue, pela propriedade 4, estudada na seção de divisibilidade, que $a \mid c$.

■

Exercícios

Questão 48. *Achar o máximo divisor comum dos números 471 e 1176.*

Questão 49. *Provar que a fração $\frac{2n+8}{4n+15}$ é irredutível para todo número natural n.*

Questão 50. *Sabe-se que a e b são dois números naturais não nulos tais que $(a, b) = 11$. A grade de divisões sucessivas é dada abaixo.*

Figura 18 – Grade de divisões sucessivas

	2	1	3
a	b		11
		0	

Fonte: Produzido pelo autor

Determine os valores de a e b.

Questão 51. *Dona Maria comprou* 160 *pirulitos,* 198 *caramelos e* 370 *chocolates para presentear as crianças de sua rua. Para tanto, ela colocou os doces em sacolas de modo que cada sacola contivesse um único tipo de doce, que a quantidade de doces em cada sacola fosse sempre a mesma e de modo que cada sacola contivesse a maior quantidade possível de doces. Depois de colocar os doces nas sacolas, Dona Maria percebeu que sobraram* 7 *pirulitos,* 11 *caramelos e* 13 *chocolates. Quantas sacolas Dona Maria fez?*

Questão 52. *O MDC de dois números naturais é* 10 *e o maior deles é* 120*. Determine o maior valor possível para o outro número.*

Questão 53. *Dividindo-se dois números naturais pelo seu MDC, a soma dos quocientes obtidos é igual a 8. Determine esses números, sabendo que sua soma é 384.*

Questão 54. *(U.E. Londrina - PR) Para levar os alunos de certa escola a um museu, pretende-se formar grupos que tenha iguais quantidades de alunos e de modo que em cada grupo todos sejam do mesmo sexo. Se nessa escola estudam 1350 rapazes e 1224 garotas e cada grupo deverá ser acompanhado de um único professor, qual o número mínimo de professores necessários para acompanhar todos os grupos nessa visita?*

Questão 55. *Entre algumas famílias de um bairro, foi distribuído um total de 144 cadernos, 192 lápis e 216 borrachas. Essa distribuição foi feita de modo que o maior número possível de famílias fosse contemplado e todos recebessem o mesmo número de cadernos, o mesmo número de lápis e o mesmo número de borrachas, sem haver sobra de qualquer material. Determine o número de cadernos que cada família ganhou.*

Questão 56. *O máximo divisor comum de dois números é 20. Para se chegar a esse resultado pelo processo das divisões sucessivas, os quocientes encontrados foram, pela ordem, 2,1,3 e 2. Ache os números.*

Questão 57. *Mostre que*

a) $(n, 2n+1) = 1$

b) $(n+1, 2n) = 1$ *ou* 2

c) $(2n+1, 5n+3) = 1$

Questão 58. *Uma concessionária vendeu no mês de outubro* n *carros do tipo A e* m *carros do tipo B, totalizando* 216 *carros. Sabendo-se que o número de carros vendidos de cada tipo foi maior do que* 20*, que foram vendidos menos carros do tipo A do que do tipo B, isto é,* $n < m$*, e que* $(n, m) = 18$*, determine os valores de* n *e* m *.*

Questão 59. *(OBM 2014 - F1N2) Um número natural maior do que um é primo quando tem somente dois divisores naturais: 1 e o próprio número. Assim, são primos os números*

2, 3, 5, 7, etc. Qual dos números a seguir não pode ser igual à diferença entre dois números primos?

a) 4

b) 6

c) 7

d) 8

e) 9

Relatório

Nessa aula, falamos de um dos assuntos que são cruciais na Teoria dos Números: O máximo divisor comum de dois ou mais inteiros. No início, falamos que todos os presentes já tinham, de alguma forma, familiaridade com esse assunto, mas nessa aula abordaríamos sob uma perspectiva mais avançada, mostrando alguns fatos que, provavelmente, eles nunca tinham estudado. Mostramos o conceito, fizemos alguns exemplos iniciais que facilmente foram compreendidos pelos alunos e depois generalizamos um método para resolução do MDC, que é conhecido como Algoritmo de Euclides. Em seguida, vimos o método utilizando as grades, finalizando com algo que deixou os alunos bastante interessados pela simplicidade e, ao mesmo tempo pela riqueza de aplicações, que é o Teorema de Bachet-Bezout e suas consequências. Prosseguimos a aula resolvendo alguns exercícios da ficha e de olimpíadas de matemática e finalizamos com a aplicação do "jogo Baralho do M.D.C", que está descrito mais detalhadamente no apêndice desse trabalho.

Figura 19 – Alunos jogando o jogo Baralho do MDC

Fonte: Foto tirada pelo autor

2.6 Mínimo Múltiplo Comum - MMC

Plano de Aula

Tema: Mínimo Múltiplo Comum e Aplicações

Objetivos:
Levar o(a) aluno(a) a:

- Compreender o conceito de MMC;
- Resolver problemas que envolvam a ideia de MMC;
- Compreender e aplicar as propriedades do MMC;
- Relacionar os conceitos de MMC e de MDC.

Conteúdos:
MMC, Múltiplos e Divisores de um inteiro.

Metodologia:
Iniciaremos a aula definindo o conceito de MMC e, em seguida resolveremos problemas relacionados com o assunto retirados de olimpíadas de matemática.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila.

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Maurício, Eufélix Monteiro.**Uma proposta de Sequência Didática para o Ensino de MDC e MMC na Educação Básica**. 2014.46f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Espírito Santo, Vitória.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.

Texto didático

Suponhamos que no alto de uma torre de uma emissora de televisão duas luzes piscam com frequências diferentes. A primeira pisca 15 vezes por minuto e a segunda pisca 10 vezes por minuto. Se num certo instante as luzes piscam simultaneamente, após quantos segundos elas voltarão a piscar simultaneamente?. Para resolvermos esse problema de uma maneira muito prática, estudaremos o conceito de MMC (menor múltiplo comum).

Definição 2.6.1. *Sejam a e b inteiros não nulos. Chamamos de menor múltiplo comum de a e b, e indicamos por $[a, b]$, o inteiro positivo m tal que m é o menor número que é divisível por a e b ao mesmo tempo.*

Por exemplo, considerando $M(n)$ o conjunto dos múltiplos positivos de um inteiro n, temos que

- $M(24) = \{24, 48, 72, 96, 120, 144, ...\}$ e
- $M(30) = \{30, 60, 90, 120, 150, ...\}$.

Notemos que 120 é o menor número da lista que é divisível ao mesmo tempo por 24 e 30, ou seja, é o menor número inteiro positivo que é múltiplo ao mesmo tempo de 24 e 30. Portanto, $[24, 30] = 120$.

Um método bastante prático para o cálculo do MMC de dois inteiros dados será visto a seguir, utilizando a decomposição em fatores primos, assim como foi feito para o MDC. Mas antes disso, observemos a seguinte definição:

Definição 2.6.2. *O inteiro positivo m é chamado de MMC dos inteiros positivos $b_1, b_2, ..., b_n$, se m for um múltiplo comum de $b_1, b_2, ..., b_n$ e se, para todo múltiplo comum m' de $b_1, b_2, ..., b_n$, ocorre que $m \mid m'$.*

Para utilizar esse método, considere $b_1, b_2, b_3, ..., b_n$ inteiros não nulos. Decompondo em fatores primos cada número desse, temos que $[b_2, b_3, ..., b_n]$ será o produto de todos os fatores primos, comuns e não-comuns a eles cada um elevado ao maior expoente que aparece "acompanhado" cada um dos fatores primos. É claro que se algum b_i, $i \in \{1, 2, 3, ..., n\}$ é negativo, basta decompor $|b_i|$.

Vamos, por exemplo calcular $[18, 24, 30]$. Temos

- $18 = 2 \cdot 3^2$
- $24 = 2^3 \cdot 3$
- $30 = 2 \cdot 3 \cdot 5$.

Temos então que $[18, 24, 30] = 2^3 \cdot 3^2 \cdot 5 = 360$. Note que tal procedimento também poderia ser realizado através do seguinte método, que consiste em colocar os três números um ao lado do outro, separados por vírgulas e com uma barra vertical à direita desses números e, assim, realizamos as divisões sucessivas. Abaixo de cada número colocamos o quociente da divisão de cada um deles pelo menor primo que divide pelo menos um deles. Se algum deles não for divisível por esse primo, ele é repetido na linha seguinte. O procedimento termina quando todos os quocientes forem iguais a 1. Observe:

Figura 20 – Divisões sucessivas

18, 24, 30	2
9, 12, 15	2
9, 6, 15	2
9, 3, 15	3
3, 1, 5	3
1, 1, 5	5
1, 1, 1	

Fonte: Produzido pelo autor

Portanto, $[18, 24, 30] = 2^3 \cdot 3^2 \cdot 5 = 360$.

Agora, vejamos uma situação bastante interessante. Já vimos anteriormente que $[24, 30] = 120$. Calculando $(24, 30)$, teremos

- $24 = 2^3 \cdot 3$
- $30 = 2 \cdot 3 \cdot 5$.

Pelo que vimos na seção de MDC, temos que $(24, 30) = 2 \cdot 3 = 6$. Efetuando $[24, 30] \cdot (24, 30)$, teremos

$$[24, 30] \cdot (24, 30) = 120 \cdot 6 = 24 \cdot 30$$

.

Vejamos agora outro exemplo. Temos $[6, 9] = 18$, $(6, 9) = 3$ e $[18, 9] \cdot (18, 9) = 3 \cdot 18 = 6 \cdot 9$.

Será que isso sempre será verdade? Veremos mais adiante um teorema importante que generaliza esse fato. Mas antes, estudaremos dois lemas que fundamentarão a prova desse teorema.

Lema 2.6.1. *Sejam a e b inteiros não nulos e $(a, b) = d$. Sendo $a = dm_1$ e $b = dm_2$, então $(m_1, m_2) = 1$.*

Demonstração . *Suponhamos que $(m_1, m_2) = k$, tal que $k > 1$. Sendo assim, teremos*

- $m_1 = kn_1 \Rightarrow a = dkn_1 \Rightarrow dk \mid a$ *e*
- $m_2 = kn_2 \Rightarrow b = dkn_2 \Rightarrow dk \mid b$.

Daí, concluímos que dk é um divisor comum de a e b. Como, como por hipótese $k > 1$, teremos $dk > d$, o que é absurdo pois d é o maior divisor comum de a e b. Portanto, $(m_1, m_2) = 1$.

■

Lema 2.6.2. *Sejam a e b inteiros não nulos e $[a, b] = m$. Sendo $m = ak_1$ e $m = bk_2$, então $(k_1, k_2) = 1$.*

Demonstração . *Suponhamos que $(k_1, k_2) = l$, tal que $l > 1$. Sendo assim, teremos*

- $k_1 = lr_1 \Rightarrow m = alr_1$
- $k_2 = lr_2 \Rightarrow m = blr_2$.

Das duas igualdades acima, concluímos que

$$alr_1 = blr_2 \Rightarrow ar_1 = br_2.$$

Se $m_1 = ar_1 = br_2$, temos $m_1 < m$. Como m_1 é um múltiplo comum de a e b e menor que m, chegamos a um absurdo, pois o $[a, b] = m$. Portanto, $(k_1, k_2) = 1$.

■

Agora, vejamos o seguinte teorema.

Teorema 1. *Sejam a e b inteiros não nulos. Então $(a, b) \cdot [a, b] = |ab|$.*

Demonstração . *Seja $(a, b) = d$. Então*

- $a = dh_1$ *e*
- $b = dh_2$.

Daí, pelo ***Lema 2.6.1****, temos que $(h_1, h_2) = 1$. Sejam também $[a, b] = m$. Temos que*

- $m = a\alpha_1$ *e*
- $m = b\alpha_2$.

Sendo assim, pelo ***Lema 2.6.2****, temos $(\alpha_1, \alpha_2) = 1$. Podemos escrever, então*

- $m = a\alpha_1 = dh_1\alpha_1$
- $m = b\alpha_2 = dh_2\alpha_2$.

Daí, temos que $dh_1\alpha_1 = dh_2\alpha_2 \Rightarrow h_1\alpha_1 = h_2\alpha_2$. Portanto, $h_1 \mid h_2\alpha_2$. Mas, como $(h_1, h_2) = 1$, só nos resta concluir que $h_1 \mid \alpha_2$. Analogamente, temos $h_2 \mid h_1 \cdot \alpha_1$. No entanto, como já foi visto antes, $(h_1, h_2) = 1$, concluímos que $h_2 \mid \alpha_1$. Utilizando a mesma argumentação, chegaremos a conclusão que $\alpha_2 \mid h_1$ e que $\alpha_1 \mid h_2$ e, consequentemnte

- $h_1 = \alpha_2$ *e que*
- $h_2 = \alpha_1$.

Por fim, teremos

$$ab = dh_1dh_2 = d^2\alpha_1\alpha_2 = d^2\frac{m}{a} \cdot \frac{m}{b} = \frac{d^2m^2}{ab} \Rightarrow a^2b^2 = d^2m^2$$

.

Donde segue que $|ab| = dm$, como queríamos demonstrar.

■

Observação: uma importante consequência desse fato é que sendo a e b inteiros não nulos e primos entre si, ou seja, $(a, b) = 1$, temos

$$(a, b) \cdot [a, b] = ab \Rightarrow [a, b] = ab$$

.

Para finalizarmos, vamos resolver o problema proposto no início da seção. O problema era o seguinte:

- Suponhamos que no alto de uma torre de uma emissora de televisão duas luzes piscam com frequências diferentes. A primeira pisca 15 vezes por minuto e a segunda pisca 10 vezes por minuto. Se num certo instante as luzes piscam simultaneamente, após quantos segundos elas voltarão a piscar simultaneamente?

Solução. *Se a primeira pisca 15 vezes por minuto, é claro que ela vai piscar a cada* $60 \div 15 = 4$ *segundos. Por outro lado, a segunda irá piscar a cada* $60 \div 10 = 6$ *segundos. Se num certo instante ambas piscam simultaneamente, para encontarmos após quanto segundos vão piscar ao mesmo tempo, basta calcularmos o MMC entre 6 e 4. Pelo método que estudamos, temos*

Figura 21 – Divisões sucessivas

6, 4	2
3, 2	2
3, 1	3
1, 1	

Fonte: Produzido pelo autor

Portanto, $[6, 4] = 2^2 \cdot 3 = 24$. *Sendo assim, a resposta é 24 segundos.*

Exercícios

Questão 60. *(PROFMAT - 2011) O máximo divisor comum entre dois números naturais é 16 e o mínimo múltiplo comum desses mesmos números é 576. Podemos garantir que*

a) os dois números são maiores do que 50.

b) o produto dos dois números é maior que 8000.

c) os dois números são múltiplos de 32.

d) os dois números são divisores de 96.

e) um dos números é múltiplo do outro.

Questão 61. *O MMC de dois números a e b vale 60 e o MDC de ambos vale x. Determine todos os pares de números que satisfazem a condição:*

$$\frac{a}{x} + \frac{b}{x} = 7$$

Questão 62. *(COLÉGIO NAVAL) Qual a diferença de dois números naturais, que têm para produto 2304, e para máximo divsor comum o número 12?*

a) 180

b) 72

c) 0

d) 192

e) 168

Questão 63. *(COVEST MAT 2 /06) Os naturais $2^6 \cdot 3^m \cdot 5^4$ e $2^p \cdot 3^7 \cdot 5^n$ têm máximo divisor comum $2^6 \cdot 3^6 \cdot 5^4$ e mínimo múltiplo comum $2^8 \cdot 3^7 \cdot 5^n$. Calcule os naturais m, n e p e indique sua soma.*

Questão 64. *Um doente precisa tomar os remédios A, B e C a cada 3, 4 e 5 horas, respectivamente. Ele tomou o remédio A ás 2h da manhã, o remédio B às 3h da manhã e o remédio C às 4h da manhã. Sabendo que ele vai tomar os remédios por 30 dias, quantas vezes ele tomará os três remédios simultaneamente?*

Questão 65. *O MDC de dois números é igual a 3 e o MMC desses mesmos números é igual a 42. Determine os possíveis valores desses números.*

Questão 66. *Se os ovos em uma cesta são separados em grupos de 2, 3, 4, 5 e 6, sobram 1, 2, 3, 4 e 5 ovos, respectivamente. Se esses ovos são separados em grupos de 7, não sobram ovos. Qual é o menor número possível de ovos na cesta?*

Relatório

Nessa aula, estudamos o conceito de menor múltiplo comum de dois ou mais inteiros dados e a relação fundamental que diz que o produto do MMC e MDC de dois inteiros é igual ao produto desses inteiros. Fizemos várias aplicações resolvendo questões de olimpíadas de matemática. Nesse momento do curso, os alunos não tiveram muitas dificuldades de compreender os temas abordados.

2.7 Equações Diofantinas

Plano de Aula

Tema: Equações Diofantinas

Objetivos:
Levar o(a) aluno(a) a:

- Estudar aplicações das equações diofantinas na resolução de situações problemas;
- Resolver eficientemente uma equação diofantina;
- Estudar a relação entre equações diofantinas e a geometria;
- Mostrar uma das aplicações do Teorema de Bezout.

Conteúdos:
Equações Diofantinas, MDC, Teorema de Bezout .

Metodologia:
Iniciaremos a aula com o "jogo da escova diofantina" para depois darmos a definição formal de uma equação diofantina. Posteriormente, resolveremos alguns exercícios sobre o assunto.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila

Referências:

- Bispo, Dinguiston dos Santos.**Equações Diofantinas Lineares e suas Aplicações**.2013.76 f. Monografia (Licenciatrua em Matemática). Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista.
- Costa, Eduardo S..**Equações Diofantinas Lineares e o Professor do Ensino Médio**. 2007. 119f. Dissertação. Mestrado Acadêmico em Educação Matemática. Pontifícia Universidade Católica de São Paulo, São Paulo.
- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Santos, Rafael Prado. **Uma Proposta de Ensino de Equações Diofantinas Lineares no Ensino Básico Utilizando a Metodologia de Resolução de Problemas**. 2014.78f. Trabalho de Conclusão de Curso Superior em Licenciaturra Plena em Matemática. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), São Paulo.

Texto didático

Suponhamos a seguinte situação: Pedro deseja comprar selos de 5 reais e de 3 reais e, para isso, quer gastar exatamente 50 reais. De quantas maneiras ele pode fazer essa compra?

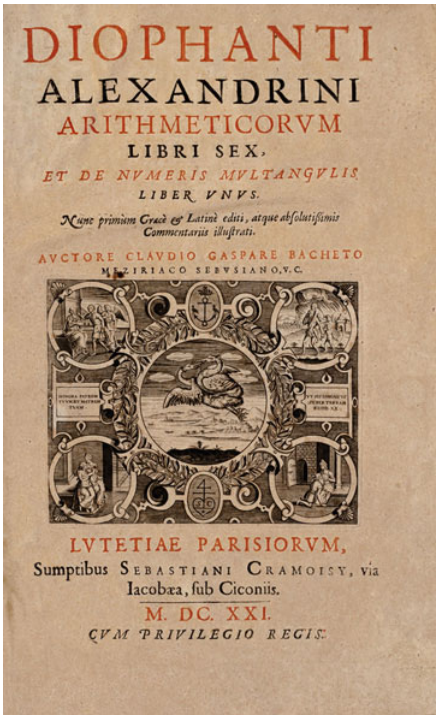
Para resolvermos o problema acima, chamemos de x e y a quantidade de selos de 5 reais e 3 reais, respectivamente. Então, chegaremos a seguinte equação:

$$5x + 3y = 50,$$

onde devemos encontrar x e y inteiros positivos.

A equação encontrada é um exemplo do que chamamos de equação diofantina e será objeto de estudo nessa seção. O nome diofantina é uma homenagem ao matemático grego Diofanto (214-299 d.C) considerado por muitos como o "pai da Álgebra". Sua obra "Arithmetica", que foi escrita por volta de 250 d.C, já traz referências a esses tipos de equações e como resolvê-las.

Figura 22 – Capa do livro Arithmetica



Fonte: google

Definição 2.7.1. *Chamamos de Equação Diofantina, toda equação da forma*

$$ax + by = c, \ \ com \ \ a, b, c \in \mathbb{Z} \ \ e \ a, b \neq 0$$

.

Na equação $5x + 3y = 50$, temos $a = 5$, $b = 3$ e $c = 50$. Vejamos mais exemplos de equações diofantinas:

- $3x + y = 100$
- $x + y = 23$
- $4x + 6y = 9$

Na equação resultante do problema proposto no início da seção, uma possível solução seria $x = 4$ e $y = 10$. Mas, será que sempre uma equação diofantina terá solução? Veremos, através da proposição a seguir que a resposta é não e, mais ainda, analisaremos quais as condições para que ela possua solução. Um outro ponto a ser destacado é que quando falamos de solução de uma equação diofantina, estamos em busca de números inteiros que satisfazem essa equação.

Proposição 2.7.1. *A equação diofantina*

$$ax + by = c, \ \ com \ \ a, b, c \in \mathbb{Z} \ \ e \ a, b \neq 0$$

possui solução se, e somente se, $(a, b) = d \mid c$. *Mais ainda, se o par* (x_0, y_0) *é uma solução dessa equação, temos que o conjunto dessa equação será formada por todos os pares de inteiros* (x, y) *da forma*

$$x = x_0 + t\frac{b}{d} \ \ e \ \ y = y_0 - t\frac{a}{d}, \ \ \ onde \ \ \ t \in \mathbb{Z}.$$

Demonstração . *Suponhamos, por hipótese, que o par* (x_0, y_0) *seja uma solução da equação. Logo, teremos* $ax_0 + by_0 = c$. *Como* $d \mid a$ *e* $d \mid b$, *temos que* $d \mid c$, *pela propriedade* 6 *estudada na seção de divisibilidade.*

Da mesma forma, se $d \mid c$, *existe* $q \in \mathbb{Z}$ *de forma que* $c = qd$. *No entanto, pelo Teorema de Bézout, existem dois inteiros* x_0 *e* y_0 *tais que* $ax_0 + by_0 = d$. *Daí, multiplicando os dois membros dessa última igualdade por* q, *teremos*

$$aqx_0 + bqy_0 = dq = c$$

Portanto, o par (x_1, y_1), *com* $x_1 = x_0q$ *e* $y_1 = y_0q$ *é solução da equação difantina inicial.*

Agora, considerando a solução (x_0, y_0) *e seja o par* (x, y) *uma outra solução da equação difantina. Sendo assim,* $ax_0 + by_0 = ax + by$. *Então*

$$a(x - x_0) = b(y_0 - y),$$

e dividindo essa última igualdade por d, *teremos*

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Mas, como $(\frac{a}{d}, \frac{b}{d}) = 1$, *pelo* ***Lema 2.6.1***, *cocluímos que* $\frac{b}{d} \mid (x - x_0)$. *Portanto, existe* $t \in \mathbb{Z}$ *tal que*

$$x - x_0 = t\frac{b}{d} \Rightarrow x = x_0 + t\frac{b}{d},$$

e fazendo a substituição seguinte, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \Rightarrow \frac{a}{d} \cdot t\frac{b}{d} = \frac{b}{d}(y_0 - y) \Rightarrow t\frac{a}{d} = y_0 - y,$$

donde concluímos que

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

■

Observação: Em termos de solução de uma equação diofantina, só tem duas possibilidades. São elas:

- Não possui soluções
- Possui infinitas soluções

Por exemplo, vamos resolver $15x + 10y = 20$.

Solução. *Inicialmente, observemos que* $(15, 10) = 5$ *e que* $5 \mid 20$. *Logo, é garantido que essa equação possui solução. Vamos encontrar uma solução particular e, assim, encontrar a solução geral. Utilizando o algoritmo de Euclides para calcular* $(15, 10)$, *encontraremos as seguintes igualdades:*

$$\begin{aligned} 15 &= 10 \cdot 1 + 5, \\ 10 &= 5 \cdot 2 + 0. \end{aligned}$$

daí, temos que $5 = 15 \cdot 1 - 10 \cdot 1$. *Multiplicando essa igualdade por* 4, *teremos,* $20 = 15 \cdot 4 + 10 \cdot (-4)$. *Portanto,* $x_0 = 4$ *e* $y_0 = -4$ *são soluções particulares dessa equação e a solução geral dessa equação será*

$$x = 4 + t\frac{10}{5} = 4 + 2t \quad e \quad y = -4 - \frac{15}{5}t = -4 - 3t$$

. *Para* $t = 2$, *por exemplo, teremos* $x = 4 + 2 \cdot 2 = 8$ *e* $y = -4 - 3 \cdot 2 = -10$. *De fato,* $15 \cdot 8 + 10 \cdot (-10) = 120 - 100 = 20$.

Iremos agora resolver a equação gerada pelo problema do início da seção, a saber $5x + 3y = 50$. Mais uma vez, pelo algoritmo de Euclides, temos

$$\begin{aligned} 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 1 + 1. \end{aligned} \tag{2.3}$$

Da primeira e segunda igualdade temos

$$1 = 3 - 2 \cdot 1 \ e \ 2 = 5 - 3 \cdot 1.$$

Usando essas duas últimas, vamos obter

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ &= 5 \cdot (-1) + 3 \cdot (2), \end{aligned} \tag{2.4}$$

mas, multiplicando por 50 essa última igualdade, teremos

$$5 \cdot (-50) + 3 \cdot (100) = 50$$

e daí, temos $x_0 = -50$ e $y_0 = 100$ soluções particulares dessa equação, donde concluímos que a solução geral será, para $t \in \mathbb{Z}$,

$$x = -50 + 3t \quad e \quad y = 100 - 5t$$

. No entanto, pela natureza do problema, as soluções devem ser naturais. Para encontrá-las, basta fazermos

$$-50 + 3t \geq 0 \Rightarrow t \geq \frac{50}{3} \Rightarrow t \in \{17, 18, 19, ...\},$$

e mais ainda

$$100 - 5t \geq 0 \Rightarrow t \leq \frac{100}{5} \Rightarrow t \leq 20 \Rightarrow t \in \{20, 19, 18, 17, ...\},$$

e daí, $t \in \{17, 18, 19, 20\}$.

Para acharmos as soluções do problema, temos

- para $t = 17$, $x = 1$ e $y = 15$,
- para $t = 18$, $x = 4$ e $y = 10$,
- para $t = 19$, $x = 7$ e $y = 5$,
- para $t = 20$, $x = 10$ e $y = 20$.

Exercícios

Questão 67. *Resolva as seguintes equações:*

a) 8x + 13y = 23

b) 4x + 8y = 30

c) 9x - 6y = 6

d) 5x + 3y = 12

Questão 68. *Numa criação de coelhos e galinhas, contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?*

Questão 69. *Dispondo de R$ 100,00, de quantas maneiras podemos comprar selos de R$ 5,00 e R$ 7,00?*

Questão 70. *Subindo uma escada de dois em dois degraus, sobra uma degrau. Subinda a mesma escada de três em três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que seu número é múltiplo de* 7 *está compreendido entre* 40 *e* 60.

Questão 71. *(COLÉGIO NAVAL - 2012 - ADAPTADA) Quais valores de* x *e* y *que fazem com que de* $2160x + 1680y$ *resulte no menor valor positivo?*

a) $x = 1$ *e* $y = 2$

b) $x = 3$ *e* $y = 4$

c) $x = -3$ *e* $y = -4$

d) $x = -3$ *e* $y = 4$

Questão 72. *Determinar o menor inteiro positivo que dividido por 8 e por 15 deixa os restos* 6 *e* 13*, respectivamente.*

Questão 73. *Determinar as duas menores frações positivas que tenham* 13 *e* 17 *para denominadores e cuja soma seja igual a* $\frac{305}{221}$.

Relatório

Nessa aula, resolvemos muitos exercícios contextualizados. Iniciamos com o "jogo da escova diofantina" e, em determinado momento da aula, começamos uma discussão sobre o porquê de um conteúdo tão interessante e que possui tantas aplicações não ser trabalhado no ensino básico. Por fim, fizemos uma relação das equações diofantinas com o estudo das retas.

2.8 Congruências

Plano de Aula

Tema: Congruências e Aplicações
Objetivos: Levar o(a) aluno(a) a: • Compreender o conceito de congruências; • Estudar as propriedades da aritmética dos restos; • Estabelecer critérios de divisibilidade para números naturais.

Conteúdos:
Estudo da congruência modular e suas propriedades.

Metodologia:
Iniciaremos a aula lendo um texo cujo título é "Sexta-feira 13" da Revista RPM, página 43, que encontra-se no apêndice desse trabalho. Esse texto traz uma boa introdução para trabalharmos a ideia de analisarmos o resto das divisões aplicados a uma situação do cotidiano. Em seguida, falaremos da definição formal de congruência modular, resolveremos alguns exercícios interessantes e falaremos de algumas outras aplicações da aritmética modular.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Fonseca, Rubens. **Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Oliveira, Maycon Costa de.**Aritmética: Criptografia e outras aplicações de Congruências**.2013.74 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Mato Grosso do Sul, Campo Grande.

Texto didático

O estudo da aritmética modular introduz o conceito de congruências, linguagem que foi desenvolvida por Karl Friedrich Gauss no início do século XIX e faz parte da Teoria dos Números e é de grande importância pois possui muitas aplicações nos dias

atuais como por exemplo na criptografia e na geração de números pseudoaleatórios. Este conceito é útil ainda para a resolução de problemas bastante interessantes, cuja resolução seria muito engenhosa sem o uso dessa ferramenta matemática. Por exemplo, considere os seguintes problemas abaixo:

1. Que horas serão daqui a 50 horas?
2. No ano de 2006 o dia $1^{\underline{o}}$ de janeiro foi em um domingo. Que dia da semana será o $186^{\underline{o}}$ dia desse ano?
3. Qual é o resto da divisão de 17^{301} por 5?

Problemas como esses podem ser facilmente resolvidos, utilizando-se as propriedades da congruência.

Definição 2.8.1 (Aritmética Modular). *A aritmética modular é um sistema em que as operações entre números inteiros são feitas em módulo um outro inteiro n, positivo e diferente de zero. Para isto definimos que um inteiro a é congruente a outro inteiro b módulo m, $m \in \mathbb{Z}$, $m > 1$, se a divisão de a e b por m deixam o mesmo resto. Indica-se $a \equiv b \ (mod\, m)$. Por exemplo, $9 \equiv 5 \ (mod\, 4)$ pois, ambos deixam restos 1 na divisão por 4. Temos também que, $15 \equiv 2 \ (mod\, 13)$.*

Proposição 2.8.1. *$a \equiv b \ (mod\, n) \Leftrightarrow a - b$ é divisível por m.*

Demonstração . *De fato, se a e b deixam o mesmo resto na divisão por m, temos*

$$a = mq_1 + r_1 \quad e \quad b = mq_2 + r_2, \ com \ \ 0 \leq r_1 < m \ \ e \ \ 0 \leq r_2 < m$$

mas como, por hipótese, $r_1 = r_2$, temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2)$, donde concluímos que $m \mid (a - b)$.

Vamos provar agora a outra implicação. Temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$. Mas, como $m \mid (a - b)$ e $m \mid m(q_1 - q_2)$, concluímos que $m \mid (r_1 - r_2)$. No entanto, notemos que $-m < r_1 - r_2 < m$. Porém, como $r_1 - r_2$ é um múltiplo de m e, entre $-m$ e m, o único múltiplo de m é 0, concluímos que $r_1 - r_2 = 0$, o que resulta $r_1 = r_2$.

■

As propriedades abaixo serão importantes na resolução de vários exercícios.

Propriedades. *Sejam a, b, c e m inteiros, $m > 1$ e $n \in \mathbb{N}$, então*

1. *$a \equiv a \ (mod\, m)$. (Reflexividade)*

2. *Se* $a \equiv b \ (mod\, m)$ *, então* $b \equiv a \ (mod\, m)$*. (Simetria)*

3. *Se* $a \equiv b \ (mod\, m)$ *e* $b \equiv c \ (mod\, m)$ *, então* $a \equiv c \ (mod\, m)$*. (Transitividade)*

4. *Se* $a \equiv b \ (mod\, m)$ *e* $c \equiv d \ (mod\, m)$ *, então* $a + c \equiv b + d \ (mod\, m)$*.*

5. *Se* $a \equiv b \ (mod\, m)$ *e* $c \equiv d \ (mod\, m)$ *, então* $ac \equiv bd \ (mod\, m)$*.*

6. *Se* $a \equiv b \ (mod\, m)$*, então* $a^n \equiv b^n \ (mod\, m)$*,* $c \in \mathbb{N}$*.*

7. $a + c \equiv b + c \ (mod\, m) \Leftrightarrow a \equiv b \ (mod\, m)$*.*

8. *Se* $ac \equiv bc \ (mod\, m)$ *e* $(c, m) = 1$*, então* $a \equiv b \ (mod\, m)$*.*

9. *Se* $a \equiv b \ (mod\, m_i), i = 1, 2, ..., r$*, então* $a \equiv b \ (mod\, [m_1, m_2, ..., m_r])$*.*

Demonstração . *Vejamos a demonstração de cada uma dessas propriedades.*

1 *De fato,* $m \mid (a - a)$ *para todo* $a \in \mathbb{Z}$*.*

2 *Com efeito, se* $m \mid (a - b)$*, então* $m \mid (b - a)$*.*

3 *De fato, se* $m \mid (a - b)$ *e* $m \mid (b - c)$*, então* $m \mid (a - b) + (b - c)$*. Daí,* $m \mid (a - c)$*, donde concluímos que* $a \equiv c \ (mod\, m)$*.*

4 *De fato, se* $m \mid (a - b)$ *e* $m \mid (c - d)$*, então* $m \mid (a - b) + (c - d) = (a + c) - (b + d)$*, o que mostra que* $a + c \equiv b + d \ (mod\, m)$*.*

5 *Note que* $ac - bd = a(c - d) + d(a - b)$*. Portanto,* $m \mid (ac - bd)$*. Daí,* $ac \equiv bd \ (mod\, m)$*.*

6 *Com efeito, utilizando a propriedade 5 reiteradamente, temos*

$$\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n fatores} \equiv \underbrace{b \cdot b \cdot b \cdot b \cdots b}_{n fatores} \ (mod\, m),$$

o que mostra que $a^n \equiv b^n \ (mod\, m)$*.*

7 *De fato, como* $(a + c) - (b + c) = a - b$*, então* $m \mid a - b \Leftrightarrow m \mid (a + c) - (b + c)$*. Daí,* $a + c \equiv b + c \ (mod\, m) \Leftrightarrow a \equiv b \ (mod\, m)$*.*

8 *Com efeito, se* $ac \equiv bc \ (mod\, m)$*, então* $m \mid (ac - bc) = c(a - b)$*. No entanto, sendo* m *e* c *primos entre si, temos que* $m \mid (a - b)$*, o que mostra que* $a \equiv b \ (mod\, m)$*.*

9 *Com efeito, como* $a \equiv b \ (mod\, m_i), i = 1, 2, ..., r$*, então* $m_i \mid (a - b)$*, para todo* i*. Sendo assim,* $(a - b)$ *é um múltiplo de cada* m_i*, donde segue que* $[m_1, m_2, ..., m_r] \mid (a - b)$*, como queríamos demonstrar.*

■

Observação: As três primeiras propriedades descritas anteriormente, permite-nos dizer que a congruência modular é uma relação de equivalência no conjunto dos números inteiros.

Vejamos um exemplo bastante interessante que aborda algumas das propriedades vistas anteriormente. Iremos mostrar que, para todo $n \in \mathbb{N}$, $101^{6n} - 1$ é divisível por 70. É claro que para isso, basta mostrar que $101^{6n} \equiv 1 \ (mod\, 70)$. Com efeito, $101 \equiv 3 \ (mod\, 7)$. Da propriedade 6, temos $101^6 \equiv 3^6 \ (mod\, 7)$. Mas, $3^6 \equiv 1 \ (mod\, 7)$. Daí, pela propriedade 3, $101^6 \equiv 1 \ (mod\, 7)$ e, pela propriedade 6, para todo $n \in \mathbb{N}$, teremos $101^{6n} \equiv 1 \ (mod\, 7)$. Além disso, temos $101 \equiv 1 \ (mod\, 10)$. Sendo assim, temos $101^{6n} \equiv 1 \ (mod\, 10)$. Portanto, pela propriedade 9, $101^{6n} \equiv 1 \ (mod\, [7, 10])$, ou seja, $101^{6n} \equiv 1 \ (mod\, 70)$, como queríamos mostrar.

Um outro exemplo seria calcularmos o resto da divisão de $50^{20} + 35^{35}$ por 3. Utilizando as propriedades das congruências estudadas, tal cálculo será bastante simples. Para isso, notemos que $50 \equiv -1 \ (mod\, 3)$. Portanto, $50^{20} \equiv (-1)^{20} \equiv 1 \ (mod\, 3)$. Temos também que $35 \equiv -1 \ (mod\, 3)$ e, portanto, $35^{35} \equiv (-1)^{35} \equiv -1 \ (mod\, 3)$. Utilizando a propriedade 4, temos que $50^{20} + 35^{35} \equiv 1 + (-1) \equiv 0 \ (mod\, 3)$, mostrando que o resto da divisão de $50^{20} + 35^{35}$ por 3 é 0.

Agora, vamos ver importantes consequências dessas propriedades que serão bastante úteis na resolução de alguns problemas muito interessantes.

Proposição 2.8.2. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $(a - b) \mid (a^n - b^n)$.*

Demonstração . *De fato, em particular sendo $m = a - b$, temos $a \equiv b \ (mod\, m)$, pois é claro que $a-b \mid a-b$. Da propriedade 6, temos $a^n \equiv b^n \ (mod\, m)$, o que prova a proposição.*

■

Proposição 2.8.3. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, $(a + b) \mid (a^{2n+1} + b^{2n+1})$.*

Demonstração . *Com efeito, considerando em particular $m = a + b$, temos $a \equiv -b \ (mod\, m)$. Como, para todo $n \in \mathbb{N}$, temos que $2n + 1$ é um número ímpar, é fácil ver que $a^{2n+1} \equiv -b^{2n+1} \ (mod\, m)$, o que prova a proposição.*

■

Proposição 2.8.4. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, temos que $(a + b) \mid (a^{2n} - b^{2n})$.*

Demonstração . *Mais uma vez, considerando $m = a+b$, verificando que $a \equiv -b \ (mod\, m)$ e que, para todo $n \in \mathbb{N}$, o número $2n$ é par, facilmente observa-se que $a^{2n} \equiv b^{2n} \ (mod\, m)$, como queríamos demonstrar.*

■

Como exemplo, vamos mostrar que, para todo $n \in \mathbb{N}$, $11 \mid (10^{2n+1} + 1)$. De fato, pela **proposição 2.8.3**, $11 = (10 + 1) \mid (10^{2n+1} + 1^{2n+1}) = 10^{2n+1} + 1$, como queríamos demonstrar.

Por fim, veremos uma definição que será importante nas seções que estão por vir.

Definição 2.8.2. *Um inteiro a é dito inversível módulo m se existir um outro inteiro a' tal que*

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

Por exemplo, 2 e 4 são inversíveis módulo 7, pois $2 \cdot 4 = 8 \equiv 1\ (mod\, 7)$.

Proposição 2.8.5. *Se um inteiro a é inversível módulo m, então $(a, m) = 1$.*

Demonstração . *De fato, como por hipótese a é inversível módulo m, temos que*

$$a \cdot a' \equiv 1\ (mod\, m) \Rightarrow aa' = mk + 1 \Rightarrow aa' - mk = 1,$$

daí, pela Propriedade 1 da seção de MDC, temos que $(a, m) = 1$.

Vejamos como o problema 3 proposto no início da seção será resolvido facilmente utilizando-se as propriedades estudadas nessa seção. O problema consiste em saber qual é o resto da divisão de 17^{301} por 5. É simples verificar, inicialmente, que $17 \equiv 2\ (mod\, 5)$. Daí, temos que $17^2 \equiv 2^2 \equiv 4 \equiv -1\ (mod\, 5)$. Portanto,

$$(17^2)^{150} = 17^{300} \equiv (-1)^{150} \equiv 1\ (mod\, 5)$$

.

No entanto, como $17 \equiv 2\ (mod\, 5)$, teremos

$$17^{300} \cdot 17 \equiv 1 \cdot 2\ (mod\, 5) \Rightarrow 17^{301} \equiv 2\ (mod\, 5)$$

.

Mostrando assim que o resto dessa divisão é 2. Sem o uso dessas propriedades, encontrar esse resultado seria um processo bastante engenhoso.

Exercícios

Questão 74. *Ache o resto da divisão de*

a) 7^{10} *por* 51

b) 2^{100} *por* 11

Questão 75. *Mostre que, para todo* $n \in \mathbb{N}$,

a) $9 \mid 10^n - 1$

b) $8 \mid 3^{2n} - 1$

c) $3 \mid 10^n - 7^n$

d) $13 \mid 9^{2n} - 2^{4n}$

e) $17 \mid 10^{2n+1} + 7^{2n+1}$

Questão 76. *(COLÉGIO NAVAL) O número a, dividido por* 11*, deixa resto* 2 *e b, dividido pelo mesmo divisor, deixar resto* 3*. Calcule o menor número a ser subtraído de* $a^3 + b^2$*, para que se obtenha um múltiplo de* 11*.*

Questão 77. *Prove que, para todo* $n \in \mathbb{N}$, $3^{6n} - 2^{6n}$ *é divisível por* 35*.*

Questão 78. *Mostre que a equação* $x^3 - 117y^3 = 5$ *não possui soluções inteiras.*

Questão 79. *Mostre que para todo* $n \in \mathbb{N}$*, é verdade que* $13|7^{2n+1} + 6^{2n+1}$.

Relatório

Nessa aula, estudamos conceito de congruência modular, demonstrando as propriedades e chamando por vezes os alunos para irem até o quadro e resolverem alguns problemas desafiantes, inclusive alguns problemas do Teste 1. Para nossa surpresa, os alunos demonstraram bastante desenvoltura na resolução dos exercícios, mostrando-se mais uma vez surpresos com as aplicações das propriedades estudadas.

2.9 Teorema de Euler e Fermat

Plano de Aula

Tema: Teorema de Euler e Fermat e aplicações

Objetivos:
Levar o(a) aluno(a) a:

- Aplicar na resolução de problemas o Teorema de Euler;
- Aplicar na resolução de problemas o Teorema de Fermat.

Conteúdos:
Estudo do Teorema de Euler e Fermat.

Metodologia:
Iniciaremos a aula propondo alguns desafios que cujas resoluções serão bastante engenhosas com objetivo de levar os alunos a pensarem em uma maneira mais prática de resolvê-los. A partir daí, definiremos a função "fi" de Euler e, em seguida, trataremos de uma maneira mais formal os conceitos a serem estudados.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila

Referências:

- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.

Texto didático

Qual é o resto da divisão de 400^{110} por 23 ? Bem, apesar de já termos conhecimento de várias propriedades da congruência modular, o problema proposto não seria tão simples de ser resolvido. No entanto, estudaremos a seguir o teorema de Euler e, em seguida, o teorema de Fermat, que serão ferramentas úteis na resolução de problemas em que queremos achar o resto da divisão de inteiros por números primos. Como já foi dito antes, esses dois matemáticos muito contribuíram para o desenvolvimento da Teoria dos Números.

Figura 23 – Leonhard Euler

Fonte: google

Vejamos inicialmente a seguinte definição:

Definição 2.9.1. *Seja* $m \in \mathbb{N}^*$. *Seja* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_n}$ *a decomposição de* m *em fatores primos. Definimos:*

$$\varphi(m) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot ... \cdot p_n^{\alpha_n - 1}(p_1 - 1)(p_2 - 1) \cdots (p_n - 1).$$

onde

$$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N},$$

é chamada de função fi de Euler.

Por exemplo, vamos calcular $\varphi(20)$. Como $20 = 2^2 \cdot 5$, então $\varphi(2^2 \cdot 5) = 2^{2-1} \cdot 5^{1-1}(2-1)(5-1) = 8$. E qual é o valor de $\varphi(36)$?. Ora, $\varphi(36) = \varphi(2^2 \cdot 3^2) = 2^{2-1} \cdot 3^{2-1}(2-1)(3-1) = 12$.

Note que se se p é primo, então $\varphi(p) = p - 1$. De fato, pela definição vista, $\varphi(p) = p^{1-1} \cdot (p-1) = p - 1$. Por exemplo, $\varphi(23) = 23 - 1 = 22$.

A função φ é de grande utilidade na Teoria dos Números, em especial no estudo do Teorema de Euler e do Teorema de Fermat.

Os próximos exemplos serão fundamentais para a sequência do nosso estudo.

- **Exemplo 1** - Qual é o resto da divisão de 7^{50} por 20?

Para resolvermos esse problema, notemos que

$$7^2 \equiv 9 \,(mod\, 20) \Rightarrow 7^4 \equiv 81 \equiv 1 \,(mod\, 20) \Rightarrow 7^8 \equiv 1 \,(mod\, 20)$$

Mas, como $50 = 8 \cdot 6 + 2$, temos

$$7^{50} = (7^8)^6 \cdot 7^2 \equiv 1 \cdot 7^2 \equiv 9 \, (mod \, 20)$$

Portanto, o resto da divisão de 7^{50} por 20 é 9.

- **Exemplo 2** - Qual é o resto da divisão de 3^{100} por 34?

Mais um vez, utilizando as propriedades de congruências estudadas, temos que

$$3^4 \equiv 81 \equiv 13 \, (mod \, 34) \Rightarrow 3^8 \equiv 169 \equiv -1 \, (mod \, 34) \Rightarrow 3^{16} \equiv 1 \, (mod \, 34).$$

Mas, como $100 = 16 \cdot 6 + 4$, temos

$$3^{100} = (3^{16})^6 \cdot 3^4 \equiv 1 \cdot 3^4 \equiv 13 \, (mod \, 34),$$

donde concluímos que o resto dessa divisão é 13.

Notemos, porém, que $(7, 20) = (3, 34) = 1$ e que para resolvermos o exemplo 1, foi crucial descobrirmos que $7^8 \equiv 1 \, (mod \, 20)$ e, no exemplo 2, que $3^{16} \equiv 1 \, (mod \, 34)$. No entanto, é fácil ver que $\varphi(20) = \varphi(2^2 \cdot 5) = 2^{2-1} \cdot 5^{1-1} \cdot (2-1) \cdot (5-1) = 5 \cdot 4 = 8$. Mais ainda, também é bastante simples verificarmos que $\varphi(34) = 2^{1-1} \cdot 17^{1-1}(2-1)(17-1) = 16$. Em outras palavras, nesses dois exemplos, podemos observar que

$$7^{\varphi(20)} \equiv 1 \, (mod \, 20) \text{ e que } 3^{\varphi(34)} \equiv 1 \, (mod \, 34)$$

Esses dois fatos observados podem ser generalizados com o seguinte teorema.

Teorema 2.9.1 (**Teorema de Euler**). *Sejam $m, a \in \mathbb{N}$ com $m > 1$ e $(a, m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 \, (mod \, m)$$

A demonstração desse teorema está no apêndice desse trabalho.

Por exemplo, qual é o resto da divisão de 5^{61} por 33? Ora, como $(5, 33) = 1$, e $\varphi(33) = 3^0 \cdot 11^0(3-1)(11-1) = 20$, pelo Teorema de Euler, $5^{20} \equiv 1 \, (mod \, 33)$. Daí,

$$5^{61} = 5^{60+1} \equiv (5^{20})^3 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \, (mod \, 33),$$

o que mostra que o resto dessa divisão é 5.

Uma consequência desse Teorema será vista a seguir.

Teorema 2.9.2 (**Teorema de Fermat**). *Seja p um número primo e $a \in \mathbb{Z}$ com $(a, p) = 1$. Então,*

$$a^p \equiv a \ (mod\, p).$$

Demonstração . *Como p é primo, $\varphi(p) = p-1$ e, mais ainda, como $p \nmid a$, pelo Teorema de Euler, teremos*

$$a^{\varphi(p)} \equiv 1 \ (mod\, p) \Rightarrow a^{p-1} \equiv 1 \ (mod\, p).$$

Como $a \equiv a \ (mod\, p)$ e utilizando as propriedades das congruências, temos

$$a^{p-1} \cdot a \equiv 1 \cdot a \ (mod\, p) \Rightarrow a^p \equiv a \ (mod\, p)$$

.

■

Observação: Sendo p primo, $a \in \mathbb{Z}$ com $(a, p) = 1$, concluímos, na demonstração anterior, que

$$a^{p-1} \equiv 1 \ (mod\, p)$$

Esse resultado é conhecido como **Pequeno Teorema de Fermat**.

Por fim, vamos analisar o seguinte situação: quais são os dois últimos algarismos do número 3^{121} ? É claro que para descobrirmos esses dois algarismos, precisamos dividir 3^{121} por 100. Como $(3, 100) = 1$, uma boa estratégia é utilizarmos o Teorema de Euler. Com um simples cálculo, descobrimos que $\varphi(100) = 40$ e, portanto, $3^{40} \equiv 1 \ (mod\, 100)$. Daí

$$3^{121} = 3^{40 \cdot 3+1} \equiv (3^{40})^3 \cdot 3 \equiv 3 \ (mod\, 100).$$

Logo, os dois últimos algarismos do número 3^{121} é 03.

Porém, fazendo os devidos cálculos, também poderíamos descobrir que o menor inteiro n tal que $3^n \equiv 1 \ (mod\, 100)$ é $n = 20$, ou seja, $3^{20} \equiv 1 \ (mod\, 100)$ (fica a cargo de leitor fazer tal verificação). Dizemos nesse caso que 20 é a ordem de 3 com relação a 100. Em notação, $\text{ord}_{100}(3) = 20$. De uma maneira geral, temos

Definição 2.9.2. *Sejam $a, m \in \mathbb{N}^*$, com $m > 1$ e $(a, m) = 1$. Definimos como a ordem de a com relação a m como sendo o número natural tal que*

$$ord_m(a) = min\{i \in \mathbb{N}^*; a^i \equiv 1 \ (mod\, m)\}.$$

Proposição 2.9.1. *Se $k = ord_m(a)$, então $k \mid \varphi(m)$.*

Demonstração . *De fato, pela divisão euclidiana, podemos escrever*

$$\varphi(m) = kq + r, \text{ com } 0 \leq r < k.$$

Daí, supondo, por absurdo, que $r \neq 0$*, teremos*

$$1 \equiv a^{\varphi(m)} \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv a^r \ (mod\, m),$$

mas isso é um absurso pois supomos $0 < r < k$ *e* k *é o menor expoente não nulo tal que* $a^k \equiv 1 \ (mod\, m)$*.*

■

Vejamos abaixo alguns exemplos resolvidos que mostram aplicações do que acabamos de estudar.

Exemplos resolvidos

1 Mostre que $18 \mid 5^{1000} + 5$.

2 Qual é o resto da divisão de 4^{110} por 23?

Resolução

1. Inicialmente, notemos que $(5, 18) = 1$. Daí, podemos utilizar o Teorema de Euler. Temos então que $\varphi(18) = \varphi(2 \cdot 3^2) = 2^{1-1} \cdot 3^{2-1} \cdot (2-1) \cdot (3-1) = 3 \cdot 2 = 6$. Portanto, $5^6 \equiv 1 \ (mod\ 18)$. No entanto, como $1000 = 6 \cdot 166 + 4$, segue que $5^{1000} \equiv (5^{166})^6 \cdot 5^4 \equiv 1 \cdot 625 \equiv 13 \ (mod\ 18)$. Portanto, $5^{100} + 5 \equiv 13 + 5 \equiv 0 \ (mod\, 18)$, como queríamos mostrar.

2. Note que $(4, 23) = 1$ e, como 23 é primo, pelo Pequeno Teorema de Fermat, temos

$$4^{23-1} = 4^{22} \equiv 1 \ (mod\, 23) \Rightarrow (4^{22})^5 \equiv 1^5 \ (mod\, 23) \Rightarrow 4^{110} \equiv 1 \ (mod\, 23).$$

Portanto, o resto divisão de 4^{110} por 23 é 1.

Exercícios

Questão 80. *Determine:*

a) $\varphi(30)$

b) $\varphi(120)$

c) $\varphi(35)$

d) $\varphi(36)$

Questão 81. *Calcule* 3^n*, com* $1 \leq n \leq 20$ *e conclua que, de fato,* $ord_{100}(3) = 20$*. Verifique se é preciso calcular todas as potências de* 3 *para encontrar* $ord_{100}(3)$*.*

Questão 82. *Encontre o resto da divisão de* 39^{3602} *por* 14*.*

Questão 83. *Prove que* $2222^{5555} + 5555^{2222}$ *é divisível por* 7*.*

Questão 84. *Mostre que não existe inteiro* x *tal que* $103 \mid x^3 - 2$*.*

Questão 85. *O resto da divisão de* $2^{70} + 3^{70}$ *por 13 é*

a) 0

b) 1

c) 2

d) 3

e) 4

Questão 86. *Se* n *é um inteiro não divisível por* 5*, mostre que ao dividir* $n^4 - 1991$ *por* 5*, o resto é zero.*

Questão 87. *Demonstre que* $61 \mid 20^{15} - 1$*.*

Questão 88. *Mostre que, para todo* $n \in \mathbb{N}$*, é natural o número*

$$\frac{3}{5}n^5 + \frac{2}{3}n^3 + \frac{11}{15}n.$$

Relatório

Nessa aula, trabalhamos com os alunos alguns problemas cujas resoluções seriam bastante engenhosas sem o uso dos Teoremas de Euler e Fermat. Houve bastante participação dos discentes durante a aula e os mesmos mostraram-se muito entusiasmados com as aplicações desses respectivos teoremas.

2.10 Criptografia RSA

Plano de Aula

Tema: Estudo da Criptografia RSA

Objetivos:
Levar o(a) aluno(a) a:

- Estudar e compreender o conceito de Criptografia e sua aplicação nos dias atuais;
- Conhecer os métodos de Criptografia mais usados nos dias atuais;
- Fazer uso da Aritmética Modular e dos Números Primos como aplicação da ideia de Criptografia.

Conteúdos:
Teorema de Euler e Fermat, Aritmética Modular, Criptografia.

Metodologia:
Iniciaremos a aula com um vídeo no Youtube sobre Criptografia, em seguida mostraremos o método de criptografia chamado RSA. Por fim, iremos propor algumas mensagens para os alunos decifrarem.

Avaliação:
Cada discente será avaliado através da participação nas discussões.

Recursos Didáticos:
Quadro branco, pincel, aparelho de som, notebook, data-show e apostila.

Referências:

- Coutinho, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.
- Fomin, Dmitri. **Círculos Matemáticos**. Rio de Janeiro: IMPA, 2012.
- Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.
- Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números**. Rio de Janeiro: SBM, 2012.
- Oliveira, Maycon Costa de.**Aritmética: Criptografia e outras aplicações de Congruências**.2013.74 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Mato Grosso do Sul, Campo Grande.

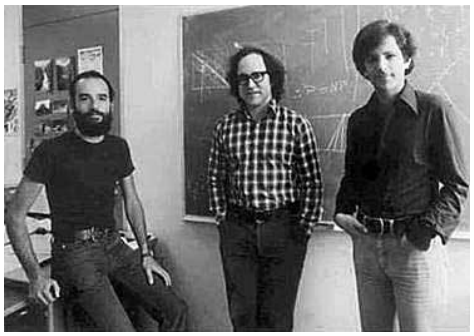
Texto didático

Maria e José são dois adolescentes bastante estudiosos. Certo dia, José perguntou a Maria: "qual é a matéria que você mais gosta?". Maria respondeu: "PDWHPDWLFD". Sabendo-se que José conseguiu decifrar esse código, qual foi a resposta de Maria?

Bem, parece um pouco esquisita essa resposta, mas Maria utilizou uma forma de codificar sua mensagem. Em outras palavras, ela criptografou a sua resposta.

Umas das áreas mais importantes da Teoria dos Números é criptografia. O termo criptografia vem do grego kryptós, "escondido", e gráphein, "escrita" e é um processo através do qual uma mensagem é codificada de forma que apenas o emissor e receptor da mensagem consigam decifrá-la. Nessa seção, estudaremos um método criptográfico chamado de RSA, que leva este nome devido aos seus inventores Ronald Rivest, Adi Shamir e Leonard Adleman em 1977.

Figura 24 – Criadores do método RSA - Da esquerda para a direita, temos Adi Shamir, Ronald Rivest e Leonard Adleman.



Fonte: google

O RSA, por ser um método de chave pública, permite que qualquer usuário codifique mensagens, mas como a chave de decodificação é secreta, só o destinatário legítimo poderá decodificá-la.

A impossibilidade de quebrar a chave de decodificação é possível pela não existência de algoritmos eficientes para a fatoração de inteiros em fatores primos, sobretudo, se o número de algarismos é 100 ou maior. O tempo de codificação de uma mensagem é praticamente desprezível, mas o tempo de decodificação pode tornar o processo inviável.

Veremos abaixo como funciona tal método.

- **Passo 1 -** Estabelecer o seguinte critério abaixo (que na verdade é arbitrário), associando a cada letra do alfabeto um número.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Iremos codificar a palavra SPORT. Mas, antes disso iremos fazer a pré-codificação. De acordo com a tabela acima, a mensagem pré-codificada será

2825242729

.

Segundo o método RSA, devemos escolher dois primos , p e q e calcular $n = pq$. Por exemplo, se $p = 5$ e $q = 7$, $n = 35$. Para codificar a mensagem utilizaremos n. O valor de n pode tornar-se público, já p e q precisam ser mantidos em segredo.

- **Passo 2 -**Separar a mensagem em blocos, onde cada bloco deve ser composto por números menores que n. Como no nosso caso, $n = 35$, teremos

$$28 - 25 - 24 - 27 - 29$$

Na verdade, a maneira de escolher os blocos não é única e eles não precisam ter, necessariamente, o mesmo tamanho. No entanto, é importante alguns cuidados serem tomados, como por exemplo, não iniciar um bloco com 0 para não gerar problemas na decodificação já que, por exemplo, o bloco 065 poderia ser confundido com o bloco 65. Denotaremos b_i cada bloco, onde $i = 1, 2, 3, .., k$. Para codificar a mensagem, precisamos de n e de um inteiro positivo r tal que r seja inversível módulo $\varphi(n)$. Em outras palavras, o MDC entre r e $(p-1)\cdot(q-1)$ deve ser igual a 1. No nosso caso, como $p = 5$ e $q = 7$, podemos, por exemplo, escolher $r = 5$ já que $(5-1)\cdot(7-1) = 24$ e $(5, 24) = 1$. O par (r, n) será a chave de codificação e a regra de codificação será

$$b^r \equiv a \,(mod\, n), \text{ com } a < n.$$

Os valores de a encontrados, formarão os blocos da mensagem codificada. Vamos, então, efetuar os cálculos da codificação da palavra SPORT, considerando $r = 5$ e $n = 35$.

1 - Precisamos achar a tal que $28^5 \equiv a \,(mod\, 35)$. Facilmente, descobrimos que nesse primeiro bloco $a = 28$.

2 - Agora, calculemos $25^5 \equiv a \,(mod\, 35)$ que facilmente resultará em $a = 30$.

3 - Nesse bloco, calculando $24^5 \equiv a \,(mod\, 35)$, achamos $a = 19$.

4 - Basta calcular $27^5 \equiv a \,(mod\, 35)$ onde acharemos $a = 27$.

5 - Por fim, nesse bloco, efetuando os cálculos de $29^5 \equiv a \,(mod\, 35)$, encontramos $a = 29$.

Agora, reunindo todos os valores de a encontrados, a mensagem codificada fica

$$28 - 30 - 19 - 27 - 29$$

- **Passo 3 -** Agora, procederemos a decodificação da mensagem. Devemos encontrar a chave de decodificação (d, n) tal que d é o inverso de r módulo $\varphi(n)$. Como $\varphi(35) = 24$ e $r = 5$, teremos

$$5d \equiv 1 \,(mod\, 24)$$

Facilmente encontramos $d = 5$, pois $5 \cdot 5 = 25 \equiv 1\ (mod\ 24)$.

Portanto, a chave de decodifação também é o par $(5, 35)$. Sendo a um bloco codificado, denotaremos por $D(a)$ o resultado do processo de decodificação do bloco a, de forma que

$$D(a) = \text{resto da divisão de } a^d \text{ por } n$$

Bem, ficará a cargo do leitor fazer a decodificação e verificar se de fato a mensagem decodificada será SPORT.

Obviamente, pelo fato de escolhermos primos pequenos, os cálculos são bastante triviais. No entanto, o método RSA mostra-se bastante seguro quando a escolha dos primos para formar a chave de codificação são muito grandes, com a diferença $|p - q|$ grande, ficando assim extremamente difícil quebrar a mensagem e asssim desvendando-a.

Exercícios

Questão 89. *Utilizando o método de Criptografia RSA , crie uma chave de codificação, mostre a um colega e peça pra ele fazer a codificação de alguma palavra do nosso alfabeto. De posse da mensagem codificada por seu colega, tente decodificá-la.*

Questão 90. *Utilizando o método RSA e considerando os primos $d = 3$ e $p = 7$, faça a codificação da palavra MATEMÁTICA.*

Questão 91. *Sabendo-se que $n = 3552377$ e que o produto $(p-1)(q-1)$ é igual a 3548580, encontre os valores de p e q.*

Questão 92. *A chave pública utilizada por determinado banco é a seguinte $n = 10403$ e $r = 8743$. Recentemente, o computadores do banco receberam, de local indeterminado, a seguinte mensagem:*

$$4746 - 8214 - 9009 - 4453 - 8198$$

.

O que diz a mensagem enviada a esse banco?

Relatório

Iniciamos a aula com um vídeo que trata de maneira lúdica a criptografia. Em seguida, falamos da importância da criptografia nos dias atuais e definimos o método criptográfico chamado de RSA, mostrando como funciona tal método. Por fim, resolvemos alguns exercícios bastante interessantes cuja participação dos alunos foi intensa.

3 Teste 2 e análise dos resultados

Com o objetivo de verificarmos o aprendizado dos alunos nos temas específicos abordados durante o curso, realizamos um segundo teste chamado de "Teste 2". As questões abordadas nesse teste foram semelhantes aos do "Teste 1". A análise por questão e análise geral será apresentada a seguir.

3.1 Análise das questões do Teste 2

Questão 1

Qual é o resto da divisão de 7^{121} por 13?

(a) 4 (b) 5 (c) 6 (d) 7 (e)8

Alternativa correta: D

A tabela abaixo mostra o percentual de alunos (de um total de 18 participantes) que assinalaram cada alternativa da questão 1.

Tabela 16 – Questão 1T2

Alternativa	Percentual de alunos
a	11,1
b	11,1
c	0
d	61,1
e	16,7

Essa questão tinha como objetivo verificar se os alunos compreenderam bem o conceito de congruência modular e uma aplicação do Teorema de Euler. A partir da **Tabela 16**, vemos que um percentual razoável apropiou-se desse tema.

Questão 2

Se hoje é sábado, que dia será daqui a 999 dias?

(a) segunda-feira (b) sábado (c) domingo (d) quarta-feira (e) sexta-feira

Alternativa correta: D

A tabela abaixo mostra o percentual de alunos (de um total de 18 participantes) que assinalaram cada alternativa da questão 2.

Tabela 17 – Questão 2T2

Alternativa	Percentual de alunos
a	5,5
b	0
c	0
d	94,4
e	0

Nessa questão, queríamos avaliar se os alunos apropriaram-se do tema Divisão Euclidiana, pois seria necessário, para resolver essa questão, realizar a divisão e analisar o resto da mesma. Pelo percentual de acertos apresentado pela **Tabela 17**, concluímos que o aproveitamento desse conhecimento foi bastante satisfatório.

Questão 3

Em um pedágio, cada carro paga R$ 7,00 e cada motocicleta paga R$ 4,00. Sabendo que foi arrecadado em um certo período de tempo R$ 142,00, a alternativa que apresenta a menor e a maior quantidade possível de motos, respectivamente, é:

(a) 10 e 12 (b) 3 e 15 (c) 4 e 30 (d) 4 e 32 (e)4 e 32

Alternativa correta: D

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 3.

Tabela 18 – Questão 3T2

Alternativa	Percentual de alunos
a	11,1
b	0
c	5,5
d	83,3
e	0

O objetivo dessa questão foi analisarmos os avanços no que se refere ao conhecimento das Equações Diofantinas verificando se os alunos conseguiriam criar o modelo necessário bem como reslover de maneira satisfatória a equação. A partir da **Tabela 18**, notamos que uma porcentagem bastante alta de alunos obtiveram sucesso nessa questão.

Questão 4

O número de divisores do número $6^3 \cdot 25$ é

(a) 45 (b) 48 (c) 65 (d) 70 (e)80

Alternativa correta: B

A **Tabela 19** mostra o percentual de alunos que assinalaram cada alternativa da questão 4.

Tabela 19 – Questão 4T2

Alternativa	Percentual de alunos
a	5,5
b	77,8
c	5,5
d	5,5
e	5,5

Para obter corretamente o número de divisores desse número, o aluno deveria ter o conhecimento de decomposição em números primos e, em seguida, efetuar o cálculo do número de divisores. De acordo com a **Tabela 19**, um percentual de 77,8% alunos obtiveram êxito nessa questão. Isso mostra que tal tema foi bem aproveitado pelos alunos.

Questão 5

O resto da divisão por 3 do número $1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + \cdots + 3^9 + 3^{10}$ é

(a) 1 (b) 2 (c) 3 (d) 4 (e)5

Alternativa correta: A

A **Tabela 20** mostra o percentual de alunos que assinalaram cada alternativa da questão 5.

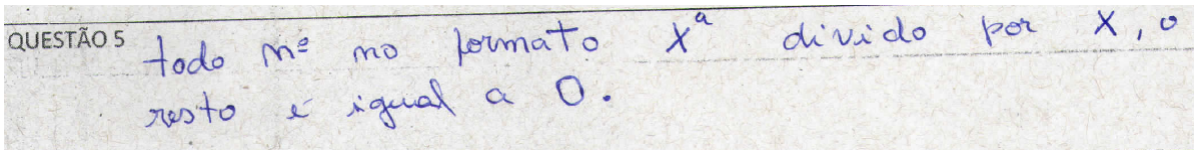
Tabela 20 – Questão 5T2

Alternativa	Percentual de alunos
a	100
b	0
c	0
d	0
e	0

O objetivo dessa questão era verificar se os educandos apropriaram-se de uma das aplicações do lema dos restos. Vemos que 100% obtiveram êxito nessa questão mostrando

um avanço considerável de conhecimento. Destacamos, na figura abaixo, uma resposta bastante interessante de um dos alunos avaliados.

Figura 25 – Resposta de um aluno - 4



Nessa questão, o aluno generaliza e, a partir dessa generalização, observa que, o resto será portanto igual a 1. É claro que o rigor matemático não foi respeitado nesse caso, visto que o aluno necessitava considerar que $x \in \mathbb{Z}$, $a \geq 1$ e $x \neq 0$. No entanto, já se observa uma certa desenvoltura para um aluno do ensino médio tentar fazer generalizações e que se configura um fato importante a se considerar.

Questão 6

O resto da divisão de $31^{99} + 61^{100}$ por 3 é:

(a) 0 (b) 1 (c) 2 (d) 3 (e)4

Alternativa correta: C

A **Tabela 21** mostra o percentual de alunos que assinalaram cada alternativa da questão 6.

Tabela 21 – Questão 6T2

Alternativa	Percentual de alunos
a	5,5
b	11,1
c	77,7
d	5,5
e	0

Para resolver essa questão, bastava utilizar o Teorema de Euler ou o Lema dos Resto. Analisando a **Tabela 21** acima, observamos que 77,7% dos discentes obtiveram sucesso na resolução dessa questão, mostrando assim o avanço significativo.

Questão 7

Para que o número $65786b8138a2$ seja divisível por 9, assinale a alternativa que possui um par de valores que a e b, respectivamente, podem assumir.

(a) $(3, 6)$ (b) $(1, 4)$ (c) $(3, 7)$ (d) $(4, 2)$ (e)$(1, 5)$

Alternativa correta: A

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 7.

Tabela 22 – Questão 7T2

Alternativa	Percentual de alunos
a	72,2
b	11,1
c	5,5
d	0
e	11,1

Com essa questão, desejava-se verificar se os alunos compreenderam os critérios de divisibilidade que foram trabalhados no curso. Com base na **Tabela 22** observa-se que os alunos se apropriaram dos conteúdos exigidos na questão, já que a grande maioria a resolveram com sucesso (72,2%). Em comparação com o teste 1, verifica-se um avanço de 66,6%.

Questão 8

Se o resto da divisão de um inteiro n por 12 é 7, qual é o resto da divisão de $2n$ por 12?

(a) 1 (b) 2 (c) 3 (d) 4 (e)5

Alternativa correta: B

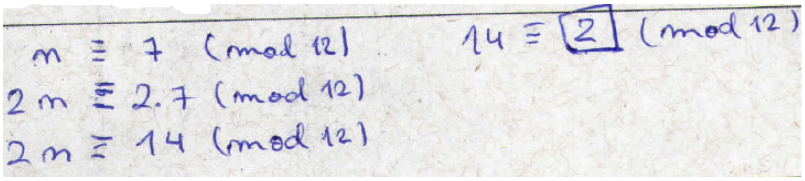
A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 8.

Tabela 23 – Questão 8T2

Alternativa	Percentual de alunos
a	11,1
b	66,6
c	16,7
d	5,5
e	0

De posse do Lema dos Restos, facilmente essa questão seria resolvida. Através dessa questão, o objetivo era analisar se esse conteúdo foi bem assimilado pelos alunos o que, de fato, ocorreu pois, ao analisarmos a **Tabela 23**, vemos que 66,7% dos alunos acertaram essa questão. Na verdade, outra forma de resolver essa questão era utilizando o conhecimento de congruência modular. A figura a seguir, mostra a estratégia utilizada por um dos alunos avaliados.

Figura 26 – Resposta de um aluno - 6



Nessa resolução apresentada pelo aluno, vemos um grande avanço em termos da utilização da linguagem da Congruência Modular bem como as suas propriedades.

Questão 9

(CMR - RECIFE) Sejam p_1, p_2 e p_3 números primos distintos que dividem n e $100n^3 + 8n^2 + 5n + 105$. Então, o valor de $p_1 + p_2 + p_3$ é

(a) 5 (b) 11 (c) 13 (d) 15 (e)17

Alternativa correta: D

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 9.

Tabela 24 – Questão 9T2

Alternativa	Percentual de alunos
a	5,5
b	11,1
c	0
d	77,8
e	5,5

Para resolver essa questão, o aluno teria que perceber que, como os primos p_1, p_2 e p_3 são fatores de n, também serão fatores de n^3, n^2 e n. Portanto, para descobrir os valores de p_1, p_2 e p_3, bastava decompor em fatores primos o número 105. De acordo com a **Tabela 24**, verifica-se que 77,8% dos alunos obtiveram sucesso nessa questão.

Questão 10

O menor natural n tal que $2^n - 1$ seja divisível por 7 é

(a) 1 (b) 2 (c) 3 (d) 4 (e) 5

Alternativa correta: C

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 10.

Tabela 25 – Questão 10T2

Alternativa	Percentual de alunos
a	5,5
b	0
c	88,9
d	5,5
e	0

Para resolver eficientemente essa questão, uma possível estratégia era analisar o conjunto dos divisores de 7. De acordo com a **Tabela 25**, vemos que 88,9% dos discentes obtiveram êxito nessa questão.

Questão 11

Pedro comprou um caderno com 96 folhas e numerou-as de 1 a 192. Vitor arrancou 25 folhas do caderno de Pedro e somou os 50 números que encontrou escritos nas folhas. Esta soma poderia ser igual a 1990?

(a) SIM (b) NÃO

Alternativa correta: B

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 11.

Tabela 26 – Questão 11T2

Alternativa	Percentual de alunos
a	27,8
b	72,2

Essa questão tinha o objetivo de verificar se os participantes do curso compreenderam bem o conceito de paridade e suas aplicações em situações do cotidiano. Vemos que 72,2% dos participantes do curso obtiveram êxito e, comparando com a análise da questão 12 do Teste 1, vemos também um avanço de 16,7%.

Questão 12

(UNICAMP-1993) De quantas maneiras podem ser escolhidos três números distintos, de 1 a 30, de modo que a soma dos três seja par?

(a) 2015 (b) 2020 (c) 2025 (d) 2030 (e)2035

Alternativa correta: D

A tabela abaixo mostra o percentual de alunos que assinalaram cada alternativa da questão 12.

Tabela 27 – Questão 12T2

Alternativa	Percentual de alunos
a	16,7
b	5,5
c	11,1
d	66,7
e	0

Assim como na questão 11, essa questão também envolvia o conceito de Paridade de Inteiros. No entanto, além da ideia de paridade, também seria necessário o conhecimento de técnicas de contagem, porém esse assunto já tinha sido estudado recentemente pelos alunos e os mesmos também tinham visto no curso resoluções desse modelo de questão e compreedido muito bem. Vemos que 66,7% conseguirem acertar essa qusetão. Talvez os demais não obtiveram sucesso pelo fato de não ter compreendido o fato de ter de utilizar as técnicas de contagem.

Questão 13

Se o resto da divisão de a e b por 6 é 3 e 2, respectivamente, qual é o resto da divisão de $a^3 + b^5$ por 6?

(a) 1 (b) 2 (c) 3 (d) 4 (e) 5

Alternativa correta: E

A **Tabela 28** mostra o percentual de alunos que assinalaram cada alternativa da questão 13.

Tabela 28 – Questão 13T2

Alternativa	Percentual de alunos
a	5,5
b	11,1
c	5,5
d	0
e	77,8

É claro que para resolver essa questão seria bastante aplicar o Lema dos Restos. Vemos que os alunos compreenderam bem esse conteúdo pois, conforme a **Tabela 28** 77,8% conseguiram acertar essa questão.

Questão 14

Um marceneiro deseja cortar uma placa retangular de madeira de medidas 256 cm por 96 cm em quadrados iguais de maior lado possível, de forma que não haja desperdício (sobras) de madeira. Qual deve ser, em cm, a medida do lado de cada quadrado obtido?

(a) 15 (b) 18 (c) 20 (d) 24 (e)32

Alternativa correta: E

A tabela abaixo mostra o percentual de alunos (de um total de 29 participantes) que assinalaram cada alternativa da questão 14.

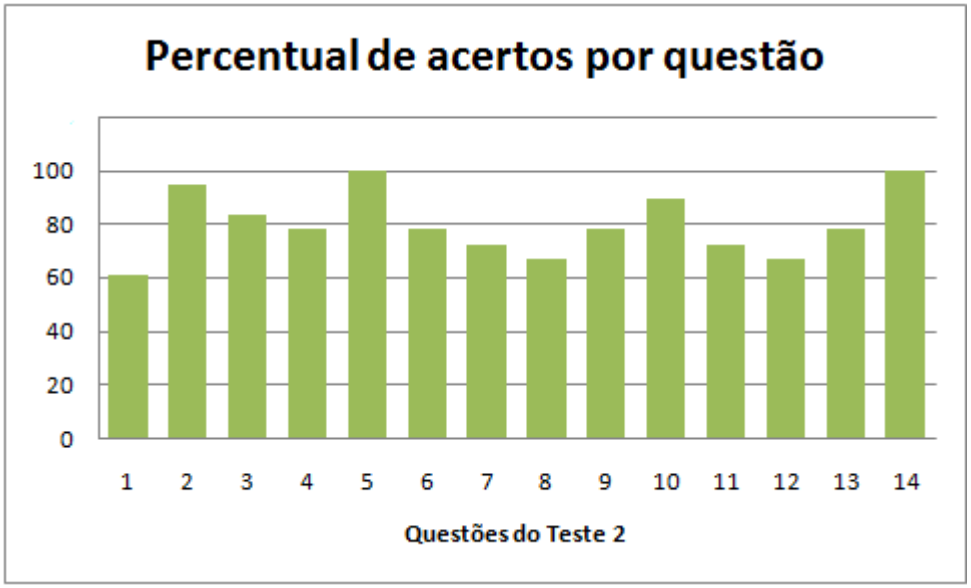
Tabela 29 – Questão 14T2

Alternativa	Percentual de alunos
a	0
b	0
c	0
d	0
e	100

Essa questão é uma aplicação clara do conceito de MDC. Através dos resultados expostos na **Tabela 29**, notamos todos os alunos fizeram essa questão de maneira correta.

3.2 Análise dos resultados

O gráfico abaixo é uma análise do percentual de acertos por cada questão do Teste 2.



Analisando os resultados do Teste 2, observamos um avanço significativo dos educandos participantes do curso. O percentual médio de acertos neste último teste foi de 79,75%. As questões com maiores percentuais de acertos foram as questões 5 e 14 e a questão com menor percentual de acerto foi a questao 1 com um percentual de 61,1%. Apesar do curso ser realizado no segundo semestre, onde já se percebe um certo cansaço por parte dos alunos e apesar dos discentes já terem suas responsabilidades acadêmicas e terem que ficar na escola no horário do contra-turno, os resultados foram satisfatórios mostrando que é possível abordarmos os temas tratados no curso no currículo de matemática do ensino médio, visto que apesar da aritmética fazer parte do currículo obrigatório da educação básica, não é realizado um estudo mais aprofundado desse tema. Mais ainda, a aritmética modular não faz parte do currículo obrigatório o que ao nosso ver, é uma chance perdida de serem trabalhados temas interessantes para os alunos.

É importante ressaltar, no entanto, a importância de serem utilizadas estratégias didáticas que possam viabilizar a construção do conhecimento. É de extrema importância que, na prática do ensino de matemática, o professor esteja ciente que o uso de vídeos, jogos, textos matemáticos, etc. são úteis e, porque não dizer, necessários para o sucesso do processo ensino-aprendizagem. O ensino dos conceitos e temas abordados no curso são uma forma de cumprir o que orienta os PCN's de matemática do ensino médio em [4, p. 9]:

> A Matemática ciência, com seus processos de construção e validação de conceitos e argumentações e os procedimentos de generalizar, relacio-

> nar e concluir que lhe são característicos, permite estabelecer relações e interpretar fenômenos e informações. As formas de pensar dessa ciência possibilitam ir além da descrição da realidade e da elaboração de modelos.

Sendo assim, a inclusão de alguns conceitos da Teoria dos Números no ensino médio com uma abordagem mais aprofundada para alguns temas já vistos no Ensino Fundamental é uma forma de despertar o interesse do aluno pela aprendizagem da disciplina de matemática pelo caráter desafiante e curioso que tais temas possuem.

Acreditamos também que o material pedagógico desenvolvido pode servir de apoio para os docentes de matemática que atuam especialmente no ensino médio. Obviamente, o material pedagógico aqui apresentado pode ser aperfeiçoado, bem como os jogos, vídeos e textos utilizados nas aulas propiciando, portanto, um aperfeiçoamento desse trabalho.

3.3 Análise comparativa do percentual médio de acertos por conteúdo

Logo abaixo, segue a **Tabela 30** que mostra a comparação do desempenho dos estudantes participantes do curso nos "Teste 1" e "Teste 2" em relação aos conteúdos abordados nesses respectivos testes.

Como pode ser observado na tabela, houve avanços significativos em relação a todos os tópicos abordados nas provas. Alguns desses avanços já eram esperados, como por exemplo os tópicos de congruências, Teorema de Euler e Fermat, Lema dos restos e Equações Diofantinas. Ao dizer que "alguns desses avanços já eram esperados" não estamos de forma alguma sendo arrogantes, mas simplesmente entendemos que essa parte tem sido negligenciada ao longo dos anos como parte do conteúdo programático do ensino básico. Também entendemos que essa situação deve ser mudada pois é justamente nesses tópicos que encontramos aplicações para temas como divisibilidade, algoritmo da divisão, números primos, MMC e MDC.

Tabela 30 – Comparação entre percentual médio de acertos

Conhecimento exigido	Teste 1 (T1)	Percentual médio de T1	Teste 2 (T2)	Percentual médio de T2
Divisibilidade	Q2-38,9% Q7-5,50% Q9-11,10%	18,5%	Q7-72,2%	72,2%
Algoritmo da Divisão	Q4-94,4% Q8-22,2% Q11-44,4%	53,7%	Q2-94,4%	94,4%
Paridade de Inteiros	Q12-55,5%	55,5%	Q11-72,2% Q12-66,6%	69,4%
Números Primos	Q10-5,5%	5,5%	Q4-77,8% Q9-77,8%	77,8%
Máximo Divisor Comum	Q14-33,4%	33,4%	Q14-100%	100%
Equações Diofantinas	Q3-77,7% Q6-66,7%	72,2%	Q3-83,3%	83,3%
Congruências, Teoremas de Euler e Fermat	Q1-16,7%	16,7%	Q1-61,1% Q6-77,7% Q10-88,9%	75,9%
Lema dos Restos	Q5-55,6% Q13-77,8%	66,7%	Q5-100,0% Q8-66,6% Q13-77,8%	81,4%

3.4 Análise comparativa dos resultados por nota

A **Tabela 31** retrata as notas dos alunos no "Teste 1" e no "Teste 2". Através dessa tabela, é possível detectar os avanços obtidos pelos alunos após o curso ofertado.

Tabela 31 – Comparação entre notas

Aluno(a)	Nota no Teste 1 (N_1)	Nota no Teste 2 (N_2)	$N_2 - N_1$	Percentual de avanço
A_1	7,8	10,0	2,2	28,2%
A_2	3,5	7,9	4,4	125,7%
A_3	4,2	7,9	3,7	88,1%
A_4	6,4	7,9	1,5	23,4%
A_5	5	9,3	4,3	86%
A_6	2,9	7,1	4,2	144,8%
A_7	3,5	6,4	2,9	82,8%
A_8	2,1	7,9	5,8	276,2%
A_9	7,8	9,3	1,5	19,2%
A_{10}	1,4	7,9	6,5	464,3%
A_{11}	5,0	7,9	2,9	58%
A_{12}	3,6	7,9	4,3	119,4%
A_{13}	2,8	7,9	5,1	182,1 %
A_{14}	5,0	7,1	2,1	42,5%
A_{15}	5,0	7,9	2,9	58%
A_{16}	3,6	8,6	5,0	138,9%
A_{17}	3,6	7,1	3,5	97,2%
A_{18}	4,3	7,9	3,6	83,7%

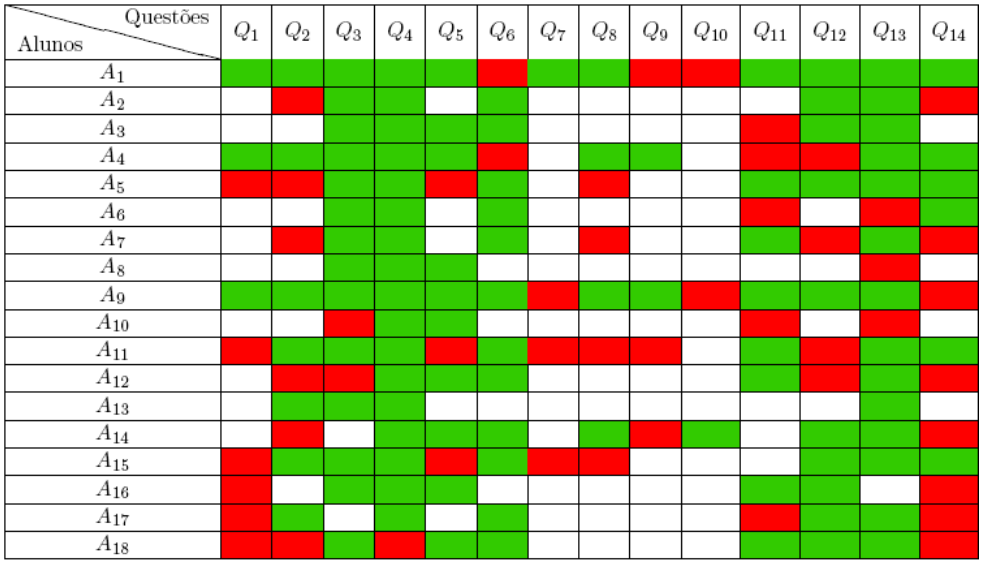
Na **Tabela 31** observamos que todos os alunos obtiveram melhores notas no segundo teste, sendo que a média da turma passou de 4,3 no primeiro teste para 8,0 no segundo. Além disso, observamos que exceto pelo discente A_7, todos obtiveram um nota acima de 7,0 no segundo teste, ao contrário do primeiro teste em que apenas 2 atingiram esse rendimento.

Não podemos deixar de citar os alunos A_8 e A_{10} que tiveram um superação muito acima do esperado e atribuimos isso principalmente pela assiduidade, comprometimento e participação nos jogos e atividades que desenvolvemos ao longo do curso.

3.5 Análise comparativa do desempenhos nos Teste 1 e Teste 2

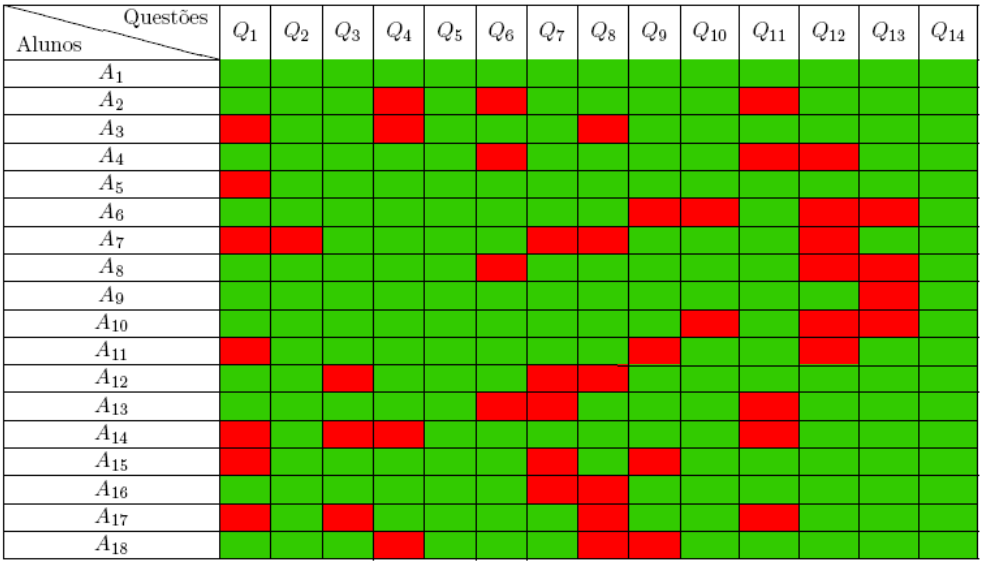
As tabelas a seguir demonstram o desempenho dos discentes participantes do curso nos "Teste 1" e "Teste 2". As células de cor verde, vermelho e em branco representam questões cujos discentes acertaram, erraram e não responderam, respectivamente.

Figura 27 – Desempenho no Teste 1



Observando a **Figura 16**, notamos que as Q_1, Q_7, Q_8, Q_9 e Q_{10} foram as que mais os alunos deixaram em branco. Acreditamos que isso se deve ao fato de terem sido modelos de questões que não são muito trabalhadas no ensino básico.

Figura 28 – Desempenho no Teste 2



Observando a **Figura 17**, é nítida a verificação do avanço dos alunos em vários aspectos, mas destacamos o fato dos alunos sentirem-se mais confiantes em responder as questões não deixando nenhuma em branco.

4 Considerações Finais

O desejo de desenvolver esse projeto surgiu quando estávamos cursando o mestrado PROFMAT e nos deparamos com a disciplina MA 14 - ARITMÉTICA. Nessa disciplina, tivemos experiências bastante interessantes com os desafios inerentes ao tema e entendemos que muitos desses desafios poderiam ser trabalhados no ensino médio e que, através desses desafios, as aulas poderiam ser mais interessantes e, consequentemente, poderíamos motivar os alunos para gostarem das aulas de matemática. A partir daí, desenvolvemos o projeto obtendo resultados satisfatórios conforme análise dos resultados apresentados. Sendo assim, esperamos com esse trabalho fomentar mais ainda o debate da reformulação do currículo de matemática na educação básica. Entendemos que trabalhar estes temas utilizando jogos, vídeos e desafios possibilita um melhor aproveitamento da aprendizagem por parte dos alunos. Na verdade, é fundamental que os professores de matemática na sua prática docente busquem sempre variados meios para que os alunos consigam êxito no processo de construção da aprendizagem e que, assim, consigamos melhores resultados no que tange à aprendizagem dos alunos. Enfim, a proposta desse trabalho vem em conformidade com o objetivo do PROFMAT que é o aprimoramento da formação profissional de professores da educação básica para o ensino de matemática. Além disso, segundo as normas que regem esse mestrado, o trabalho de conclusão final do PROFMAT deve versar sobre temas específicos pertinentes ao currículo de matemática da educação básica com impacto em sala de aula o que, no nosso entendimento, foi atingido na realização desse trabalho.

Referências Bibliográficas

[1] Bispo, Dinguiston dos Santos. **Equações Diofantinas Lineares e suas Aplicações**.2013.76 f. Monografia (Licenciatura em Matemática). Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista.

[2] Boyer, Carl B. **História da Matemática**. 3ª ed. Rio de Janeiro: SBM, 2011.

[3] Bracher, Daniele; Burket, Rogério S.; Gehling, Carla G. **IV EIEMAR Escola de Inverno de Educação Matemática**. Universidade Federal de Pelotas - UFPel. Disponível em `http://w3.ufsm.br/ceem/eiemat/Anais/arquivos/ed_4/RE/RE_Bracher_Daniele.pdf`. Acesso em 12/09/2016.

[4] Brasil. Ministério da Educação. Secretaria de Educação Básica. **Parâmetros Curriculares Nacionais(PCN+): ciências da natureza e suas tecnologias**. Brasília: MEC, 2002.

[5] Costa, Eduardo S. **Equações Diofantinas Lineares e o Professor do Ensino Médio**. 2007. 119f. Dissertação. Mestrado Acadêmico em Educação Matemática. Pontifícia Universidade Católica de São Paulo, São Paulo.

[6] Coutinho, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA,2014.

[7] Dias, Cristina Helena Bovo Batista. **Números Primos e Divisibilidade: Estudo de Propriedades**. 2013.49f. Dissertação (Mestrado Profissinal em Matemática). Universidade Estadual Paulista, São Paulo.

[8] Fomim, Dmitri. **Círculos Matemáticos.** Rio de Janeiro: IMPA, 2012.

[9] Fonseca, Rubens. **Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.

[10] Hefez, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.

[11] Maurício, Eufélix Monteiro. **Uma proposta de Sequência Didática para o Ensino de MDC e MMC na Educação Básica**.2014.46 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Espírito Santo, Vitória.

[12] Morais Filho, Daniel Cordeiro de. **Manual de redação matemática**. Rio de Janeiro: SBM, 2014.

[13] Moreira, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números.** Rio de Janeiro: SBM, 2012.

[14] Moreira, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª**. 1ª ed. Rio de Janeiro: SBM, 2003.

[15] Oliveira, Krerley Irraciel Martins. **Iniciação à Matemática: um curso com problemas e soluções**. 2ª ed. Rio de Janeiro: SBM, 2010.

[16] Oliveira, Maycon Costa de.**Aritmética: Criptografia e outras aplicações de Congruências**.2013.74 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Mato Grosso do Sul, Campo Grande.

[17] Resende, M. R. **Re-significando a disciplina de Teoria dos Números na formação do professor de Matemática na Licenciatura**. 2007. 281f. (Doutorado em Educação Matemática). Programa de Pós-Graduação em Educação Matemática, Pontifícia Universidade Católica, São Paulo.

[18] Sampaio, João C. V. **Mágica com números**. Revista do Professor de Matemática - RPM, Edição Especial, SBM, São Paulo, 2009.

[19] Santos, Rafael Prado. **Uma Proposta de Ensino de Equações Diofantinas Lineares no Ensino Básico Utilizando a Metodologia de Resolução de Problemas**. 2014.78f. Trabalho de Conclusão de Curso Superior em Licenciaturra Plena em Matemática. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), São Paulo.

[20] Tao, Terence. **Como resolver problemas matemáticos - Uma perspectiva pessoal**. Rio de Janeiro: SBM, 2013.

[21] Zeni, José Ricardo de Rezende. **Três Jogos para o Ensino e Aprendizagem de Números e Operações no Ensino Fundamental** . Universidade Estadual Paulista (UNESP). Disponível em:`http://www.feg.unesp.br/jrzeni/pesquisa/2007/3Jogos/3Jogos-Zeni.pdf`. Acesso em 12/09/2016.

ANEXO A – Materiais utilizados nas aulas

A.1 Jogo do Resto

Este jogo foi utilizado na aula sobre o Algoritmo da Divisão.

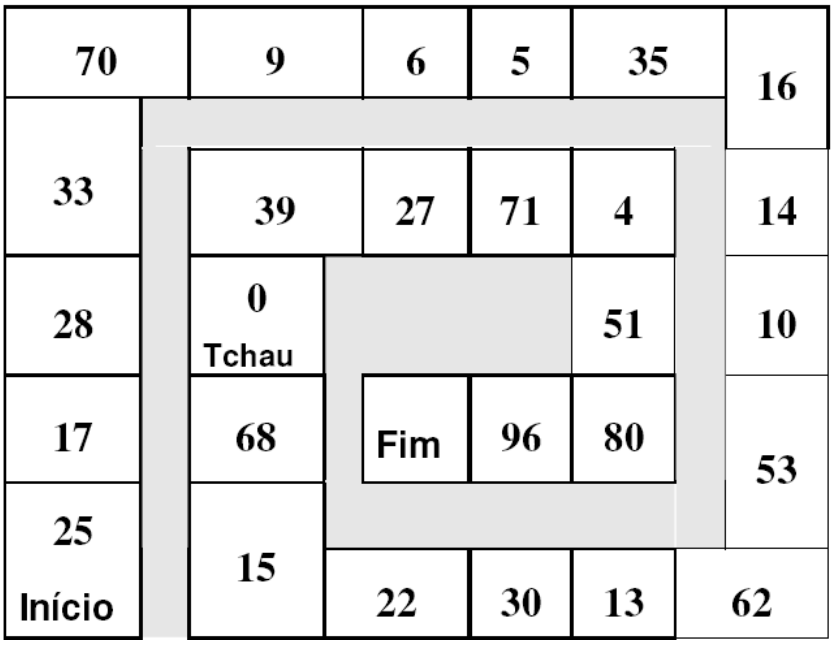
Organização da sala: dividir a sala em duplas.

Material necessário: um tabuleiro (ver figura 18) e um dado para cada dupla.

Conteúdo abordado: Algoritmo da Divisão.

Como jogar: cada dupla sorteia uma ordem para os jogadores. Todos os jogadores iniciam na primeira casa, que possui o número 25. Em cada rodada, na sua vez, um jogador lança um dado: o número de casas que o jogador deve avançar é igual ao resto da divisão do número da casa em que se encontra (dividendo) pelo número que sai no dado (divisor). Ganha o jogo quem atingir primeiro a casa "Fim".

Figura 29 – Jogo do Resto



Fonte: Adaptado de ZENI, José Ricardo de Rezende

Metodologia: pedir para os alunos registrarem os cálculos efetuados. Após o jogo, pode-se introduzir as questões abaixo. Para respondê-las, os alunos deverão analisar a divisão pelos números de 1 a 6.

1. No começo do jogo, quais os resultados do dado que não permitem ao jogador

avançar?

2. Qual é o maior número de casas que um jogador pode andar?
3. Por que na casa "0" está escrito a palavra "Tchau"?
4. Estando em uma casa qualquer, quais os resultados no dado que não permitem ao jogador avançar?

A.2 Bingo dos Múltiplos

Este jogo foi utilizado na aula sobre Números Primos.

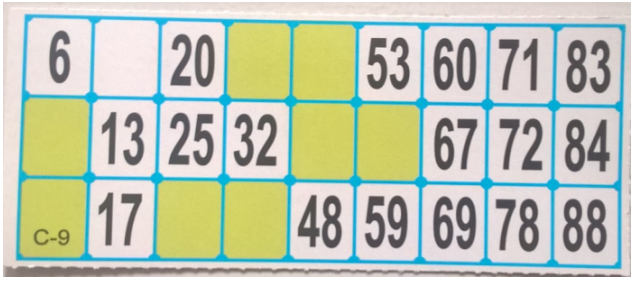
Organização da sala: da forma tradicional, ou seja, cada aluno em sua cadeira.

Material necessário: um jogo de bingo e grãos de feijão ou milho para marcação das cartelas.

Conteúdo abordado: Números Primos, Múltiplos e Divisores.

Como jogar: cada aluno receberá uma cartela, que, no nosso caso, continha 18 números aleatórios entre 2 e 90 e alguns grãos de feijão ou milho. As cartelas contêm números diferentes de forma que nenhuma cartela era exatamente igual a outra. Dentro do globo, estarão apenas números primos de 2 até 90 e quando um desses primos for sorteado, os alunos marcam os múltiplos desse primo que estão na cartela. Vence o aluno que conseguir marcar todos os números de sua cartela.

Figura 30 – Cartela do Bingo dos Múltiplos



Fonte: Foto tirada pelo autor

A.3 Texto: Mágica com números

Esse texto contém o desafio chamado de "mágica dos números" que seria utilizado na aula cujo tema foi Paridade de Inteiros. Tal desafio é, na nossa concepção, uma excelente forma de trabalhar o conceito de Paridade de Inteiros e sistema binário.

Truques de adivinhações aritméticas têm sido apresentados a pessoas e alunos de vários níveis de escolaridade e sempre causam surpresa e fazem muito sucesso. Vamos apresentar o truque da **adivinhação egípcia** com a subseqüente exploração das propriedades aritméticas subjacentes a ele.

Nesse truque o apresentador pede a um espectador que pense em um número de 10 a 100. O apresentador segue então os seguintes passos:

1. Pergunta ao espectador se o número é par ou ímpar. Ouvida a resposta, se for par, pede ao espectador que divida o número por 2. Se for ímpar, pede a ele que subtraia 1 e que então divida o resultado por dois.

2. Pergunta se o resultado obtido é par ou ímpar e, ouvida a resposta, pede ao espectador para repetir o procedimento descrito no item 1.

3. O procedimento continua com cada novo resultado até o resultado (quociente de uma divisão por 2) tornar-se igual a 1, quando então os cálculos do espectador terminarão.

Quando o apresentador é informado de que o resultado é igual a 1, ele revela imediatamente ao espectador o número pensado por ele.

Como funciona o truque da advinhação egípcia

Suponhamos que o número pensado pelo espectador seja 52. Nas sucessivas etapas, ele efetuará as contas da coluna abaixo à esquerda, enquanto simultaneamente o apresentador irá fazendo, secretamente, as anotações da coluna à direita.

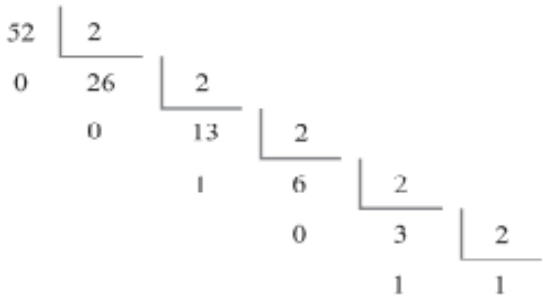
Aluno	**Professor**
52 (número pensado)	1
26	2
13	4 ✓
6	8
3	16 ✓
1	32 ✓

Para cada número ímpar informado pelo espectador, o apresentador anota "✓" . Nos sucessivos estágios da brincadeira, o apresentador marca as potências de 2, iniciando em $2^0 = 1$. Em seguida, o apresentador soma as potências de 2 correspondentes às marcas ✓,

$$4 + 16 + 32 = 52,$$

e resgata o número que foi pensado pelo espectador!

O truque foi concebido observando o método das divisões sucessivas por 2, usado para representar um inteiro positivo no sistema binário, isto é, como soma de potências (distintas) de 2, a partir de sua representação no sistema decimal. Nesse método, tomando como exemplo o número 52, fazemos a seguinte "escada" de divisões sucessivas por 2, até atingirmos quociente igual a 1, quando o algoritmo termina. Lendo da direita para a esquerda os 0's e 1's, que são o último quociente e os restos das divisões, obtemos a representação do número 52 (aqui representado no sistema decimal) no sistema de numeração de base 2:



$52 = (110100)2 = 1 \times 2^5 + 1 \times 2^4 + +0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 = 2^2 + 2^4 + +2^5$.

Na sequência das divisões, um resto será 0 quando o dividendo for par, e 1 quando o dividendo for ímpar, daí a importância de tomar nota apenas das potências de 2 correspondentes aos restos ímpares.

O título *adivinhação egípcia* é inspirado nos algoritmos de multiplicação dos antigos egípcios, baseados na decomposição de inteiros positivos como somas de potências distintas de 2.

Adaptado do artigo "Mágicas com números"

João C. V. Sampaio, RPM 60.

A.4 Baralho do MDC

Este jogo foi utilizado na aula sobre MDC.

Organização da sala: dividir a sala em grupos de 4.

Material necessário: um baralho do MDC para cada grupo de 4 alunos.

Conteúdo abordado: MDC, Conjunto dos Divisores.

Como jogar:

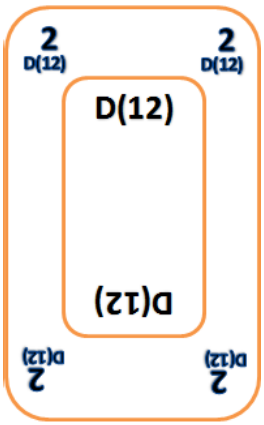
- As cartas com valores que representam MDC entre as probabilidades de formação de pares de conjuntos foram marcadas de forma diferente;
- Quando o grupo forma uma sequência de divisores completa ganha 200 pontos;
- Quando o grupo ao comparar 2 conjuntos de divisores, mesmo que estejam incompletos, mas que estejam sendo formados na mesa, identificar o MDC e colocar a carta de MDC nesse valor correto para os 2 números de conjunto de divisores em questão, ganhará mais 200 pontos;
- Se o grupo conseguir formar as duas sequências de divisores e ainda tiver a carta de MDC entre os dois ganha 500 pontos;
- Para iniciar o jogo, basta baixar à mesa uma sequência correta de 3 cartas de qualquer nipe;
- São 4 jogadores (como no jogo do buraco do baralho comum), 2 duplas que sentam cruzadas, ou seja, os jogadores da mesma dupla não sentam lado a lado, pois um completará o jogo do outro sem saber as cartas que o outro tem e por isso, devem sentar-se afastados;
- Cada jogador recebe 9 cartas e o que sobra forma o bolo da mesa;
- No final ganha quem acumular maior número de pontos.

Metodologia: a ideia é trabalhar, através desse jogo, o conceito de MDC, como formar a sequência correta de cada conjunto de divisores e observar que todo conjunto de divisores começa com 1 e termina no próprio número. Para isso, foram escolhidos 7 números e o conjunto dos seus divisores:

$D(10) = \{1, 2, 5, 10, \}$
$D(12) = \{1, 2, 3, 4, 6, 12\}$
$D(15) = \{1, 3, 5, 15\}$
$D(20) = \{1, 2, 4, 5, 10, 20\}$
$D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$
$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$
$D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

Cada conjunto de divisores é um "naipe" do baralho. Sendo assim, são 5 nipes, e no nosso caso, cada naipe tem uma quantidade diferente de cartas. Vejamos a seguir um exemplo de carta:

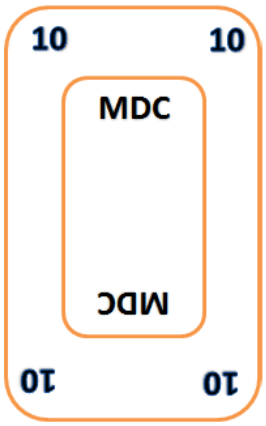
Figura 31 – Carta Baralho do MDC



Fonte: Criado pelo autor

A parte interna da carta identifica de qual naipe (conjunto de divisores) ela é e as pontas indicam um dos valores desse conjunto. Além disso, foram construídas cartas com o valor do MDC de cada dupla de números dentre os sete escolhidos formando, portanto, 66 cartas. Abaixo, segue um exemplo desse modelo de carta.

Figura 32 – Carta Baralho do MDC



Fonte: Criado pelo autor

Adaptado do blog `http://bisbilhotarte.blogspot.com.br/p/jogos.html`

A.5 Jogo da Escova Diofantina

Este jogo foi utilizado na aula sobre Equações Diofantinas.

Organização da sala: dividir a sala em grupos de 4.

Material necessário: um baralho comum no qual serão retirados as figuras (rei, dama e valete) dos quatro naipes e também os curingas para que se tenha um baralho com 40 cartas composto por quatro sequências de Ás a 10.

Como jogar: Após embaralhar as cartas, distribuir 3 para cada jogador. Abrir as próximas 4 cartas e colocá-las no centro da mesa mostrando os números. O monte restante é posto de lado. O objetivo é jogar uma carta de modo que a soma do seu valor com o valor de uma ou mais cartas da mesa dê 15, utilizando no máximo dois valores de carta diferentes. O jogador coloca à sua frente as cartas retiradas da mesa, assim como a carta de sua mão que permitiu a soma de 15, com a face voltada para baixo. Caso ele não consiga pegar nenhuma carta da mesa, deve simplesmente descartar na mesa uma das cartas de sua mão e o jogo prossegue. Se o jogador conseguir pegar todas as cartas restantes na mesa de uma única vez, o jogador fez uma escova diofantina. Quando os jogadores tiverem utilizado suas 3 cartas, uma nova mão de 3 cartas é distribuída, utilizando o monte que havia sido posto de lado. A partida prossegue da mesma maneira até que o monte de cartas termine. Aí é feita a contabilização dos pontos, considerando que cada combinação resultante em 15 vale um ponto e, cada escova diofantina, vale cinco pontos.

Fonte: TCC do curso Licenciatura em Matemática de Rafael Prado dos Santos

A.6 Apresentação de vídeo

Apresentação de vídeo, cujo link de acesso é `https://youtu.be/MNpgJmNKuUQ`. Tal vídeo é do programa Telecurso 2000 e foi utilizado na aula cujo tema foi Divisibilidade. Nesse vídeo é apresentado, de forma lúdica, o conteúdo "Múltiplos e divisores".

A.7 Apresentação de vídeo

Apresentação de um documentário da BBC (British Broadcasting Corporation), utilizado na aula cujo tema foi Números Primos, sobre a história dos Números Primos. Nesse documentário, cujo link de acesso é `https://youtu.be/eHp0cQy-2S4`, é mostrado a importância dos números primos ao longo da história e aplicações nos dias atuais. Na execução do vídeo durante a aula, o documentário foi exibido até o minuto 10.

A.8 Apresentação de vídeo

Exibição de um vídeo da Matemática Multimídia, que contém recursos educacionais multimídias desenvolvidos pela Unicamp (Universidade de Campinas). Tal vídeo, cujo link de acesso é `https://youtu.be/vj7DpfQ-pa0`, foi utilizado na aula cujo tema

foi Criptografia. Nesse vídeo, de uma maneira bastante lúdica e divertida, é introduzida a ideia de Criptografia.

ANEXO B – Teorema de Euler

O Teorema de Euler é um dos mais importantes na Teoria dos Números. Estudaremos nessa seção a demosntração desse belo teorema.

Antes de provrarmos, vamos lembrar que estudamos, ao longo do curso, o **Pequeno Teorema de Fermat** que afirma que sendo p primo, $a \in \mathbb{Z}$ com $(a, p) = 1$, tem-se que

$$a^{p-1} \equiv 1 \ (mod\, p)$$

Por exemplo, $4^{3-1} \equiv 1 \ (mod\, 3)$. No entanto, pelas condições expostas no teorema, não podemos generalizar para um inteiro qualquer, ou seja, por exemplo, notemos que $3^{4-1} \not\equiv 1$ $(mod\, 4)$. Através do Teorema de Euler, poderemos generalizar para todo inteiro.

Definição B.0.1. *Definimos como* ***sistema completo de resíduos módulo*** m *,* $m \in \mathbb{N}$*,* $m > 1$ *todo conjunto de números inteiros* $\{r_1, r_2, ..., r_s\}$ *que satisfazem*

i) $r_i \not\equiv r_j \ (mod\, m)$ *para todos* $i, j \in \{1, 2, ..., s\}$*, tais que* $i \neq j$*.*

ii) Para todo $n \in \mathbb{Z}$ *existe* $i \in \{1, 2, ..., s\}$ *tal que* $n \equiv r_1 \ (mod\, m)$*.*

Por exemplo, seja $m = 12$, os conjuntos

- $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ e
- $B = \{12, 15, 14, 13, 16, 17, 18, 19, 20, 21, 22, 23\}$

são exemplos de um sistema completo de resíduos módulo 12.

Definição B.0.2. *Chamamos de* ***sistema reduzido de resíduos módulo*** m*,* $m \in \mathbb{N}$*,* $m > 1$*, a todo conjunto de inteiros* $\{r_1, r_2, ..., r_s\}$*, tais que*

i) $(r_i, m) = 1$*, para todo* $i \in \{1, ..., s\}$*.*

ii) $r_i \not\equiv r_j \ (mod\, m)$ *se* $i, j \in \{1, 2, ..., s\}$ *e* $i \neq j$*.*

iii) Para cada $n \in \mathbb{Z}$*, com* $(n, m) = 1$*, existe* $i \in \{1, 2, ..., s\}$ *tal que* $n \equiv r_i \, mod\, m$*.*

Por exemplo, seja $m = 15$, um sistema reduzido de resíduos, módulo m, seria o conjunto $C = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

A proposição a seguir será fundamental para a demonstração do Teorema de Euler.

Proposição B.0.1. *Sejam $a, b, c \in \mathbb{Z}$. Se $(a, b) = 1$ e $(c, b) = 1$, então $(ac, b) = 1$.*

Demonstração . *Suponhamos, por absurdo, que $(ac, b) = d$, com $d \neq 1$. Daí, podemos decompor d em fatores primos e escrever $d = p_1 \cdot p_2 \cdots p_\alpha$. Considere o primo p_i, com $i \in \{1, 2, ..., \alpha\}$. Como $p_i \mid d$, temos que $p_i \mid b$ e $p_i \mid ac$. Logo, como p_i é primo, teremos que $p_i \mid a$ ou $p_i \mid c$. Mas*

- *se $p_i \mid a$, teremos um absurdo pois p_i será um divisor comum de a e b e, por hipótese, $(a, b) = 1$.*
- *se $p_i \mid c$, analogamente, teremos também um absurdo pois $(c, b) = 1$.*

Portanto, $(ac, b) = 1$.

■

Lema B.0.1. *Sejam $a \in \mathbb{Z}$, $m \in \mathbb{N}$ com $m > 1$ e $(a, m) = 1$. Se $\{r_1, r_2, ..., r_s\}$ é um sistema completo de resíduos módulo m, então*

$$\{ar_1, ar_2, ..., ar_s\}$$

também é um sistema completo de resíduos módulo m.

Demonstração . *Com efeito, como $(a, m) = 1$, temos para $i, j \in \{1, 2, ..., s\}$, pela **propriedade 8**, estudada no tema **Congruência**, que*

$$ar_i \equiv ar_j \pmod{m} \Longrightarrow r_i \equiv r_j \pmod{m} \Longrightarrow i = j,$$

pois $\{r_1, r_2, ..., r_s\}$ forma, por hipótese, um sistema completo de resíduos.

Isso mostra que $\{ar_1, ar_2, ..., ar_s\}$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m.

■

Proposição B.0.2. *Sejam $a \in \mathbb{Z}$, $m \in \mathbb{N}$ com $m > 1$ e $(a, m) = 1$. Se $\{r_1, r_2, ..., r_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então*

$$\{ar_1, ar_2, ..., ar_{\varphi(m)}\}$$

também um sistema reduzido de resíduos módulo m.

Demonstração . *Seja $\{b_1, b_2, ..., b_s\}$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos $\{r_1, r_2, ..., r_{\varphi(m)}\}$. Ora, como $(r_i, m) = 1$, $i \in \{1, 2, ..., \varphi(m)\}$ e $(a, m) = 1$, pela **proposição B.0.1**, temos que $(ar_i, m) = 1$, como queríamos demonstrar.*

■

Proposição B.0.3. *Dado $m \in \mathbb{N}$, $m > 1$ todos os sistemas reduzidos de resíduos modulo m tem o mesmo número de elementos.*

Demonstração . *Sejam $A = \{r_1, r_2, ..., r_k\}$ e $B = \{s_1, s_2, ..., s_t\}$ dois sistemas reduzidos de resíduos módulo m. Queremos mostrar que $k = t$. Com efeito, seja $r_i \in \{r_1, r_2, ..., r_k\}$, $i \in \{1, 2, ..., k\}$. Como $(r_i, m) = 1$, pelo ítem iii da* ***Definição B.0.2*** *existe um, e apenas um elemento $s_j \in \{s_1, s_2, ..., s_t\}$, $j \in \{1, 2, ..., t\}$ tal que $r_i \equiv s_j \, (mod\, m)$. Portanto, isso define uma função f de A em B. Vamos mostrar agora que f é injetiva. De fato, é claro que sendo $l \in \{1, 2, ..., k\}$, temos que $r_i \equiv s_j \, (mod\, m)$ e $r_l \equiv s_j \, (mod\, m) \Rightarrow i = l$, pois do contrário teríamos um absurdo pelo ítem ii da* ***Definição B.0.2****, sendo assim $k \leq t$. Analogamente, trocando os papéis dos sistemas, como o conjunto B também é um sistema reduzido de resíduos, teremos definida uma função g, de B em A também injetiva de forma que teremos $t \leq k$. Portanto, só nos resta concluir que $k = t$, seguindo o resultado.*

■

Definição B.0.3. *Definimos a função fi de Euler , por*

$$\varphi : \mathbb{N}^* \to \mathbb{N},$$

em que $\varphi(1) = 1$ e, para $m > 1$, $\varphi(m)$ é o número de elementos de um sistema reduzido de resíduos módulo m, isto é, corresponde à quantidade de números inteiros entre 0 e $m - 1$ que são co-primos com m.

Por exemplo, $\varphi(12) = 4$, $\varphi(6) = 2$, $\varphi(10) = 4$. É claro que, se p é primo, $\varphi(p) = p - 1$.

Teorema 2. ***[De Euler]*** *Sejam $a \in \mathbb{Z}$, $m \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$. Então*

$$a^{\varphi(m)} \equiv 1 \, (mod\, m).$$

Demonstração . *Seja $r_1, r_2, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Como $(a, m) = 1$, temos, pela* ***proposição B.0.2****, que o conjunto $ar_1, ar_2, ..., ar_{\varphi(m)}$ é também um sistema reduzido de resíduos módulo m. Sendo assim,*

$$a^{\varphi(m)} r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \, (mod\, m)$$

Mas, como $(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$, concluí-se , pela ***propriedade 8****, estudada no tema* ***Congruência****, que*

$$a^{\varphi(m)} \equiv 1 \, (mod\, m)$$

■