Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Aritmética Modular: uma Aplicação no Ensino Fundamental

Rodolfo Cavalcante Pinheiro

Goiânia

2018

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[x] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: Rodolfo Cavalcante Pinheiro

Título do trabalho: Aritmética modular: uma aplicação no Ensino Fundamental

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Rodolfo C. Pinheiro

Assinatura do(a) autor(a)[2]

Ciente e de acordo:

Assinatura do(a) orientador(a)[2]

Data: 12 / 06 / 2018

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[2] A assinatura deve ser escaneada.

Rodolfo Cavalcante Pinheiro

Aritmética Modular: uma Aplicação no Ensino Fundamental

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientador: Dr. Paulo Henrique de Azevedo Rodrigues

Goiânia

2018

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Cavalcante Pinheiro, Rodolfo
Aritmética modular: uma aplicação no Ensino Fundamental [manuscrito] / Rodolfo Cavalcante Pinheiro. - 2018.
LXXX, 80 f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2018.
Bibliografia. Anexos.
Inclui gráfico, tabelas, lista de figuras, lista de tabelas.

1. Ensino Fundamental. 2. Aritmética. 3. Criptografia. I. de Azevedo Rodrigues, Paulo Henrique , orient. II. Título.

CDU 51

Universidade Federal de Goiás - UFG
Instituto de Matemática e Estatística - IME
Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG
Campus Samambaia – Caixa Postal 131 – CEP: 74.001-970 – Goiânia-GO.
Fones: (62) 3521-1208 e 3521-1137 www.ime.ufg.br

Ata da reunião da banca examinadora da defesa de Trabalho de Conclusão de Curso do aluno Rodolfo Cavalcante Pinheiro – Aos quinze dias do mês de maio do ano de dois mil e dezoito, às 16:00 horas, reuniram-se os componentes da Banca Examinadora: Prof. Dr. Paulo Henrique de Azevedo Rodrigues – Orientador, Prof. Dr. Ricardo Nunes de Oliveira e a Profª. Drª. Silvia Cristina Belo e Silva, para, sob a presidência do primeiro, e em sessão pública realizada no auditório do IME, procederem a avaliação da defesa intitulada **"Aritmética Modular: uma Aplicação no Ensino Fundamental"**, em nível de mestrado, área de concentração Matemática do Ensino Básico, de autoria de Rodolfo Cavalcante Pinheiro, discente do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás. A sessão foi aberta pelo presidente da banca, Prof. Dr. Paulo Henrique de Azevedo Rodrigues, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida ao autor do TCC que, em 30 minutos, procedeu à apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se à avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1403/2016 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG, e procedidas as correções recomendadas, o Trabalho foi **APROVADO** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega, na secretaria do IME, da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 18:00 horas, a presidência da mesa encerrou a sessão e, para constar, eu, Sóstenes Soares Gomes, secretário do PROFMAT/UFG, lavrei a presente ata que, após lida e aprovada, segue assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Presidente – IME/UFG

Prof. Dr. Ricardo Nunes de Oliveira
Membro – IME/UFG

Silvia Cristina Belo e Silva

Profª. Drª. Silvia Cristina Belo e Silva
Membro – PUC/GO

Rodolfo Cavalcante Pinheiro graduou-se em Licenciatura Plena em Matemática pela Universidade Estadual de Goiás em 2008. Após concluir a graduação, atuou como professor de Matemática no Ensino Fundamental e Médio da rede privada do Estado de Goiás. Paralelamente à carreira de professor já em 2010 se especializou em Gestão bancária, finanças e controladoria pelo instituto de pós graduação IPOG e iniciou a carreira bancária até meados de 2015 quando decidiu seguir unicamente a carreira de professor. Trabalhando com jovens ambiciosos, sempre se incomodou com a repetição de conteúdos ministrados nas séries do Ensino Fundamental II.

Dedico este trabalho à Deus , à minha esposa e à minha família.

Agradecimentos

Agradeço à Deus por me dar a força necessária para completar e conquistar esse objetivo.

Agradeço à todos que puderam contribuir para que eu completasse esse sonho, principalmente minha esposa que sempre esteve ao meu lado nos momentos de dificuldades impedindo que eu desanimasse.

Agradeço também a todos meus amigos e parceiros de curso pelos dias de troca de conhecimento que fizeram com que eu me tornasse profissional melhor.

Agradeço ao meu orientador Dr. Paulo Henrique pelas orientações e direcionamentos para a conclusão deste material.

Resumo

Este trabalho apresenta uma proposta de se trabalhar com Aritmética Modular com os alunos do Ensino Fundamental II (6º, 7º, 8º e 9º anos) com o intuito de tornar o ensino de matemática mais aprofundado e de se desprender dos livros didáticos. Apresentamos uma sequência de conteúdos que se inicia nos números primos e compostos, discute-se os significados de múltiplos, divisores (e os restos das divisões) e as regras de divisibilidade. Para desenvolver o tema Aritmética Modular ainda exploramos as definições das Equações Diofantinas. Concluímos mostrando a aplicabilidade do tema com o estudo da Criptografia (cifra de César e método RSA). O trabalho ainda trás resultados da aplicação do projeto realizado com um grupo específico de alunos em uma escola da rede particular de ensino do estado de Goiás.

Palavras-chave Ensino Fundamental, Aritmética Modular, Criptografia.

Abstract

This paper presents a proposal to work with Modular Arithmetic with elementary students II (6th, 7th, 8th and 9th years) in order to make the teaching of mathematics more in depth and to get rid of textbooks. We present a sequence of contents that begins in the prime and compound numbers, discusses the meanings of multiples, divisors (and the remainders of divisions) and divisibility rules. To develop the Modular Arithmetic theme we are still exploring the definitions of Diophantine Equations. We conclude by showing the applicability of the theme to the study of Cryptography (Caesar cipher and RSA method). The work still brings results of the application of the project carried out with a specific group of students in a private school in the state of Goiás.

Keywords

Elementary Education, Modular Arithmetic, Cryptography.

Lista de Figuras

Sumário

1 Introdução

A matemática é uma das ciências que fornece instrumentos eficazes para compreender e atuar no mundo que nos cerca. No entanto trabalhar com esta disciplina , sobretudo no Ensino Fundamental, exige do professor uma mediação eficaz e uma didática capaz de atrair a atenção dos alunos, o que torna uma tarefa bem complexa. A heterogeneidade dos alunos em uma salade aula assusta e dificulta muito o trabalho feito pelas escolas e pelos professores. Geralmente, dentro de uma sala a aprendizagem de matemática é polarizada. De um lado aqueles com alto rendimento e no outro extremo aqueles com graves problemas relacionados à compreensão dos conteúdos matemáticos, ficando este último sendo o foco da escola.

A escola privada acaba preocupando-se e voltando a atenção aos alunos de baixo rendimento oferecendo aulas de plantão de dúvidas, seguidas recuperações bimestrais e atendimentos personalizados para tentar sanar tais dificuldades, o que na minha percepção acaba por negligenciar um cuidado com o potencial daqueles que poderiam desenvolver melhor as habilidades matemáticas. No contexto do ensino das escolas privadas, percebe-se que os alunos com baixo rendimento tendem a possuir maior risco de reprovação e se confirmada a reprovação, a mudança de escola é iminente. Portanto, a atenção da escola fica normalmente focada nesses alunos para tentar evitar prejuízo financeiro nos anos seguintes, e assim, por não ser um "problema", os alunos de alto rendimento acabam sendo excluídos. Como podemos perceber nas falas de Andreia e Soraia, Revista do Centro de Educação, a preocupação com esse nicho de alunos com alta perfomance deve ser constante, uma vez que tal exclusão pode causar "desânimo, tédio e frustração, pois o que o professor está ensinando o aluno com altas habilidades já sabe.". Elas ainda mencionam que estimular o talento humano deve ser um dos objetivos da escola, e citam Guenther (2000, p. 14) “desenvolver talentos, sob esse olhar, é ao mesmo tempo um investimento social e uma responsabilidade coletiva”.

Diagnosticar possíveis reclamações de tais alunos, é primeiramente uma responsabilidade do professor e em sequência da escola. Ambos devem estar sempre atentos às situações em que presenciarem frases do tipo: "Nossa professor, de novo esse conteúdo!", "já estudamos isso no ano passado", "porque não aprendemos isso antes?", "está muito fácil esse ano, igual ao ano passado"ou ainda quando presenciarem alunos que terminam muito rapidamente a atividade sem mostrar nenhum tipo de dificuldade, mesmo em se tratando de um tema novo. Uma vez diante de tal situação, cabe ao professor buscar formas de incentivar esses alunos seja através de desafios, listas

extras com exercícios mais difíceis, aulas para olimpíadas de matemática dentre outras opções.

Diante de tal percepção em algumas escolas privadas buscamos através de uma minunciosa pesquisa nos livros didáticos de matemática das séries finais do Ensino Fundamental I (5º ano) e Ensino Fundamental II (6º, 7º, 8º e 9º anos) mapear conteúdos que são repetidos e que por algum motivo não apresentam real avanço gradual e considerável de dificuldades no decorrer das séries. Devido a anos de experiência no ensino de matemática no ensino básico, sabíamos que encontraríamos vários conteúdos em tal situação. Alguns deles serão citados abaixo:

1. Múltiplos, divisores e regras de divisibilidade;
2. Geometria plana - estudo e classificações de ângulos e triângulos;
3. Geometria plana - áreas de figuras planas;
4. Operações numéricas e potenciação.

Analisando um dos tópicos acima, percebemos que desde as séries finais do Ensino Fundamental I e no decorrer das séries do Ensino Fundamental II o tópico de divisibilidade é apresentado aos alunos, iniciando no 5º ano e permanecendo na grade curricular até o 7º ano, sempre com foco nas mesmas regras de divisibilidade dos números $2, 3, 4, 5, 6, 8, 9, 10$, sem que a maioria dos livros abordarem regras diferentes como a regra de divisibilidade dos números 7 e 11 e outras regras de números compostos usuais como dos números 12 e 15. Mesmo fato ocorre com o ensino dos temas Máximo Divisor Comum (mdc) e Mínimo Múltiplo Comum (mmc) que são trabalhados de forma exaustiva deste o 5º ano inclusive com o uso do algoritmo de Euclides, método esse que é substituído pelo método das fatorações sucessivas, porém sem grandes avanços (aumento de dificuldades/nível de exercícios). Esse aprofundamento é feito apenas no Ensino Médio, com foco na resolução de questões de vestibulares.

Me deparando diariamente com as situações (frustantes) descritas acima e por trabalhar nas 4 séries do Ensino Fundamental II a quase 10 anos, senti a necessidade de desenvolver um projeto que buscasse responder às perguntas que me cercavam: Como não tornar o ensino de matemática cada vez mais superficial e repetitivo nas séries do Ensino Fundamental II? Como valorizar o aluno com bom desempenho escolar? Seria possível aprofundar os conteúdos, e quem sabe abordar conteúdos do Ensino médio já no Ensino Fundamental II?

Muito motivado pelas aulas de Aritmética no mestrado, selecionamos tal área do conhecimento matemático para executar um projeto de Aritmética Modular com os alunos com alto rendimento nas 4 séries citadas, mesmo porque durante a pesquisa bibliográfica nos deparamos com um vazio nesta área pois não encontramos material que mesclasse o ensino de Aritmética com Ensino Fundamental e a efetiva aplicação em sala de aula.

O trabalho é dividido em fundamentação teórica, definição de objetivos, metodologia, descrição de conteúdos, descrição do projeto e considerações finais com os resultados da aplicação do projeto.

2 Fundamentação Teórica

A Aritmética é uma área muito abrangente da matemática. Na base curricular do Ensino Fundamental, conhecemos os números naturais e suas operações, múltiplos, divisores, números primos, númreros compostos, regra de divisibilidade, máximo divisor comum e mínimo múltiplo comum. Porém a Aritmética é muito mais ampla. Existem alguns tópicos como Aritmética Modular e Congruência Modular, que englobam a parte mais complexa do estudo. Além de sua importância, o tema também serve como base para muitas áreas da Álgebra e de sua aplicabilidade. Como diz Ilydio;

> "É um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental, é gerador de excelentes oportunidades de contextualização no processo de ensino / aprendizagem de matemática."(Ilydio de Sá)

Grande parte dos materiais sobre o tema estão em livros, em textos científicos e materiais preparatórios para olimpíadas de matemática. Alguns livros são de Teoria dos Números como é o caso do livro do professor Valdir Vilmar da Silva (Números: Construções e Propriedades). Os artigos científicos tem como base a grande aplicabilidade do tema em diversas áreas, como códigos numéricos, registros (cpf, rg), calendários e criptografia. Vários destes materiais buscam desenvolver projetos para o Ensino Médio, sem ter como foco principal a aplicação. Diferentemente dos trabalhos pesquisados, nosso trabalho busca a aplicabilidade do tema no Ensino Fundamental II, verificando a origem do estudo nas séries finais do Ensino Fundamental I e aprofundando o conteúdo até o final do Ensino Fundamental II. Dentre os materiais olímpicos podemos citar o

livro "Divisibilidade e Números Inteiros - Introdução à Aritmética Modular "(Samuel Jurkiewicz) que serviu de base para a aplicação do projeto.

2.1 Definição de objetivos

Como objetivo central do trabalho buscamos aprofundar conteúdos tradicionais de matemática e assim atender às necessidades educativas específicas, até então pouco discutidas, direcionados para um grupo de alunos com alto rendimento. Para isso, discutimos a prática de ensino superficial de alguns temas centralizados na Aritmética, valorizamos e desafiamos os alunos com alto desempenho escolar, ministrando os conteúdos baseados sempre com exemplos numéricos e exercícios do Ensino Médio, olimpíadas e vestibulares.

2.2 Metodologia

Como se tratava de um projeto piloto na escola, usamos a metodologia da pesquisa-ação. Desta forma, o professor poderia ter maior efiência na aplicação do mesmo, uma vez que apesar de haver uma "negociação"entre os participantes (aluno x professor), haveria bastante liberdade para discussões em sala de aula, estando o professor apenas como mediador das ações. Como as ações do discente se tornariam mais flexíveis diante das situações enfrentadas no decorrer das aulas, o resultado seria melhor. Moreira e Rosa (Pesquisa em Ensino: métodos qualitativos e quantitativos, p.16) retratam o papel do professor na pesquisa ação citando Kemmis:

> "Na pesquisa-ação, os professores são incentivados a questionar suas próprias idéias e teorias educativas, suas próprias práticas e seus próprios contextos como objetos de análise e crítica."(Kemmis, 1988, p. 174)

Sabíamos da importância de se planejar bem antes de implementar o projeto, principalmente devido as particularidades dos alunos, com maior destaque ao fato de trabalhar com alunos das 4 séries do Ensino Fundamental II ao mesmo tempo. Então seguimos o ciclo básico da investigação ação citado por David Tripp em "Pesquisa-ação: uma introdução metodológica"e resumido na figura abaixo.

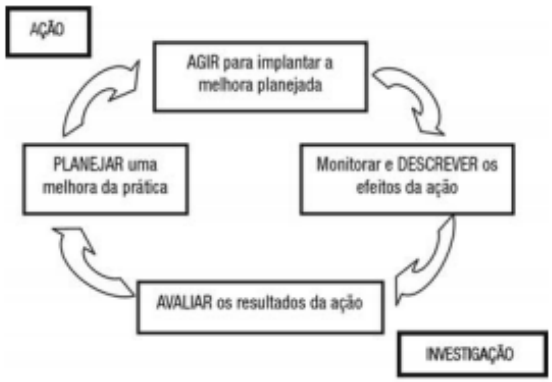


Figura 1: Representação em quatro fases da investigação - ação

Após breve discussão com os coordenadores, nos preparamos para a montagem da turma em que o projeto seria aplicado. Para isso, foi feita uma análise do histórico escolar dos alunos, onde neste histórico verificamos: as notas em todas as matérias, desempenho em olimpíadas de matemática (e de outras matérias) e comportamento escolar. Por fim foram escolhidos 5 alunos de cada ano (6º, 7º, 8º e 9º anos), totalizando então duas turmas de 20 alunos. Antes de iniciar as aulas, foi apresentado à coordenação pedagógica os conteúdos a serem trabalhado, ficando decidido que a aplicação seguiria o cronograma (anexado ao trabalho) com até 10 encontros semanais de 1h e 30 minutos de aula.

No decorrer do trabalho são apresentadas formas de construção de cartas códigos através da criptografia pelo uso de saberes matemáticos, e o uso do software livre GEOGEBRA como aliado na visualização geométrica da álgebra. Tudo isso possui como principal ponto de ancoragem a construção de um significado mais amplo de alguns conteúdos matemáticos que muitas vezes são apresentados de forma crua e sem nenhum atrativo que motive os alunos a desenvolverem conhecimentos em torno do que é ensinado.

Nos próximos capítulos serão listados os conteúdos escolhidos, de acordo com a capacidade que julgávamos que nossos alunos tinham e baseado nos conteúdos ministrados no Ensino Médio, para esta proposta. Vale salientar, que na proposta apresentada não ficaríamos amarrados em longas demonstrações, ligaríamos toda a parte teórica a exemplos numéricos, facilitando o entendimento preservando a boa utilização do tempo nas aulas.

3 Conteúdos Programáticos

Seguiremos uma sequência única de conteúdos utilizando conhecimentos pré existentes, sempre que possível com foco na resolução de exemplos e exercícios de nível mais avançado a que os alunos têm costume. Algumas demonstrações devido a sua importância serão apresentadas com base no livro de Samuel Jurkiewicz (Divisibilidade e Números Inteiros - Introdução à Aritmética Modular)oferecido pelo Programa de Iniciação Científica da OBMEP. Não daremos ênfase a assuntos já trabalhados na base curricular, pois nosso foco é a complementação (avanço) dos conteúdos.

3.1 Números Primos e Compostos

Definição 1. *Todo número natural diferente de* 0 *e de* 1 *que é apenas múltiplo de* 1 *e de si próprio é chamado de* ***número primo****.*

Definição 2. *Todo número natural diferente de* 0 *e de* 1 *que não é primo é chamado de* ***número composto****.*

Na teoria dos números primos e composto, dois resultados são muito utilizados na Aritmética. Um deles é o Teorema Fundamental da Aritmética, que afirma que qualquer número natural maior que 1 pode ser escrito de forma única (desconsiderando a ordem) como um produto de números primos: este processo se chama decomposição em fatores primos ou fatoração. Outro resultado bastante usual é o processo para determinar se um número é ou não primo. A demonstração de ambos os resultados estão disponíveis na versão digital do livro texto Matemática Elementar do Prof. Inaldo Barbosa de Albuquerque (UFPB). A seguir vamos enunciá-los.

Teorema 1. *Teorema Fundamental da Aritmética*

Todo inteiro positivo n pode ser escrito de maneira única como o produto de números primos, onde os fatores primos são escritos em ordem crescente de grandeza.

Teorema 2. *Seja a um número natural composto maior do que* 1*. Então a possui um divisor primo menor ou igual a raíz quadrada de a.*

Exemplos:

1. Os números $2, 3, 5, 11, 19$ e 3413 são primos. Mesmo com o teorema acima citado percebemos que quanto maior o número, mais difícil garantir se é primo.

2. Os números 52 e 455 são compostos, já que o primeiro é divisível por 2 e o segundo é divisível por 5.

3.1.1 Crivo de Eratóstenes

A palavra Crivo significa "peneira". Erastóstenes foi um sábio grego que desenvolveu um método para determinar todos os números primos até um certo número n utilizando um tabela com todos os números naturais até n. Feita a tabela ele retirava os múltiplos de 2 exceto o próprio 2 que é primo, na sequência os múltiplos de 3, exceto o número 3 que também é primo e assim sucessivamente. Como base no teorema 2 citado acima, Eratóstenes criou o seu crivo.

Abaixo segue o exemplo até o $n = 50$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Figura 2: Tabela de números de 1 a 50

Na sequência, serão apresentadas as tabelas segundo o método de Erastóstenes.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~

(a) Retirando múltiplos de 2 e o algarismo 1

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

(b) Retirando múltiplos de 3

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	26	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~

(c) Retirando múltiplos de 5

Figura 3: Determinando os números primos

Para concluir, basta excluir da tabela acima, os múltiplos de 7, exceto o próprio 7. Restando o número 49. Não precisamos continuar eliminando os múltiplos de 11, já que a $\sqrt[2]{50} < 11$, portanto já podemos encerrar o processo e concluir que os números primos até o 50 são: $\{2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47\}$.

3.2 Múltiplos, divisores e os restos

Apresentamos a divisão euclidiana através da equação de Euclides:

$$D = d \times q + r, r < d, d > 0, D, d, q, r \in N$$

onde D é o dividendo, d divisor, q quociente e r resto.

É comum trabalharmos com divisões exatas e não exatas através dos algoritmos de divisão como vemos abaixo:

Exemplos:

- $40 \div 2$ é uma divisão exata, já que o quociente é 20 e o resto é 0.
- $90 \div 40$ é uma divisão não exata, já que o quociente é 2 e o resto é 10.

Representando o primeiro exemplo no algoritmo da divisão temos:

$$\begin{array}{r|l} 40 & 2 \\ \hline 0 & 20 \end{array}$$

O fato do resto da divisão ser 0 é importante, uma vez que isso acontecendo, concluimos o dividendo e o quociente são **múltiplos** do divisor e mais, podemos dizer também que o dividendo e o quociente são **fatores** do 40. No exemplo acima dizemos que 40 e 20 são múltiplos de 2 e que o 20 e o 2 são fatores do 40.

É importante resaltar que o 40 possui outros fatores além dos citados uma vez que o número 40 pode ser decomposto de várias maneiras como observado abaixo:

Os fatores de 40:
1 e 40 , pois $1 \times 40 = 40$
2 e 20, pois $2 \times 20 = 40$
4 e 10, pois $4 \times 10 = 40$
5 e 8, pois $5 \times 8 = 40$
Portanto o conjunto dos fatores do 40 é $D(40) = \{1, 2, 4, 5, 8, 10, 20, 40\}$.

Representando o segundo exemplo através do algoritmo da divisão temos:

$$\begin{array}{r|l} 90 & 40 \\ \hline 10 & 2 \end{array}$$

Neste caso, a divisão é não exata, pois $r \neq 0$, algo importante para alertarmos os alunos quanto à determinação dos restos das divisões sem efetuar grandes cálculos.

Abaixo, apresentaremos alguns fatos importantes.

Fato 1) Se um número é fator (divisor) de dois outros números, ele é fator da sua soma (e da sua diferença).

Exemplo:
6 é fator de 30;
6 é fator de 48;
Então 6 é fator de $30 + 48 = 78$, e 6 é fator de $48 - 30 = 18$.

Fato 2) Dividindo dois números por um mesmo divisor, se a soma (diferença) dos restos for menor que o divisor, ela será igual ao resto da divisão da soma (diferença) dos dois números pelo divisor.

Exemplo na soma:
$22 \div 7 = 3$ e o resto é 1;
$33 \div 7 = 4$ e o resto é 5;
Como a soma dos restos $1 + 5 = 6$ é menor que 7 temos:
$22 + 33 = 55$ e $55 \div 7 = 7$ e o resto é 6.

Exemplo na diferença:
$33 \div 7 = 4$ e o resto é 5;
$22 \div 7 = 3$ e o resto é 1;
A diferença dos restos $5 - 1 = 4$ então $33 - 22 = 11$ e $11 \div 7 = 1$ e o resto é 1.

Fato 3) Dividindo dois números pelo mesmo divisor; se a soma dos restos for maior que o divisor, subtraímos o valor do divisor e o resultado será o resto da divisão da soma dos dois números pelo divisor. Se a diferença for um número negativo somamos o divisor.

Exemplo na soma:
$26 \div 7 = 3$ e o resto é 5;

$32 \div 7 = 4$ e o resto é 4;
A soma dos restos é 9 (portanto maior que 7), então o resto é $9 - 7 = 2$.
De fato, temos: $26 + 32 = 58$ e $58 \div 7 = 8$ e o resto é 2.

Exemplo na diferença:
$44 \div 7 = 6$ e o resto é 2;
$26 \div 7 = 3$ e o resto é 5;
A diferença dos restos $2 - 5 = -3$ (negativo) portanto $-3 + 7 = 4$ então $44 - 26 = 18$ e $18 \div 7 = 2$ e o resto é 4.

Fato 4) Dividindo dois números por um mesmo divisor, se a multiplicação dos restos for menor que o divisor, ela será igual ao resto da divisão do produto dos dois números pelo mesmo divisor. Caso a multiplicação dos restos seja maior que o dividor seguimos o mesmo procedimento já utilizado acima.
• Importante lembrar que para o caso de potenciação, podemos tratar como sucessivas multiplicações.

Exemplo na multiplicação:
$26 \div 7 = 3$ e o resto é 5;
$32 \div 7 = 4$ e o resto é 4;
A multiplicação dos restos é 20 (portanto maior que 7), então o resto do produto dos termos por 7 é $20 - 7 - 7 = 6$.
De fato, temos: $26 \cdot 32 = 832$ e $832 \div 7 = 118$ e o resto é 6.

Exemplo na potência:
Qual o resto de $12^6 \div 5$?
$12^6 = 12 \cdot 12 \cdot 12 \cdot 12 \cdot 12 \cdot 12$, mas como o resto de $12 \div 5$ é 2 temos que o resto de $12^6 \div 5$ será: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$, como $64 > 5(divisor)$ efetuamos $64 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 = 4$ (ou de maneira mais simples $64 \div 5$ deixa resto 4) e concluímos que o resto de $12^6 \div 5$ é 4.

3.3 Regras de divisibilidade

As regras de divisibilidade fazem parte da grade curricular do Ensino Fundamental e Médio, portanto aqui iremos apenas citá-las com base nos próprios livros didáticos (Giovanni e Giovanni Jr - A conquista da Matemática) e nos ater as apenas às demosntrações das regras de divibilidade do 7 e do 11 e à discussão quanto ao resto das divisões. Uma boa definição sobre divisibilidade está disponível no site do clube da OBMEP (http://clubes.obmep.org.br no artigo "Um pouco sobre divisibilidade – Critérios de divisibilidade".

Definição 3. *Um número natural n é divisível por d se, e somente se, a condição P é satisfeita.*

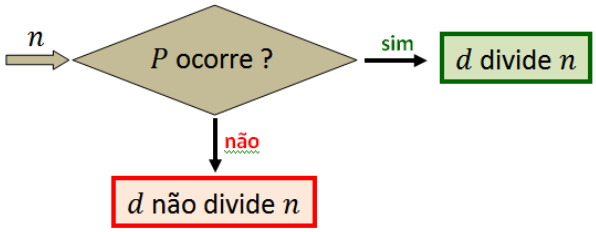


Figura 4: Organograma da divisibilidade

Isto não apenas significa que "se P for satisfeita, então n é divisível por d", mas também significa que "se a condição P não for satisfeita, então n não é divisível por d".

3.3.1 Divisibilidade por 2

Um número será divisível por 2 se terminar em $0, 2, 4, 6$ ou 8, isto é, quando for par.

Como pela divisão euclidiana temos que $r < d$ e como $d = 2$, teremos apenas duas possibilidades para o resto r: 0 (divisão por número par) e 1 (divisão por número ímpar).

Exemplo 1.

- 32 *é par portanto é divisível por* 2, *resto* 0.
- 2357 *é ímpar, resto* 1.

3.3.2 Divisibilidade por 3

Um número será divisível por 3 quando a soma dos seus algarismos for um número divisível por 3.

O resto da divisão por 3 será o resto da divisão do número formado pela soma dos algarismos por 3.

Exemplo 2.

- 4572 *é divisível por* 3, *pois a soma dos algarismos é* $4+5+7+2=18$ *que é múltiplo de* 3.
- 15983 *não é divisível por* 3, *pois a soma dos algarismos é* $1+5+9+8+3=26$ *que não é múltiplo de* 3, *e como* $26 \div 3$ *deixa resto* 2 *implica que* $15983 \div 3$ *também deixará resto* 2. *É importante ressantar que na soma dos algarismos não é necessário incluir os algarismos* 9 *e* 3, *pois estes já são múltiplos de* 3. *Bastava então calcular* $1+5+8=14$ *que também não é divisível por* 3, *deixando resto* 2.

3.3.3 Divisibilidade por 4

Um número natural será divisível por 4 quando terminar em 00 ou quando o número formado seus dois algarismos da direita for divisível por 4.

Exemplo 3.

- 500 *é divisível por* 4, *pois termina em* 00.
- 1380 *é divisível por* 4, *pois* 80 *é divisível por* 4.
- 4526 *não é divisível por* 4, *pois não termina em* 00 *e* 26 *não é divisível por* 4. *O resto da divisão é* 2, *uma vez que* $26 \div 4$ *deixa resto* 2.

3.3.4 Divisibilidade por 5

Um número natural é divisível por 5 quando terminado em 0 ou 5.

Exemplo 4.

- 420420 *é divisível por* 5, *pois termina em 0.*
- 21237 *não é divisível por* 5, *pois não termina em* 0 *ou* 5. *O resto da divisão será* 2, *uma vez que para determinar o resto analisaremos apenas o algarismo das unidades e então:* $7-5=2$.

3.3.5 Divisibilidade por 6

Um número natural será divisível por 6 quando for divisível por 2 e por 3 ao mesmo tempo.

Exemplo 5.

- 570 *é divisível por* 6, *pois termina em algarismo par (regra de divisibilidade do* 2 *e pois a soma dos algarismos* $0+5+7=12$ *é múltiplo de* 3 *(regra de divisibilidadedo* 3*).*
- 436 *não é divisível por* 6, *pois apesar de satisfazer a regra de divisibilidade do* 2, *não satisfaz a regra de divisibilidade do* 3 *já que a soma dos seus algarismos* $4+3+6=13$ *que não é múltiplo de* 3. *Para determinar o resto da divisão somamos o algarismo das unidades com o quádruplo da soma dos algarismos restantes e efetuamos a divisão por* 6. *No exemplo, temos* $6+4\cdot(4+3)=34$ *e como* $34\div 6$ *deixa resto* 4 *a dvisão* $436\div 6$ *também deixará resto* 4.

3.3.6 Divisibilidade por 7

Regra 1) Um número natural é divisível por 7 quando dado um número de três algarismos,retira-se o último algarismo da direita e calcula-se o seu dobro, subtrai-se do número que restou. Essa diferença tem que ser divisível por 7. Caso o número possua mais de três algarismos, efetua-se esse processo quantas vezes forem necessárias.

Exemplo 6.

- 294 *é divisível por* 7, *pois* $4\cdot 2=8$ *e* $29-8=21$ *que é múltiplo de* 7.
- 7557 *não é divisível por* 7, *pois* $7\cdot 2{,}755-14=741$, *efetuando o processo novamente temos:* $1\cdot 2=2$ *e* $74-2=72$ *que não é múltiplo de* 7.

Na maioria dos livros didáticos não encontramos essa regra de divisibilidade do número 7, portanto discorreremos mais sobre tal regra.

Demonstração. Para demonstrá-la podemos pensar inicialmente em um número de dois algarismos xy que pode ser escrito $10x+y$. Então queremos mostrar que:

- $10x+y$ é divisível por 7 se e só se $x-2y$ também for divisível por 7.

Mas se $10x + y$ é divisível temos:

$$\begin{aligned} &\iff 10x + y - 7x - 7y \\ &\iff 3x - 6y \\ &\iff 3(x - 2y) \\ &\iff x - 2y. \end{aligned}$$

Podemos estender a demonstração para números com mais de dois algarismos uma vez que expressar um número com vários algarismos:

$$\text{ABCDE...KLM.}$$

Se fizermos $x = ABCDE...KL$ e $y = M$, teremos:

$$ABCDE...KLM = 10x + y$$

que só será divisível por 7 se $x - 2y = ABC...KL - 2M$ também for. □

Porém essa regra não nos leva ao resto da divisão por 7. Portanto vamos enunciar outra regra que nos possibilita concluir se um número é ou não divisível por 7 e em caso negativo, determinar o resto da divisão.

Regra 2) Um número natural é divisível por 7 quando tomarmos o primeiro algarismo à esquerda, multiplicarmos por 3 e somarmos ao segundo algarismo à esquerda e em seguida substituirmos os dois primeiros algarismos à esquerda pelo resultado encontrado. Se o número original é divisível por 7 o número também será. Ao efetuar o processo até se tornar um número menor ou igual a 7 teremos o resto da divisão.

Exemplo 7.

- 3486 *é divisível por* 7, *pois ao efetuar o processo termina-se em um mútiplo de* 7, *vejamos:*

$$\begin{aligned} 3486 &\to 3 \times 3 + 4 = 13 \\ 1386 &\to 1 \times 3 + 3 = 6 \\ 686 &\to 6 \times 3 + 8 = 26 \\ 266 &\to 2 \times 3 + 6 = 12 \\ 126 &\to 1 \times 3 + 2 = 5 \\ 56 &\to 5 \times 3 + 6 = 21 \\ 21 &\to 2 \times 3 + 1 = 7 \end{aligned}$$

- 5129 *não é divisível por* 7*, pois ao efetuar o processo termina-se em um número que não é múltiplo de* 7 *vejamos:*

$$\begin{aligned} 5129 &\rightarrow 5 \times 3 + 1 = 16 \\ 1629 &\rightarrow 1 \times 3 + 6 = 9 \\ 929 &\rightarrow 9 \times 3 + 2 = 29 \\ 299 &\rightarrow 2 \times 3 + 9 = 15 \\ 159 &\rightarrow 1 \times 3 + 5 = 8 \\ 89 &\rightarrow 8 \times 3 + 9 = 33 \\ 33 &\rightarrow 3 \times 3 + 3 = 12 \\ 12 &\rightarrow 1 \times 3 + 2 = 5 \end{aligned}$$

Neste caso, o resto de $5129 \div 7$ *é 5.*

3.3.7 Divisibilidade por 8

Um número será divisível por 8 quando terminar em 000 ou quando o número formado por seus três últimos algarismos for divisível por 8.

Exemplo 8.

- *7520 é divisível por 8, pois 520 é divisível por 8.*
- *34118 não é divisível por 8, pois 118 não é divisível por 8. O resto da divisão será o mesmo da divisão de* $118 \div 8$ *que é 6.*

3.3.8 Divisibilidade por 9

Um número natural será divisível por 9 quando a soma dos seus algarismos for um número divisível por 9 (múltiplo).

Exemplo 9.

- *6408 é divisível por 9, pois a soma dos seus algarismos é 18 que é múltiplo de 9.*
- *27319 não é divisível por 9, pois a soma dos seus algarismos* $2 + 7 + 3 + 1 + 9 = 22$ *que não é múltiplo de 9. O resto da divisão é* 4 *uma vez que* $22 \div 9$ *deixa resto 4.*

É importante visualizar que na soma dos algarismos bastava somar os algarismos que não são múltiplos de 9, portanto $2+7+3+1=13$ *e verificar que 13 não é múltiplo de 9 e que* $13 \div 9$ *deixa resto 4.*

3.3.9 Divisibilidade por 10

Um número natural será divisível por 10 quando terminado em 0.

Exemplo 10.

- *11500 é divisível por 10,pois termina em 0.*
- *4203 não é divisível por 10, pois termina em 3.O resto da divisão será o próprio algarismo das unidades, portanto resto 3.*

3.3.10 Divisibilidade por 11

Um número natural é divisível por 11 quando a diferença entre a soma dos algarismos de ordem ímpar (S_i) e a soma dos algarismos de ordem par (S_p) for igual a um múltiplo de 11.

Exemplo 11.

- *6172947 é divisível por 11,pois* $S_i = 7+9+7+6 = 29$ *e* $S_p = 4+2+1 = 7$*, então* $S_i - S_p = 22$ *que é múltiplo de 11.*
- *146935 não é divisível por 11, pois* $S_i = 5+9+4 = 18$ *e* $S_p = 3+6+1 = 10$*, então* $S_i - S_p = 8$*. Como a diferença foi um número menor que 11, o resto da divisão será o próprio* 8*. Caso este número fosse maior que 11 deveríamos subtrair o múltiplo 11 mais próximo inferiormente do resultado de* $S_i - S_p$ *e então teríamos o resto da divisão.*
- *5486 não é divisível por 11, pois* $S_i = 6+4 = 10$ *e* $S_p = 8+5 = 13$*, então* $S_i - S_p = -3$*. Para determinar o resto da divisão por 11 neste caso devemos adicionar à essa diferença um múltiplo de 11 para que o resultado se torne positivo entre 0 e 11, para então sabermos o resto da divisão, portanto* $-3+11 = 8$*, resto 8.*

A regra de divisibilidade do número 11 também não aparece nos livros didáticos, então é de grande valia apresentarmos a demonstração.

Demonstração. Dado um número natural da forma:

$$a_n a_{n-1} a_{n-2} ... a_3 a_2 a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + a_{n-2} 10^{n-2} + ... a_3 10^3 + a_2 10^2 + a_1 10 + a_0$$

Efetuando as divisões de cada parcela por 11 temos que a_0 é um algarismo portanto na divisão por 11 o resto será ele mesmo a_0. Já o termo $a_1 10$ deixa resto $(-1).a_1 = -a_1$, o termo $a_2 10^2$ deixa como resto $(-1)^2.a_2 = a_2$, o termo $a_3 10^3$ deixa como resto $(-1)^3.a_3 = -a_3$ e assim sucessivamente. Conforme já citado, para descobrir o resto da divisão de um número basta efetuar a soma dos restos das divisões de suas parcelas, concluímos que:

$$a_n(-1)^n + a_{n-1}(-1)^{n-1} + a_{n-2}(-1)^{n-2} + ... - a_3 + a_2 - a_1 + a_0 = S_i - S_p$$

que será o resto da divisão de $a_n a_{n-1} a_{n-2} ... a_3 a_2 a_1 a_0$ por 11. □

3.3.11 Divisibilidade por 12 e 15

Para determinar a regra de divisibilidade de números compostos como é o caso do número 6 que já citamos, basta reescrevê-lo como produto de dois números coprimos [1] no caso do número 6 utilizamos o produto dos números 2 e 3 (que já conhecemos suas regras de divisibilidade). Portanto temos:

Um número é divisível por 12 quando for divisível por 3 e por 4 o mesmo tempo.

Um número será divisível por 15 quando for divisível por 3 e por 5 ao mesmo tempo.

Exemplo 12.

- *228 é divisível por 12, pois a soma dos algarismos* $8 + 2 + 2 = 12$ *é um múltiplo de 3 (regra de divisibilidade por 3) e os dois últimos algarismos formam um número* (28) *divisível por 4 (regra de disibilidade por 4).*
- *4732 não é divisível por 12, pois apesar de satisfazer a regra de divisibilidade por 4, não satisfaz a regra de divisibilidade por 3 uma vez que a soma dos algarismos* $2 + 3 + 7 + 4 = 16$ *não é um múltiplo de 3.*
- *45 é divisível por 15, pois como a soma dos algarismos é* 9 *e portanto múltiplo de 3 é divisível por 3 e como termina em 5 também é divisível por 5.*
- *4392 não é divisível por 15, pois não satisfaz a regra de divisibilidade por 5.*

Percebemos que quanto maior o número em que buscamos uma regra de divisibilidade, mais extenso fica o processo. Portanto para números maiores é orientável utilizar o algorítmo da divisão tradicional.

[1] Dois números são chamados de coprimos quando o mdc entre eles é 1.

3.4 Máximo Divisor Comum e Mínimo Múltiplo Comum

Dois cálculos muito utilizados em matemática, são o mmc e o mdc, respectivamente, mínimo múltiplo comum e máximo divisor comum. As definições e procedimentos para tais cálculos são comumente ensinados do final do Ensino Fundamental I(a partir do $5^o ano$) até o Ensino Fundamental II. Já no Ensino médio o conteúdo citado é aprofundado juntamente com o Ensino de divisão euclidiana. Vale ressaltar que *mmc* e *mdc* são temas recorrentes nos últimos anos em muitos vestibulares..

3.4.1 MDC

Definição 4. *O máximo divisor comum de dois números a e b é o maior número que é divisor destes dois números. Sejam dados dois números naturais a e b, distintos ou não. Um número natural d será dito um divisor comum de a e b se d/a e d/b (leia-se d divide a e d divide b).*

Analisando a apresentação do tema em vários livros percebemos que o usual para cálculo do *mdc* de dois números é o uso de dois métodos. O primeiro passo consiste em listar todos os divisores de cada número e verificar o menor divisor comum nas duas listagens. O segundo método utiliza a decomposição em fatores primos. Vejamos um exemplo:

•$Exemplo : mdc(30, 75)$

1. 1º Método

   $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

   $D(75) = \{1, 3, 5, 15, 25, 75\}$

   $mdc(30, 75) = 15$

2. 2º Método

Para se obter o *mdc* entre dois ou mais números, deve-se:

1. Decompô-los em fatores primos;

2. Tomar os fatores primos comuns com seus menores expoentes;

3. Efetuar o produto desses fatores.

Exemplo 13.

- *Calcular o máximo divisor comum de* 30 *e* 75.

Decompondo-os em fatores primos temos:

$$30 = 2.3.5 \qquad 75 = 3.5^2$$

Daí, temos que o $mdc(30, 75) = 3.5 = 15$.

Observação: Ainda existe um método prático e mais usual em que se efetua a fatoração simultanea, e seleciona os números primos que dividiu simultanamente os dois números à esquerda conforme tabela abaixo.

30,	75	2
15,	75	3
5,	25	5
1,	5	5
1,	1	$2 \cdot 3 \cdot 5^2$

Seleciona-se os números 3 e o primeiro número 5 que dividem simultaneamente 30 e 75 e portanto o $mdc(30, 75) = 3 \cdot 5 = 15$.

Outro método apresentado aos alunos do Ensino Fundamental I (5º ano)para determinar o mdc de dois números e que acaba se perdendo durante os anos seguintes é o método das divisões sucessivas. Nele construímos uma tabela com 3 linhas, na primeira linha colocamos os quocientes das divisões (sucessivas) e na terceira linha os restos. Na segunda linha iniciamos com os números que desejamos calcular o *mdc* e em seguida colocamos os restos das divisões. Quando o resto da divisão for 0, o último termo da segunda linha será o mdc procurado. Abaixo vemos dois exemplos:

$mdc(180, 50) \Rightarrow$

	3	1	1	2
180	50	30	20	***10***
30	20	10	0	

$mdc(66,40) \Rightarrow$

	1	1	1	1	6
66	40	26	14	12	***2***
26	14	12	2	0	

E então temos que:$mdc(180,50) = 10$ e $mdc(66,40) = 2$.

3.4.2 MMC

Definição 5. *O mínimo múltiplo comum de dois ou mais números naturais é o menor número natural, excluindo o zero, que é múltiplo desses números.*

Para o cálculo do *mmc* podemos também listar os múltiplos de cada números até encontrar o primeiro (mínimo) múltiplo comum em todas as listagens.

Exemplo 14.

- $mmc(30,75)$
$M(30) = \{0,30,60,90,120,150,180,210...\}$
$M(75) = \{0,75,150...\}$

Portanto como o primeiro termo que se repete (desconsiderando-se o zero) é o número 150 temos que o $mmc(30,75) = 150$

Como segunda opção para o cálculo do *mmc* entre dois números ou mais números naturais orienta-se o uso da fatoração seguindo os seguintes passos:

1. Decompô-los em fatores primos;
2. Tomar todos os fatores primos comuns e não comuns com seus maiores expoentes;
3. Efetuar o produto desses fatores:

Exemplo 15.

- *Calcular o mínimo múltiplo comum dos números* 90, 96 *e* 54.

$90 = 2.3^2.5 \quad 96 = 2^5.3 \quad 54 = 2.3^3$
Daí, temos que o $mmc(90,96,54) = 2^5.3^3.5 = 4320$

Observação: Esse processo também pode ser desenvolvido pela fatoração simultanea e multplicando todos os números primos da fatoração conforme o exemplo abaixo:

$mmc(90, 96, 54)$

90,	96,	54	2
45,	48,	27	2
45,	24,	27	2
45,	12,	27	2
45,	6,	27	2
45,	3,	27	3
15,	1,	9	3
5,	1,	3	3
5,	1,	1	5
1,	1,	1	$2^5 \cdot 3^3 \cdot 5$

Daí, temos que o $mmc(90, 96, 54) = 2^5 \cdot 3^3 \cdot 5 = 4320$

3.4.3 MMC e MDC - visualização gráfica

A utilização do software GEOGEBRA tem o intuito de dar mais materialidade ao assunto estudado buscando enriquecer as aulas e chamar a atenção do aluno para tal conteúdo, devido à constante cobrança nos vestibulares do país. Portanto usando software livre GEOGEBRA mostraremos a visão geométrica do *mmc* e do *mdc* através da construção de retângulos.

No primeiro exemplo mostraremos o *mmc* e o *mdc* dos números 5 e 10.

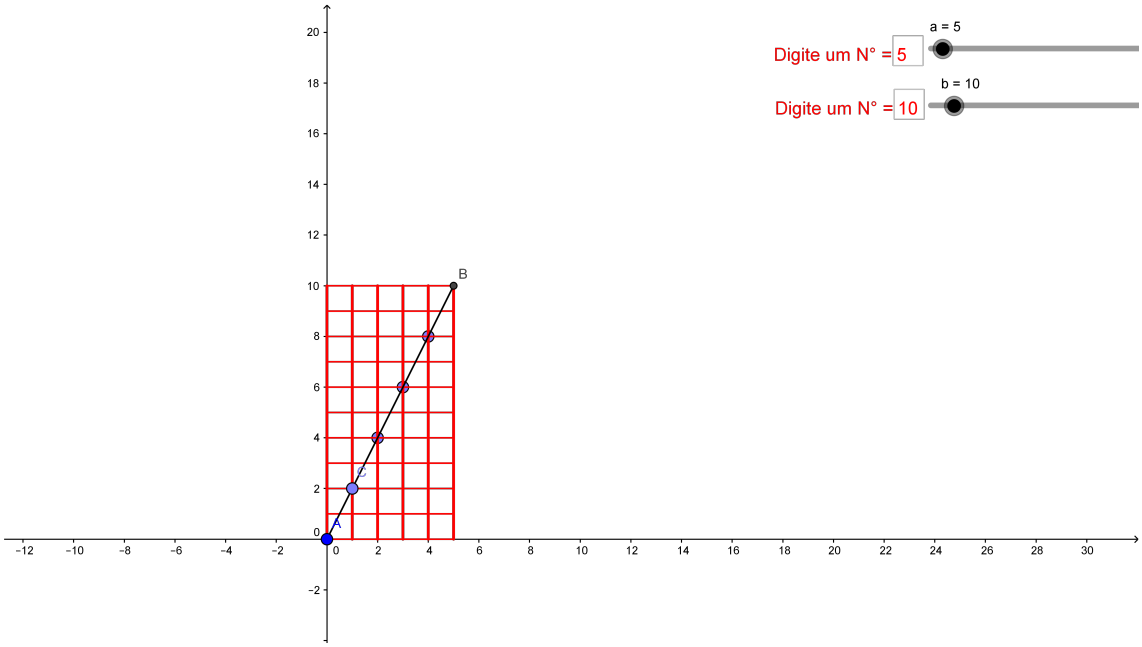


Figura 5: Visualização gráfica- $mmc(5, 10)$ e $mdc(5, 10)$

Ao construir o retângulo de comprimento 5 e largura 10 unidades, subdividiu-se em quadrados unitários.

Observe que a diagonal do retângulo passa pelos vértices de 6 quadradinhos unitários e consequentemente fica dividida em 5 partes iguais, portanto, $mdc(5, 10) = 5$. Perceba também que a diagonal divide o retângulo maior em 5 retângulos menores e cada um deles possui, igualmente, 10 quadradinhos unitários , concluindo que $mmc(5, 10) = 10$.

Vejamos mais um exemplo usando os números 8 e 12.

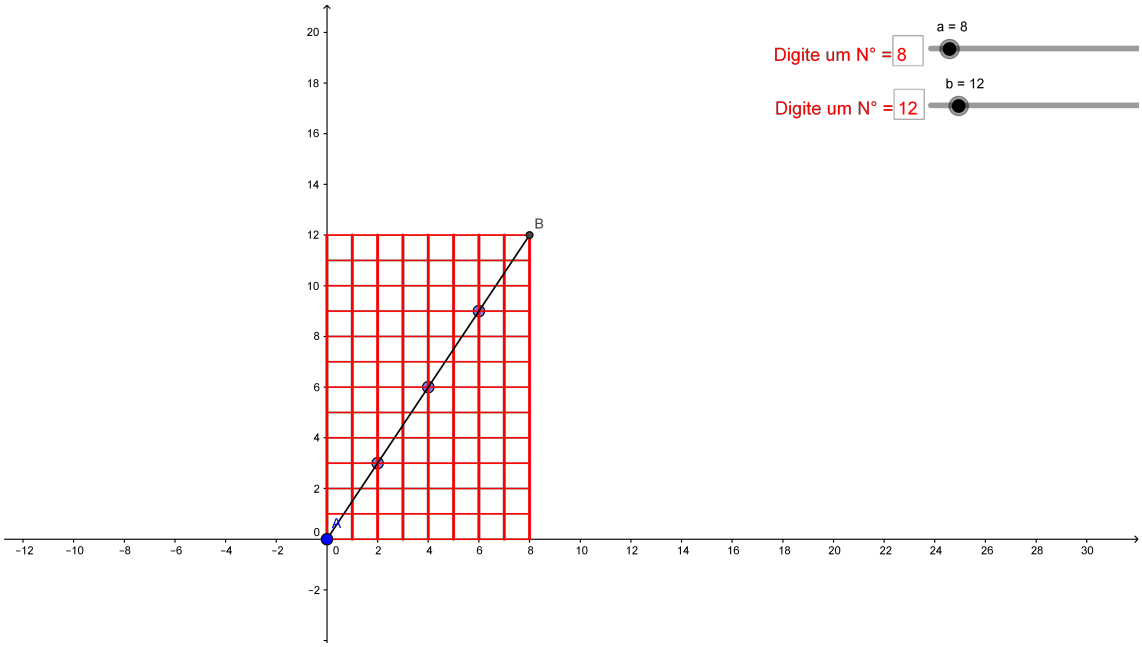


Figura 6: Visualização gráfica-$mmc(8, 12)$ e $mdc(8, 12)$

A diagonal do retângulo está dividida em 4 partes, assim, $mdc(8, 12) = 4$. Observe que a diagonal divide o retângulo maior em quatro retângulos menores, cada um contendo 28 quadradinhos unitários, portanto, $mmc(8, 12) = 24$.

3.4.4 Construção gráfica usando GEOGEBRA

Montagem no Geogebra

Construção passo a passo no software GEOGEBRA

1. Abra o Geogebra criando um novo arquivo;
2. No campo de entrada $A = (0, 0)$ e $B = (a, b)$, ao solicitar a ferramenta controles deslizantes, atribua nomes de a e b para denominar os valores.
3. Construa uma função $f(x) = y(B)/x(B)x$
4. Construa o segmento de $\overline{AB}$
5. Insera a Sequência: $[Segmento[(i, 0), (i, b)], i, 0, a]$
6. Insera a Sequência: $[Segmento[(0, i), (a, i)], i, 0, b]$

7. Digite na linha de comando de entrada:
   $Ponto[Sequncia[Se[Inteiro[f(i)],(i,f(i))],i,1,a-1]]$

8. Digite na linha de comando de entrada:
   $floor(g); controledeslizante; propriedades;$
   $alterarnomeedescrioparafloor(g)$

9. Digite na linha de comando de entrada:
   $ManterSe[x = floor(x), L_1]; controledeslizante$
   Alterar nome e descrição para mdc

10. Digite na linha de comando de entrada:
    $ManterSe[x = floor(x), L_1]$

11. Na caixa de texto, digite um texto dizendo que "O mdc entre os Números "objeto a"e "objeto b"= "Objeto mdc"

12. Insira campos de entradas onde você possa digitar manualmente os números desejados para o *mdc*.

É importante salientar, que devido a facilidade de se trabalhar com o GEOGEBRA, podemos determinar os valores máximos e mínimos dos controles deslizantes e então calcular o *mmc* e *mdc* de quaisquer valores, inclusive de valores bem maiores conforme a imagem abaixo:

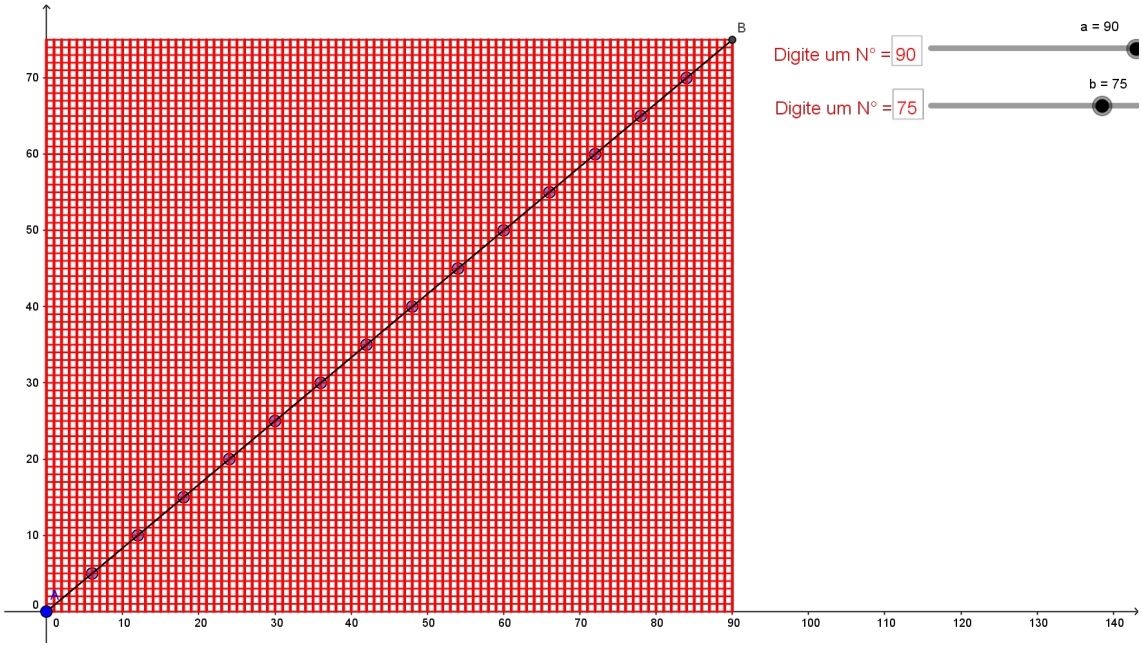


Figura 7: Visualização gráfica- $mmc(90, 75)$ e $mdc(90, 75)$

Visualmente percebe-se que a diagonal do retângulo coincide com 16 vértices dos quadrados unitários e fica dividida em 15 partes, portanto o $mdc(90, 75) = 15$. Cada uma dessas 15 partes são retângulos de 5u de largura por 90u de comprimento e então o $mmc(90, 75) = 5 \cdot 90 = 450$.

3.4.5 Consequências do estudo de mmc e mdc

Após o estudo dos temas, podemos avançar e já concluir algumas consequências imediatas. Como forma de incremento podemos definir o cálculo do número de divisores de um número e enunciar a propriedade que relaciona o *mmc*, o *mdc* e o produto de dois números.

Proposição 1. *Seja um número n e sua decomposição em fatores primos:*

$$n = p_1^{t_1}.p_2^{t_2}.p_3^{t_3}...p_{r-1}^{t_{r-1}}.p_r^{t_r}$$

Com os $p_i's$ todos diferentes. O número de divisores de n é igual a:

$$(t_1 + 1).(t_2 + 1).(t_3 + 1)...(t_{r-1} + 1).(t_r + 1)$$

Demonstração. : A demonstração utiliza a seguinte idéia:
Como vimos, todo número n possui uma única decomposição em fatores primos.

$$n = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_r^{t_r}$$

Um número primo p tem apenas dois divisores positivos: 1 e p.
p^2 tem como divisores positivos apenas os números: 1, p e p^2.
p^t tem 1,p,p^2,...,p^t como divisores positivos, totalizando $(t+1)$ divisores. Portanto pelo princípio multiplicativo (análise combinatória)o número de divisores de n é:

$$(t_1 + 1).(t_2 + 1).(t_3 + 1)...(t_{r-1} + 1).(t_r + 1)$$

□

Exemplo 16.

- *O número 360 em sua decomposição em fatores primos temos:*

$$360 = 2^3 \times 3^2 \times 5^1$$

Portanto o número de divisores de 360 *é :*

$$(3 + 1).(2 + 1).(1 + 1) = 24$$

Proposição 2. *Sendo a e b dois números naturais, temos:*

$$mmc(a, b).mdc(a, b) = a.b$$

Propriedade válida, apenas para dois números naturais.

Demonstração. Se $a = p_1^{t_1}.p_2^{t_2}.p_3^{t_3}...p_k^{t_k}$ e $b = p_1^{m_1}.p_2^{m_2}.p_3^{m_3}...p_k^{m_k}$ então: $a{\cdot}b = p_1^{s_1}.p_2^{s_2}.p_3^{s_3}...p_k^{s_k}$ com $s_i = t_i + m_i$.
Como:

$$mmc(a, b) = p_1^{max\{t_1,m_1\}}.p_2^{max\{t_2,m_2\}}.p_3^{max\{t_3,m_3\}}...p_k^{max\{t_k,m_k\}}$$

$$mdc(a, b) = p_1^{min\{t_1,m_1\}}.p_2^{min\{t_2,m_2\}}.p_3^{min\{t_3,m_3\}}...p_k^{min\{t_k,m_k\}}$$

e $min\{t_i, m_i\} + max\{t_i, m_i\} = t_i + m_i$, temos que:

$$mmc(a, b).mdc(a, b) = a.b$$

□

Exemplo 17. *Dado os números* 45 *e* 21 *verificamos a propriedade.*
$mdc(21, 45) = 3$
$mmc(21, 45) = 315$
$mdc(21, 45).mmc(21, 45) = 3.315 = 945$
Uma vez que $45 \times 21 = 945$, *e*

$$mdc(21, 45).mmc(21, 45) = 21.45 = 945$$

a propriedade é válida.

3.5 Aritmética Modular

O conceito de Aritmética Modular passa pela teoria da divisibilidade de números inteiros, se estende no vasto campo da teoria dos números com conceitos de congruência modular e possui diversos níveis de aplicabilidade. Esse tema não é contemplado pela base curricular do Ensino Fundamental, portanto sempre que possível exemplicaremos com exemplos numéricos.

Definição 6. *Seja* $m > 1$ *um número inteiro, diz-se que* a *e* b *são* ***congruentes módulo m*** *se* $m \mid (a - b)$ *(leia-se* m *divide* $(a - b)$*), ou seja, se* a *e* b *deixam o mesmo resto quando divididos por* m*. E então escrevemos:*

$$a \equiv b \pmod{m}$$

A congruência módulo m *é uma relação de equivalência pois a proposição a seguir é válida.*

Proposição 3. *Para quaisquer* $a, b, c, m \in Z$ *temos:*

1) (Reflexividade) $a \equiv a \pmod{m}$*;*

2) (Simetria) se $a \equiv b \pmod{m}$ *então* $b \equiv a \pmod{m}$*;*

3) (Transitividade) se $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$ *então* $a \equiv c \pmod{m}$*.*

Demonstração. No item 1) basta notar que $m \mid (a - a) = 0$. No item 2), como $m \mid (a - b) \Rightarrow m \mid -(a - b)$, portanto $m \mid (b - a)$. No item 3), uma vez que $m \mid (a - b)$ e $m \mid (b - c) \Rightarrow m \mid (a - b) + (b - c)$, então $m \mid (a - c)$. □

Definição 7. *Define-se* ***classe de equivalência módulo n*** *como sendo todos os possíveis restos da divisão de um número qualquer por* n*. Portanto as classes de equivalências módulo* n *podem ser qualquer elemento do conjunto* $\{0, 1, 2, 3, 4, ..., n - 1\}$.

Proposição 4. *Se $a, b \in N$ com $a > b$. Diz-se $a \equiv b \pmod{m}$, se e somente se, $a - b$ é divisível por m.*

Demonstração. : Pelo algoritmo de Euclides temos:

$$a = m.q_1 + r_1, 0 \leqslant r_1 < m \tag{1}$$

$$b = m.q_2 + r_2, 0 \leqslant r_2 < m \tag{2}$$

Se a e b são congruentes temos que $r_1 = r_2$. Efetuando a subtração de (1) por (2) chegamos a:

$$a - b = \quad m.q_1 - m.q_2 + r_1 - r_2 \tag{3}$$

$$a - b = \quad m.(q_1 - q_2) \tag{4}$$

Portanto m divide $a - b$.
Por outro lado, se $a - b$ divide m, temos ainda da equação (3):

$$a - b = \quad m.q_1 - m.q_2 + r_1 - r_2 \tag{5}$$

Implica dizer que $r_1 - r_2$ divide m, mas:

$$\Rightarrow \quad -m < r_1 - r_2 < m \tag{6}$$

$$\Rightarrow \quad r_1 - r_2 = 0 \tag{7}$$

$$\Rightarrow \quad r_1 = r_2 \tag{8}$$

□

Exemplo 18.

- $6 \equiv 2 \pmod{4}$, *pois 6-2=4 , que é múltiplo de 4.*
- $10 \equiv 2 \pmod{4}$, *pois 10-2=8 , que é múltiplo de 4.*
- $70 \equiv 10 \pmod{12}$, *pois 70-10=60 , que é múltiplo de 12.*

As possíveis classes de equivalência módulo 4 são $0, 1, 2$ e 3. Dizemos ainda que os números 6 e 10 pertencem a mesma **classe de equivalência módulo 4**, uma vez que ambos deixam resto 2 quando divididos por 4.

Exemplo 19. *Classes de equivalência módulo 3:*

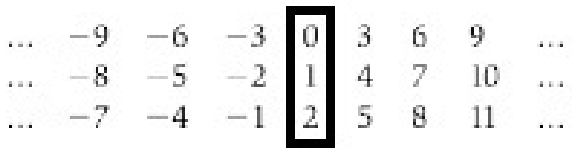


Figura 8: Equivalência módulo 3

Qualquer membro de uma classe de equivalência é substituível por qualquer outro da classe; quando vistos módulo 3*, os números* 5 *e* 11 *equivalem ao mesmo valor.*

Teorema 3. *Se* $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$ *então:*

i) $a + c \equiv b + d \pmod{m}$

ii) $ac \equiv bd \pmod{m}$

iii) $a^k \equiv b^k \pmod{m}$*, para* $K \in N$

iv) Se $mdc(k, m) = d$*, então* $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$

Os três primeiros itens já foram discutidos na seção 3.2 deste trabalho, portanto vamos demonstrar apenas o item iv. Usaremos a simbologia $a \mid b$ (leia-se a divide b).

Demonstração.

i) Temos que: $a \equiv b \pmod{m} \Leftrightarrow \exists x \in Z$ tal que, $a = b + xm$ e $c \equiv d \pmod{m} \Leftrightarrow \exists y \in Z$ tal que, $c = d + ym$. Logo,$a + c = b + d + (x + y)m \Leftrightarrow a + c \equiv (b + d) \pmod{m}$.

ii) Temos que: $a \equiv b \pmod{m} \Leftrightarrow \exists x \in Z$ tal que, $a = b + xm$ e $c \equiv d \pmod{m} \Leftrightarrow \exists y \in Z$ tal que, $c = d + ym$. Logo,

$$\begin{aligned} &\iff ac = (b + xm)(d + ym) \\ &\iff ac - bd = (b + xm)(d + ym) - bd \\ &\iff ac - bd = bd + bym + dxm + xym^2 - bd \\ &\iff ac - bd = (by + dx + xym)m \end{aligned}$$

ou seja, $ac \equiv bd \pmod{m}$.

iii) Como consequência da propriedade item ii, temos que:
Se $a \equiv b \pmod{m}$ então $a.a \equiv b.b \pmod{m} \Rightarrow a^2 \equiv b^2 \pmod{m}$. Daí temos que $a^2.a \equiv b^2.b \pmod{m} \Rightarrow a^3 \equiv b^3 \pmod{m}$. Repetindo o processo temos então que: $a^k \equiv b^k \pmod{m}$.

iv) Temos que:

$$ka \equiv kb \pmod{m} \iff m \mid (ka - kb)$$

Como o $mdc(k, m) = d$ podemos dividir ambos os membros por d e então:

$$\iff \frac{m}{d} \mid \frac{k}{d}.(a - b)$$

Mas ao efetuar essa divisão os termos $\frac{m}{d}$ e $\frac{k}{d}$ tornam-se primos entre si e então $\frac{m}{d} \nmid \frac{k}{d}$, portanto:

$$\iff \frac{m}{d} \mid (a - b)$$
$$\iff a \equiv b \pmod{\frac{m}{d}}$$

□

3.6 Equação diofantina Linear

A palavra Diofantina se refere ao matemático helenístico do século III, Diofanto de Alexandria, o qual estudou tais equações e foi um dos primeiros matemáticos a introduzir o uso de símbolos na álgebra. O estudo matemático de problemas Diofantinos propostos por Diofanto agora é chamado de análise Diofantina(Wikipédia). Uma equação diofantina é linear quando escrita da seguinte forma:

$$a_1.x_1 + a_2.x_2 + a_3.x_3 + ... + a_n.x_n = c$$

com coeficientes a_i, $1 \leq i \leq n$, sendo números inteiros. Para resolver a equação citada buscamos valores inteiros para o $x_1, x_2, x_3, ..., x_n$ que satisfaçam a equação.Nesta seção trabalharemos apenas com equações diofantinas com duas incógnitas, buscando determinar quando essas equações possuem soluções e quais são essas soluções.

É importante salientar que o tema é tratado no Ensino Fundamental como equação com duas incógnitas ocultando o nome de equação diofantina e que normalmente busca-se soluções por tentativas sem relacioná-las.

Teorema 4. *A equação diofantina linear $a.x + b.y = c$ possui solução se, e somente se, o $mdc(a, b)$ divide c.*

Demonstração. Temos por hipótese que a equação diofantina linear $a.x+b.y = c$ possui solução. Dada uma solução qualquer (x_0, y_0) teremos:

$$a.x_0 + b.y_0 = c$$

Mas sabendo por definição de máximo divisor comum que $mdc(a,b) \mid a$,$mdc(a,b) \mid b$ então $mdc(a,b)$ também dividirá a combinação linear formada por a e b.

$$mdc(a,b) \mid a \text{ e } mdc(a,b) \mid b \Rightarrow mdc(a,b) \mid a.x_0 + b.y_0 \Rightarrow mdc(a,b) \mid c$$

Supondo agora por hipótese que $mdc(a,b) \mid c$ então existe um $d \in Z$ tal que $c = d.mdc(a,b)$. Pela relação de Bézout garantimos que existe $m, n \in Z$ tais que :

$$a.m + b.n = mdc(a,b)$$

Multiplicando ambos os membros por d temos:

$$am.d + bn.d = d.mdc(a,b) \Rightarrow am.d + bn.d = c$$

Tomando $x_0 = md$ e $y_0 = nd$, a equação terá a solução (x_0, y_0). □

Exemplo 20.

- $5x + 15y = 33$
  mdc(5,15)=5
  5 não divide 33.
  Portanto a equação diofantina não possui solução.
- $3x + 5y = 223$
  mdc(3,5)=1
  1 divide 233.
  Portanto a equação diofantina possui solução.

Para determinar as soluções das equações diofantinas é necessário compreender o teorema abaixo.

Teorema 5. *Se (x_0, y_0) é uma solução particular da equação $ax + by = c$, em que o mdc(a,b)=1. Então as soluções são da forma :*

$$x = x_0 + bt \ , \ y = y_0 - at \ com \ t \in Z$$

Demonstração. A equação tem solução se $mdc(a,b)$ divide c, então dividindo a equação $ax + by = c$ pelo $mdc(a,b)$ temos uma nova equação $a'x + b'y = c'$ (*). Vamos inicialmente testar a solução $x = x_0 + b't$, $y = y_0 - a't$ substituindo em (*).

$$a'x + b'y = c' \Rightarrow a'(x_0 + b't) + b'(y_0 - a't) = c' \tag{9}$$
$$a'x_0 + a'b't + b'y_0 - a'b't = c' \tag{10}$$
$$a'x_0 + b'y_0 = c' \tag{11}$$

Portanto esse formato $x = x_0 + b't$, $y = y_0 - a't$ é solução. Agora precisamos verificar se toda solução possui esse formato.

Sabemos que mdc(a',b')= 1 na equação $a'x + b'y = c'$ e que (x_0, y_0) é uma solução particular então $a'x_0 + b'y_0 = c'$. Substituindo uma equação na outra temos:

$$a'x + b'y = a'x_0 + b'y_0 a'(x - x_0) = b'(y - y_0) \tag{12}$$

Isso implica dizer que $a' \mid b'(y - y_0)$, mas como o $mdc(a', b')$, então $a' \mid (y - y_0)$. Mesma análise nos leva a concluir que $b' \mid (x - x_0)$. Mas se isso ocorre podemos escrever:

$$(y - y_0) = a't \Rightarrow y = y_0 - a't \tag{13}$$
$$(x - x_0) = b's \Rightarrow x = x_0 + b's \tag{14}$$

Substituindo (13) e (14) em $a'x + b'y = c'$ teremos:

$$a'(x_0 + b's) + b'(y_0 - a't) = c' \tag{15}$$
$$a'x_0 + a'b's + b'y_0 - b'a't = c' \tag{16}$$
$$a'b's - a'b't + c' = c' \tag{17}$$
$$a'b's = a'b't \tag{18}$$
$$s = t \tag{19}$$

Portanto a solução sempre será do formato $x = x_0 + b't$ e $y = y_0 - a't$. □

Exemplo 21.

- *Dada a equação* $4x + 6y = 10$*, vamos encontrar as soluções se existirem.*
Como o $mdc(4, 6) = 2$ *e* $2 \mid 10$*,então a equação possui solução.Dividindo a equação pelo mdc teremos;* $2x + 3y = 5$*. Uma solução particular é* $x_0 = 1$ *e* $y_0 = 1$*.Baseando nos formatos de soluções* $x = x_0 + b't$ *e* $y = y_0 - a't$ *concluímos:*

$$x = 1 + 3t \text{ e } y = 1 - 2t$$

Substituindo valores para t, chegamos a quantas soluções quisermos, segue alguns exemplo: (-2;3),(1;1),(4;-1),(7;-3).

3.7 Criptografia

Criptografia é a técnina de escrita através de códigos com o intuito de transformar uma mensagem légivel em uma mensagem ilegível. O ato de criptografar uma mensagem chama-se de encriptação e o ato de desifrar uma mensagem chama-se descriptação. Para tal processo é necessário um chave (uma regra, um código) que é criada e fica em posse do emissor da mensagem. Caso ele queira, ele repassa ao receptor da mensagem, possibilitando que a mensagem seja decifrada. Existem várias maneiras de se criptografar uma mensagem, seja através de algoritmos simples de trocas de letras por números, ou até com o uso de algorítmos mais complexos que usam congruência modular e números primos. A aritmética modular trata de conceitos de divisibilidade e congruência que são trabalhados com conjunto dos números inteiros. O estudo da aritmética modular trabalha com módulo (mod) que segundo a comunidade Khan Academy é o operador que tem como objetivo conseguir o resto de uma divisão.

Este é um tema não abordado nos livros didáticos do Ensino Fundamental e Médio, porém é um tema muito interessante devido ao seu uso perceptível por todos nós no dia a dia. Um exemplo clássico é quando se inicia uma conversa nova no aplicativo de mensagens "Whastapp", em que aparece a seguinte mensagem : "Mensagens que você enviar para esta conversa e ligações agora são protegidas com criptografia de ponta-a-ponta, o que significa que elas não podem ser lidas ou ouvidas pelo "whastapp"ou por terceiros."

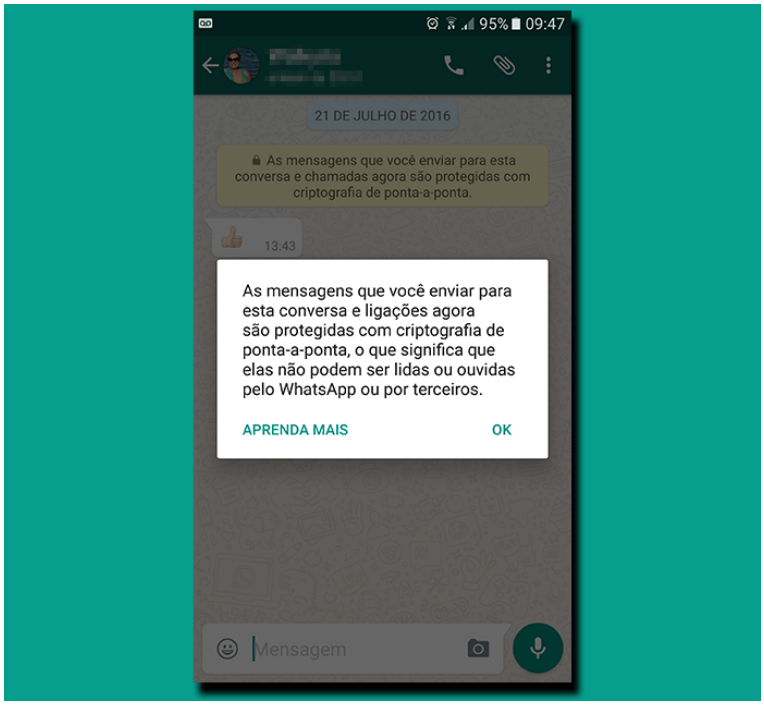


Figura 9: Nova conversa - Whastapp

Outro exemplo da necessidade do uso da criptografia são as transações bancárias, uma vez que, caso alguém intercepte a mensagem criptografada (transação) não seja possível decifrar as senhas. Um esboço da criptografia bancária está disponível no site do banco Santander.

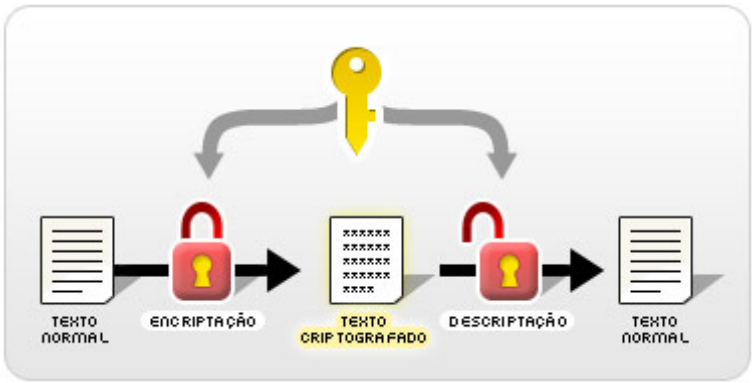


Figura 10: Modelo criptografia - Fonte: Banco Santander

3.7.1 Cifra de César

Cifra de César é uma das técnicas mais antigas que se tem notícia e foi utilizada por Júlio César (líder militar e político romano) para se comunicar com suas tropas durante as guerras que travava. O algoritmo da cifra é a troca de uma letra por outra em uma determinada posição. Ela é baseada no deslocamente de k unidades dentro do alfabeto, por exemplo:

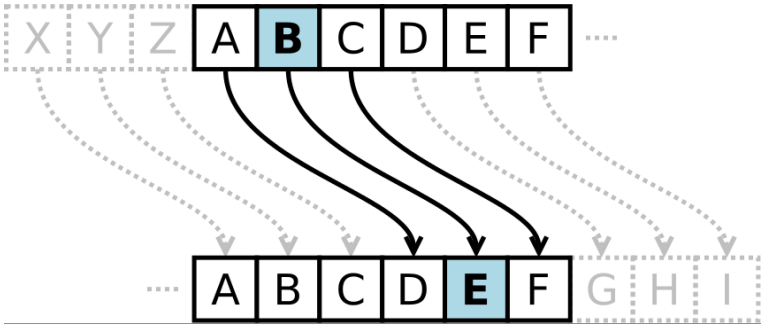


Figura 11: Exemplo - Cifra de César

No exemplo acima $K = 3$ uma vez que o B está sendo substituído por F.Portanto uma mensagem como:

Mensagem Original: ATACAR ROMA
Mensagem criptografada : DWDFDU URPD

Durante muito tempo a criptografia se resumiu à Cifra de César, porém estudiosos matemáticos desenvolveram técnicas para decifrar a cifra utilizando a frequência com que cada letra aparecia na mensagem critografada e relacionando com o estudo da frequência de cada letra nos textos em cada idioma. Como podemos ver as frequências das letras realmente permitiam tal análise.

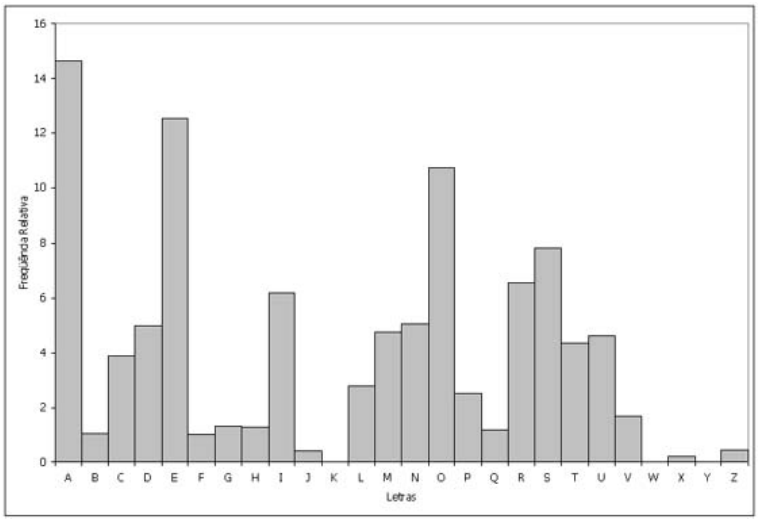


Figura 12: Frequência de cada letra em texto em português

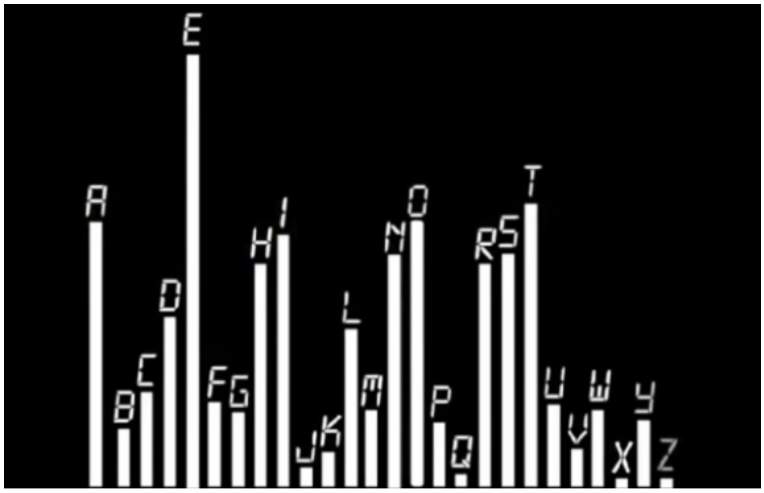


Figura 13: Frequência de cada letra em textos em inglês

3.7.2 Método RSA

Este método foi desenvolvido por três professores do Instituto de Tecnologia de Massachusetts (MIT), Ronald Rivest, Adi Shamir e Leonard Adleman, que utilizaram as letras de seus seus sobrenomes para dar nome ao método. Ele se baseia em um algorítmo que utiliza duas chaves: uma pública e outra privada. Para a criação das chaves citadas utiliza-se o estudo dos números primos e de congruência modular. O

estudo do método exige algum conhecimento prévio que ainda não foram apresentados neste trabalho como a definição Φ (leia-se *phi*) de Euller. De forma breve vamos definí-lo:

Definição 8. *Para um número natural n, a função Φ é definida como sendo igual à quantidade de números ,menores que n, coprimos em relação a ele. Defini-se ainda que dados dois números primos p e q, temos:*
$\Phi(p) = p - 1$
$\Phi(q) = q - 1$
$\Phi(p.q) = (p - 1)(q - 1)$

Exemplo 22. $\Phi(8) = 4$*, pois os números* $1, 3, 5, 7$ *são os números menores que* 8 *e coprimos a ele.*
$\Phi(5) = 5 - 1 = 4$
$\Phi(11) = 11 - 1 = 10$

O método RSA se resume nas seguintes etapas:

1) Pré codificar numericamente a mensagem;

2) Separar a mensagem em grupos b (desde que o valor de b seja menor do que a chave pública n), portanto $1 \leq b < n$;

3) Escolher dois números primos p e q e determinar a chave pública n de tal forma que $n = p.q$;

4) Escolher um expoente e (público e normalmente padronizado $e = 3$) de tal forma que $1 \leq e < \Phi(n)$ e que e e $\Phi(n)$ sejam coprimos;

5) Usar a regra de codificação : $b^e \equiv a \pmod{n}$, sendo que a será a mensagem criptografada.

Para o processo de decodificação da mensagem,já em posse da chave pública n, seguimos a regra: $a^d \equiv b \pmod{n}$. Sendo d o inverso de $e \pmod{(p-1)(q-1)}$, que significa dizer: $e.d \equiv 1 \pmod{(p-1)(q-1)}$ e b a mensagem original.

A método RSA é o mais utilizado no mundo, justamente pela segurança que ele proporciona às pessoas envolvidas. Essa segurança é adquirida principalmente pelo uso de números primos muito grandes para a construção da chave pública. O ato de decodificar a mensagem quando não se tem a chave privada envolve o processo de

fatoração da chave pública em busca dos números primos originais. Com a utilização de números primos muito grandes, essa chave se torna um número na ordem de 10^{100},e então a fatoração se torna impossível em tempo viável.

4 Descrição do projeto

O projeto foi desenvolvido em uma escola da rede particular durante três meses, um total de 10 encontros com duração de 90 minutos cada. Grande parte dessas questões foram discutidas, buscando aplicar o conteúdo ministrado no encontro, além de buscar várias formas de resoluções das mesmas questões, trazendo o aluno para o centro das discussões e assim agregando mais conhecimento a todos. Demonstraremos ao longo do capítulo como foram divididos os conteúdos em cada encontro e mostraremos alguns exercícios resolvidos em sala.

4.1 Encontros e exemplos

4.1.1 1º Encontro

Iniciamos com conteúdos que os alunos já dominavam, por isso nesse encontro preferimos trabalhar vários conteúdos e poucos exemplos. Os conteúdos ministrados foram:

1) Múltiplos, divisores e fatores;

2) Divisão euclidiana e análise dos restos (soma e subtração);

3) Números primos e compostos;

4) Critérios de divisibilidade.

Para ajudar na compreensão dos conteúdos, utilizamos os seguintes exercícios:

- Qual o resto da divisão $(40 + 26) : 6$ sem efetuar a soma que se encontra dentro dos parênteses? Explique seu raciocínio.
- Se somarmos todos os números de 1 à 587, qual o resto da divisão por 5?

- Determine se o número 3486 é divisível por 7 utilizando a regra de divisibilidade.
- O número $m = 488a9b$ é múltiplo de 45. Então o valor de $a + b$ é ?
- O número $N = 1111...11$, possui 2003 dígitos, todos 1. Qual o resto da divisão deste número por 7?
- Qual o dígito das unidades do número 3^{1998}?

Muitos alunos neste encontro se surpreenderam com os critérios de divisibilidade por 7, principalmente pelo fato de existirem dois critérios, sendo o primeiro apenas para verificar se é ou não divisível, e o segundo relacionando o resto da divisão por 7.

Durante a resoluções dos exemplos muitos alunos questionaram o fato de tal caso de divisibilidade não ser discutida em sala de aula durante o ano letivo tradicional. Ainda durante as discussões sobre as questões, no primeiro momento alguns alunos dos sextos anos sentiram dificuldade em trabalhar com pontências de expoente grande. Essa dúvidas foram sanadas com o acompanhamento mais individualizado.

4.1.2 2º Encontro

Neste segundo encontro discutimos os seguintes conteúdos:

1) Propriedades dos restos (multiplicação e divisão);
2) Cálculo do mmc e mdc;
3) Propriedade $mmc(a, b).mdc(a, b) = a.b$;
4) algoritmo de Euclides;
5) Mmc e mdc no GEOGEBRA.

Para ajudar na compreensão dos conteúdos utilizamos os seguintes exercícios:

- Qual o resto da divisão $(40.26) : 6$ sem efetuar o produto que se encontra dentro do parênteses? Explique seu raciocínio.
- Qual o resto da divisão $12^6 : 5$?
- Determine o mdc(80,36) de três maneiras diferentes, fatores individualizada, fatoração simultanea e pelo algoritmo de Euclides (fatoração sucessiva).

- Determine o valor de a sabendo que $b = 40$, $mdc(a, 40) = 10$ e o $mmc(a, 40) = 280$.

Focamos o trabalho nos dois últimos tópicos, até porque os alunos tinham muita facilidade com o cálculo de mmc e mdc. Ao chegarmos na propriedade destacada no item 3, muitos alunos se surpreenderam e questionaram o fato de tal propriedade não ser ensinada. Durante a resolução dos exercícios, os alunos não apresentaram dificuldades. Vale apenas registrar que a segunda questão gerou mais discussões em sala, já que alguns alunos haviam efetuado o cálculo 12^6 para em seguida efetuar a divisão por 5 e ao verificarem a resolução feita no quadro perceberam que poderiam encontrado apenas o resto da divisão $12 \div 5$ e elevá-lo a sexta potência conforme resolução abaixo.

Qual o resto da divisão $12^6 \div 5$?

$$12 \div 5 = 2 \text{ com resto } 2$$
Elevando o resto a quinta potência temos: $2^6 = 64$
E então: $64 \div 5 = 12$ com resto 4
Portanto o resto da divisão $12^6 \div 5$ é 4.

4.1.3 3º Encontro

Reservamos este encontro para a resolução de exercícios de vestibulares sobre o encontro passado, principalmente devido a importância do tema que é recorrente nas provas dos principais vestibulares do país. Mostraremos alguns exercícios discutidos em sala.

- (ACAFE SC) Um feirante deseja distribuir 576 goiabas, 432 laranjas e 504 maçãs entre várias famílias de um bairro carente. A exigência do feirante é que a distribuição seja feita de modo que cada família receba o mesmo e o menor número possível de frutas de uma mesma espécie. Qual a quantidade total de frutas recebida por cada família?

- (Unievangélica GO) Três barras de alumínio medem, respectivamente, 8m, 96m e 112m. Um serralheiro deseja cortá-las em pedaços de mesmo comprimento. Qual deverá ser esse comprimento, em metros, para que os pedaços tenham o maior tamanho possível?

- (UDESC SC) Qual a quantidade de números naturais que são divisores do mínimo múltiplo comum entre os números $a = 540$, $b = 720$ e $c = 1800$?
- (Unievangélica GO) Sendo x e y dois números naturais com $mdc(x, y) = 15$ e o $mmc(x, y) = 1575$ e sendo $x = 75$, qual o valor de y?
- (UEFS BA) Dados dois números naturais m e n, tais que $m.n = 720$, $mdc(m, n) = 6$ e $mdc(n, 20) = 4$, qual o valor de $m + n$?

Resolução do exercício 1 Devemos efetuar o mdc (576, 432, 504) através da fatoração simultânea, selecionando os números que dividem os três números simultaneamente.

576,	432,	504	2∗
288,	216,	252	2∗
144,	108,	126	2∗
72,	54,	63	2
36,	27,	63	2
18,	27,	63	2
9,	27,	63	3∗
3,	9,	21	3∗
1,	3,	7	3
1,	1,	7	7
1,	1,	1	

Portanto o mdc (576, 432, 504)= 72. Efetuando as divisões $576 \div 72$, $432 \div 72$ e $504 \div 72$ e somando chegará no número de 21 frutas, que é a resposta do problema.

Deixamos a cargo do leitor as outras resoluções.

4.1.4 4º Encontro

1) Aritmética Modular;

2) Congruência Modular;

3) Relação dos restos com congruência modular.

Iniciamos a apresentação do conteúdo trabalhando com o relógio e relacionando-o com a congruência módulo 12.

Como diz Prof. Ilydio Pereira de Sá:

"Aritmética do relógio trata-se de um caso de congruência, módulo 12 (nos relógios analógicos, é claro). Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5... e assim, sucessivamente."

Após apresentar os conteúdos listados e efetuar algumas demonstrações já apresentadas na seção 3.5, deixamos alguns exercícios para fixação do tema. Abaixo listamos alguns deles:

- Mostre que $47 \equiv 43 \pmod 4$.
- Usando congruência modular determine o resto de $7^{12} \div 4$ e $4^{15} \div 7$.
- Qual o resto da divisão $4^{555} \div 10$.

4.1.5 5º Encontro

Como podemos ver nas imagens abaixo,durante esse encontro resolvemos todos os exercícios deixados no encontro passado em sala, já que os alunos apresentaram dificuldades na assimilação dos conteúdos.

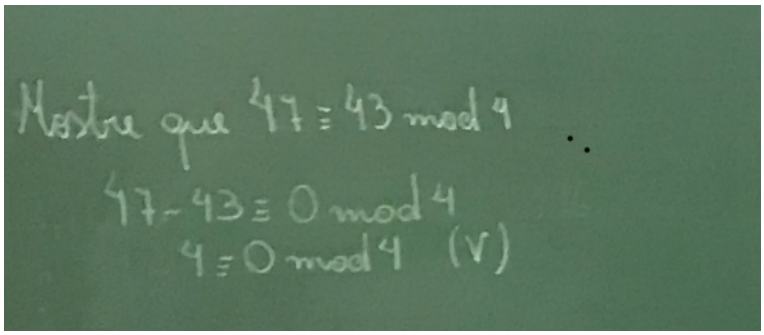


Figura 14: 5º Encontro - Exercício 1

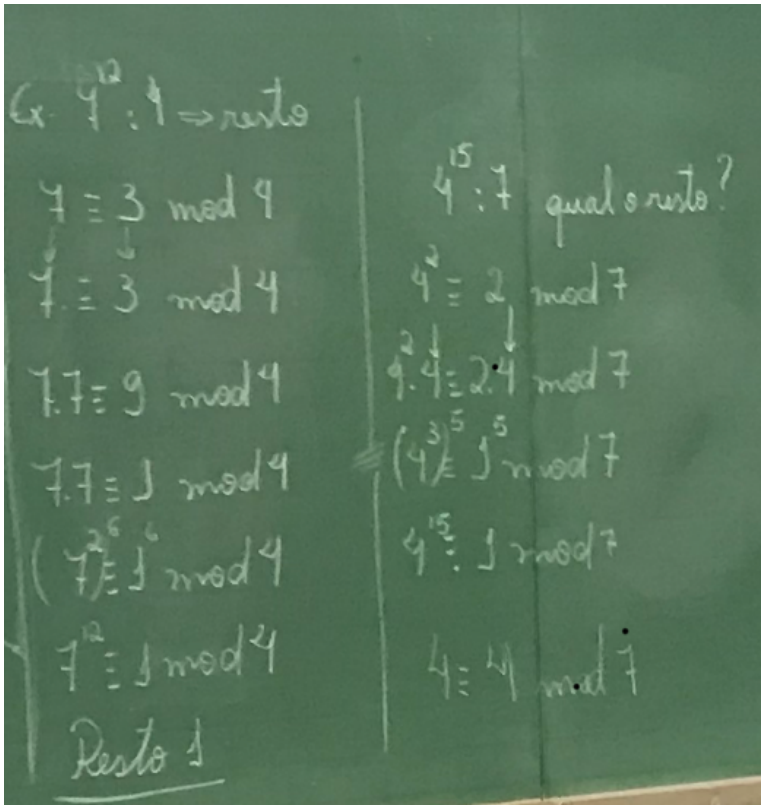


Figura 15: 5º Encontro - Exercício 2

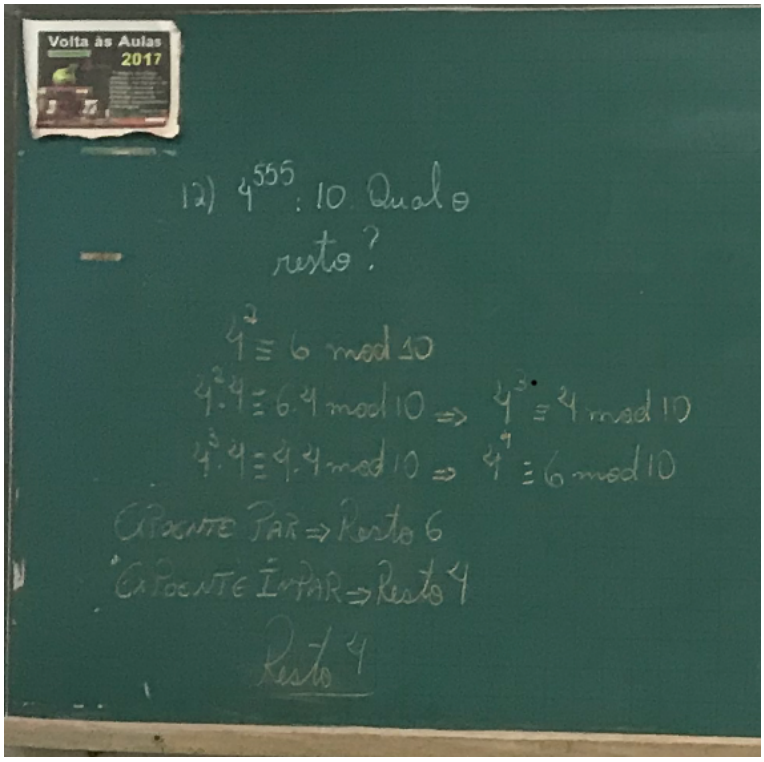


Figura 16: 5º Encontro - Exercício 3

4.1.6 6º Encontro

1) Equação diofantina;

2) Algorítmo de Euclides (relembrando);

Após expor os conteúdos iniciamos as discussões com os seguintes problemas:

- De quantas maneiras é possível comprar selos de 10 reais e de 14 reais gastando ao todo 100 reais?
- Determine todos os modos possíveis que podemos comprar selos de 5 reais e de 3 reais gastando 50 reais e comprando pelo menos um selo de cada valor.
- Determine o formato das soluções da equação : $56x + 72y = 40$.

Na primeira discussão o problema permitia encontrar solução mais triviais como por exemplo 10 selos de 10 reais e nenhum selo de 14 reais, o que facilitou as conclusões dos

alunos. Já na segunda discussão excluímos a possibilidade anterior e então os alunos apresentaram um pouco mais de dificuldade de chegar na solução. O terceiro exercício apresentado gerou muitos questionamentos, uma vez que não era fácil determinar uma solução particular e então os alunos tiveram que utilizar o algorítmo de Euclides para encontrar o $mdc(56, 72)$ e achar uma solução particular. Ao mostrar a possibilidade de simplificar a equação dividindo todos os termos por 8 muitos alunos conseguiram chegar à solução.

4.1.7 7º Encontro

Como o tema do encontro anterior era novo para os alunos, preferimos manter o tema neste encontro corrigindo alguns exercícios sobre equação diofantina. O exercício mais requesitado foi o terceiro citado acima, portanto vamos a solução discutida em sala.

Determine o formato das soluções da equação : $56x + 72y = 40$.

Solução: Calculando o $mdc(72, 56)$ pelo algoritmo de Euclides (divisões sucessivas).

$$72 = 56.1 + 16$$
$$56 = 16.3 + 8$$
$$16 = 8.2 + 0$$
$$8 = 56 - 16.3 = 56 - (72 - 56.1).3 = 56.4 - 72.3 = 56.(4) + 72(-3)$$

Temos: $40 = 8.5 = 56.(4.5) + 72.(-3.5) = 56.(20) + 72(-15)$.
Solução particular: $x_o = 20$ e $y_o = -15$.
Todas as soluções: $x = 20 + (72/8)t = 20 + 9t e y = -15 - (56/8)t = -15 - 7t$.
Resposta: $x = 20 + 9t$ e $y = -15 - 7t$

4.1.8 8º Encontro

Foi proposto aos alunos algumas discussões sobre o tema Criptografia. Após a apresentação de conceitos perguntamos se eles já haviam criptografado alguma mensagem, buscamos na memória deles algumas situações de suas infâncias em que eram feitas cartas com códigos e segredos. Na sequência apresentamos uma das formas de se criptografar através da sustituição das letras do alfabeto pelos números (Cifra de César).

Assim conseguimos de maneira bem sucinta apresentar os conteúdos e atrair a atenção dos alunos:

1) Criptografia;

2) Cifra de César;

3) Criptografando uma mensagem;

4) Descriptografando uma mensagem;

Ao final da aula os alunos criaram algumas mensagens criptografadas para que fossem coladas na escola com o intuito da discussão entre os demais alunos que não participaram do projeto. Abaixo podemos ver alguns exemplos:

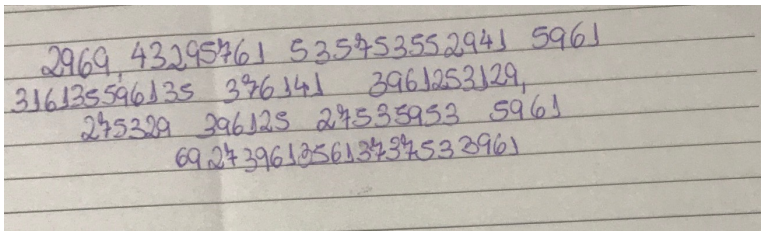


Figura 17: Cifra de César I

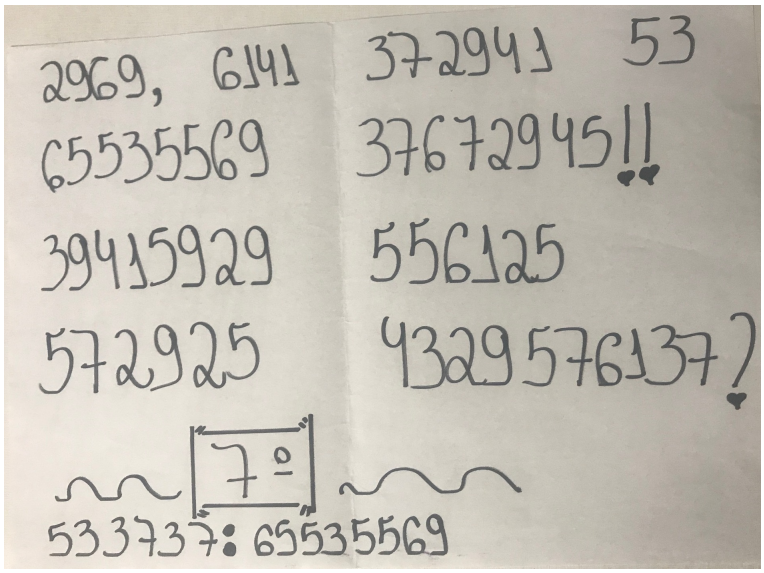


Figura 18: Cifra de César II

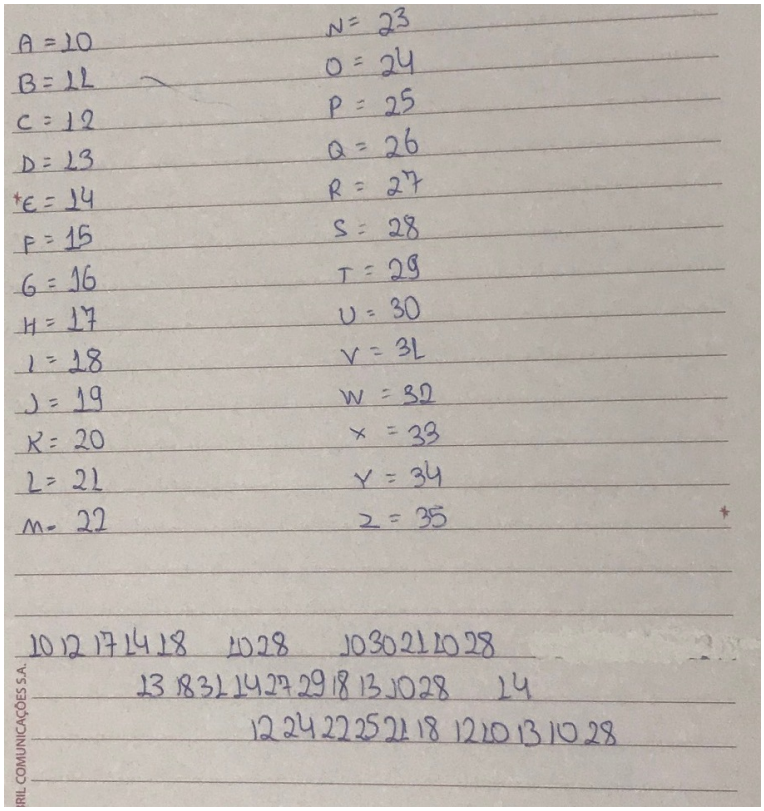


Figura 19: Cifra de César III

Em posse da chave número/letra deciframos as mensagens.

4.1.9 9º Encontro

Com o conceito de criptografia bem assimilado por todos os alunos, apresentamos situações em que a criptografia era usada, como por exemplo as transações bancárias e a troca de mensagens seja por email como por aplicativos de mensagens. Mostramos também que a segurança no mundo virtual exigia um método mais eficaz do que o apresentado anteriormente. Assim entramos no Métodos RSA apresentando três vídeo aulas que estão disponíveis no canal da OBMEP no youtube (Aritmética - Aula 65 - Apresentação do Método RSA e Aritmética - Aula 66 - Codificando uma mensagem e Aritmética - Aula 67 - Decodificando uma mensagem). Depois disso, resumimos o que foi explicado nos vídeos com o passo a passo do método RSA.

4.1.10 10º Encontro

Terminamos o projeto criptografando a palavra OMEG usando o método RSA, já que muitos alunos iriam realizar a prova da Olimpíada de Matemática do Estado de Goiás. Conforme segue o exemplo trabalhado em sala de aula:

Palavra à criptografar usando o método RSA: OMEG

Substituindo as letras do alfabeto por números usando a seguinte regra (4.1.8)

$$\text{A=10,B=11,C=12,D=13...Y=34,Z=35}$$

temos que a palavra OMEG pode ser escrita da seguinte forma: 24 22 14 16.

Tomando $e = 5$ e os números primos $p = 5$ e $q = 7$, determinamos o valor de $n = p.q = 5.7 = 35$. Para criptografar usaremos a fórmula ja definida: $b^e \equiv a \pmod{n}$.

$b_1^e \equiv a_1 \pmod{n}$	$b_2^e \equiv a_2 \pmod{n}$
$24^5 \equiv a_1 \pmod{35}$	$22^5 \equiv a_2 \pmod{35}$
$24 \equiv -11 \pmod{35}$	$22 \equiv -13 \pmod{35}$
$24^2 \equiv 121 \pmod{35}$	$22^2 \equiv 169 \pmod{35}$
$24^2 \equiv 16 \pmod{35}$	$22^2 \equiv -6 \pmod{35}$
$(24^2)^2 \equiv 256 \pmod{35}$	$(22^2)^2 \equiv 36 \pmod{35}$
$24^4 \equiv -24 \pmod{35}$	$22^4 \equiv 1 \pmod{35}$
$24^4.24 \equiv -24.(-11) \pmod{35}$	$22^4.22 \equiv 1.(-13) \pmod{35}$
$24^5 \equiv 19 \pmod{35}$	$22^5 \equiv 22 \pmod{35}$
$a_1 = 19$	$a_2 = 22$

$b_3^e \equiv a_3 \pmod{n}$	$b_4^e \equiv a_4 \pmod{n}$
$14^5 \equiv a_3 \pmod{35}$	$16^5 \equiv a_4 \pmod{35}$
$14 \equiv -21 \pmod{35}$	$16 \equiv -19 \pmod{35}$
$14^2 \equiv 441 \pmod{35}$	$16^2 \equiv 361 \pmod{35}$
$14^2 \equiv 21 \pmod{35}$	$16^2 \equiv 11 \pmod{35}$
$(14^2)^2 \equiv 21^2 \pmod{35}$	$(16^2)^2 \equiv 11^2 \pmod{35}$
$14^4 \equiv 441 \pmod{35}$	$16^4 \equiv 121 \pmod{35}$
$14^4 \equiv -14 \pmod{35}$	$16^4 \equiv -19 \pmod{35}$
$14^4.14 \equiv -14.(-21) \pmod{35}$	$16^4 \equiv -19.(-19) \pmod{35}$
$14^5 \equiv 294 \pmod{35}$	$16^5 \equiv 361 \pmod{35}$
$14^5 \equiv 14 \pmod{35}$	$16^5 \equiv 11 \pmod{35}$
$a_3 = 14$	$a_4 = 11$

Portanto a mensagem criptografada é representada pelos números: 19 22 14 11. Para o processo de decodificação da mensagem, já em posse da chave pública n, seguimos a regra: $a^d \equiv b \pmod{n}$. Sendo d o inverso de $e \pmod{(p-1)(q-1)}$, que significa dizer: $e.d \equiv 1 \pmod{(p-1)(q-1)}$ e b a mensagem original. Para nosso exemplo vamos decifrar o termo 19 e deixaremos os outros a cargo do leitor. Usando o processo descrito temos que: $e = 5$, $p = 5$, $q = 7$, $n = 35$ e $(p-1).(q-1) = 4.6 = 24$. Resolvendo a congruência $5.d \equiv 1 \pmod{24}$) temos que $d = 5$. Assim:

$$
\begin{aligned}
a_1^d &\equiv b_1 \pmod{n} \\
19^5 &\equiv b_1 \pmod{35}, Mas: \\
19 &\equiv -16 \pmod{35} \\
19^2 &\equiv 256 \pmod{35} \\
19^2 &\equiv 11 \pmod{35} \\
(19^2)^2 &\equiv 11^2 \pmod{35} \\
19^4 &\equiv 121 \pmod{35} \\
19^4 &\equiv -19 \pmod{35} \\
19^4.19 &\equiv -19.(-16) \pmod{35} \\
19^5 &\equiv 304 \pmod{35} \\
19^5 &\equiv 24 \pmod{35}
\end{aligned}
$$

Portanto o 19 na mensagem criptografada refere-se ao 24 na mensagem original, voltando a simbologia letra/número chegamos a letra O da palavra OMEG. Como vimos determinar os números primos que geraram a chave pública $n = 35$ é fundamental para decifrar a mensagem criptografada, no exemplo que usamos esse processo não é complicado, então buscamos encerrar o curso discutindo com os alunos o porque do método RSA ser tão eficiente pedindo a eles que determinassem os números primos que gerariam uma nova chave pública $n = 14.558.801$. Após breve discussão concluímos que seria inviável determinar tais números em pouco tempo, assim mostramos a solução: $p_1 = 4093$ e $p_2 = 3557$.

4.2 Cronograma

PROJETO ARITMÉTICA NO ENSINO FUNDAMENTAL

Etapa da Pesquisa	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Revisão bibliográfica		X	X	X	X	X	X	X				
Análise de livros didáticos			X	X	X							
Detalhamento do planejamento do projeto à coordenação pedagógica					X	X						
Análise dos boletins dos alunos								X				
Seleção de alunos e montagem das turmas								X				
Criação dos planos de ensino							X	X	X			
Primeiro contato com os alunos									X			
Aplicação do projeto									X	X	X	
Primeira atividade de assimilação de conteúdo										X		
Análise dos dados											X	X
Relatório final e atividade conclusiva												X

Figura 20: Cronograma do projeto

5 Considerações finais

Quando iniciamos as reuniões para adequação do projeto junto à escola muitos questionamentos surgiram, como: "É possível trabalhar junto com alunos das 4 séries ao mesmo tempo?", "Os alunos irão se interessar pelo formato proposto pelo projeto?", "Como será o desempenho dos alunos, principalmente dos alunos dos 6º e 7º anos?", "Porque muitos temas não são trabalhados no Ensino Fundamental?","Apresentar questões de vestibulares a alunos tão novos não seria loucura?", "Será que é possível fugir do tradicional e mostrar que temas do cotidiano dos alunos são fruto de estudos matemáticos ?".

Durante os dois primeiros encontros percebemos que os alunos dos 6º e 7º anos se desenvolveram com bastante facilidade e o restante nem tanto, já que muitos não se lembravam das algumas técnicas para o cálculo do mmc e do mdc e principalmente do uso do algoritmo de Euclides. Neste momento notamos que a interação dos alunos, mesmo com idades diferentes, alunos de 10/11 anos ajudando alunos com 14/15 anos, gerou momentos de bastante apredizado, mantivemos essa interação durante todo o projeto. Um destaque importante é que mesmo os alunos mais tímidos e retraídos conseguiram se relacionar com os demais, pois viam que os colegas precisavam de ajuda na resoluções das questões propostas. Ainda nesses encontros apresentamos a propriedade $mmc(a,b).mdc(a,b) = a.b$ e a fórmula para o cálculo do números de divisores de um número. Algo bastante interessante foram dois questionamentos que logo viraram discussão em sala : "porque nos ensinam mmc, mdc, que é a parte mais difícil e ninguém nos ensina essa propriedade, que é tão fácil de usar?", "então agora posso encontrar os divisores e conferir se não esqueci nenhum com essa fórmula?".

A partir do terceiro encontro, quando começamos a trabalhar com questões de vestibular notamos um choque inicial, já que nos livros para alunos dessa faixa etária não é comum aparecer questões de vestibulares, em seguida um relaxamento já que alguns alunos comentaram que não acharam as questões tão complicadas. Em determinado momento um aluno do 8º ano até comentou: "professor passei unievangélica", após resolver uma das questões propostas, gerando risos e comentários dos demais colegas. A satisfação de conseguir resolver questões de vestibular era evidente, deixando claro o quanto trazer desafios para alunos de qualquer faixa etária é importante.

No quarto encontro (apresentação do conteúdo de Aritmética Modular) as surpresas foram maiores. Como já dito iniciamos o conteúdo levando para sala de aula um relógio analógico e discutimos a congruência modular módulo 12, esse fato fez com que a turma

não demonstra-se espanto com tal conteúdo, já a apresentação de demonstrações causou espanto total. Essa situação nos forçou ainda mais a fugir de demontrações nos demais temas pois sentimos que os alunos daquela faixa etária não tinham maturidade para acompanhá-las. Contornamos a situação resolvendo muitas questões no quinto encontro para não deixar que o susto com as demonstrações gerasse desistência do curso. Já nos encontros 6 e 7 apresentamos os conteúdos de forma mais prática, com resolução de exercícios mais dinâmicos e com menos parte algébrica.

Nos encontros de 8 a 10 podemos perceber o quão importante é trazer para sala de aula assuntos do dia a dia dos alunos. Durante uma atividade a turma produziu mensagens criptogradas usando a cifra de César, neste momento percebemos a mudança de astral da aula, a empolgação em discutir o tema aumentou consideravelmente facilitando o ensino da parte mais complicada do conteúdo de criptografia (método RSA), principalmente quando apresentamos os métodos para decifrar as mensagens. Vale resaltar que muitos alunos tentavam entender o porque do método funcionar com tanta aceitação no mercado. Ao utilizar números primos grandes ficou evidente a dificuldade para decifrar uma mensagem quando utilizado o método RSA, alguns alunos comentaram: "nossa professor, aí é impossível decifrar". Ainda nestes encontros como já citado orientamos os alunos a assitir vídeo - aulas sobre o tema, o que gerou bons resultados, já cerca de 7 alunos da turma (turma de 20 alunos) conseguiram conceituar e exemplificar o assunto estudado apenas através dos vídeos, o que para uma primeira atividade consideramos bom resultado.

De forma mais sucinta percebemos que o alguns resultados apresentados no Ensino Médio podem ser discutidos já no Ensino Fundamental mesmo não aparecendo em livros principalmente pelo fato de alguns resultados serem muito imediatos de assuntos já estudados. Analisando na prática em sala de aula durante o projeto constatamos que cerca de 90 % dos alunos conseguiram resolver a parte I dos exercícios propostos (em anexo) e por volta de 70% não tiveram dificuldade na parte II dos exercícios propostos. Mediante o contato mais próximo com estes alunos notamos que às vezes subestimamos a inteligência deles simplesmente pelo fato do conteúdo não ser apresentado no livro didático daquela série. Ficou claro ainda a importância de se mostrar o caminho para o estudo independente dos alunos, através de vídeo aulas, busca por livros de outros autores e materiais na internet. Por fim destacamos o papel do professor durante a preparação das aulas em buscar a aplicabilidade do assunto a ser trabalhado com o dia a dia dos alunos, algo que prende muito a atenção dos mesmos facilitando a apresentação de temas mais complexos, no caso do nosso projeto notamos o quando

facilitou a apresentação de um tema de nível mais elevado como é o caso da congruência modular no método RSA quando trouxemos o relógio e a criptografia para sala de aula.

Propomos com o resultado deste projeto alterar a forma superficial e sem aplicabidade de se ensinar matemática fazendo com que o professor não fique preso na sequência e no conteúdo que os livros propõem. Buscamos refletir sobre a importância de trazer mais discussões para a sala de aula e não só depender das aulas tradicionais (exposição direta do conteúdo), para que o aluno seja sempre o centro das atenções e assim limitar o papel do professor em despertar nos alunos o quanto a matemática está presente no seu cotidiano, desafiando-os, seja com conteúdos de séries seguintes como com questões de vestibulares e olimpíadas nacionais e internacionais. Citamos neste trabalho apenas um caso em que a aplicabilidade permitiu prender a atenção do aluno, cabe então ao professor buscar sempre a aplicabilidade fazendo com que o aluno acredite na importância do tema no seu dia a dia.

6 Anexos

Projeto Aritmética Modular no Ensino Fundamental
Plano de Aula I

Data:20/09/2017

Sequência Didática: Múltiplos, divisores e fatores.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.
Metodologia: Primeiramente recordaremos alguns conceitos pré existentes nos conteúdos. Em seguida, os alunos irão construir o crivo de Eratóstenes identificando os números primos e compostos para a construção dos divisores de um número. Por fim o conceito de Divisão Euclidiana será enunciado e detalharemos os critérios de divisibilidade, dando ênfase aos critérios não convencionais como é o caso da divisibilidade por 7 e 11 e a divisibilidade por números compostos.

Recursos Didáticos: Folha de papel e caneta.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula II

Data:27/09/2017

Sequência Didática: Máximo Divisor Comum e Mínimo Divisor Comum.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Iniciaremos a aula com uma breve análise das propriedades dos restos do produto de dois números encerrando o tema da aula passada. Discutiremos as formas variadas dos cálculos de mdc e mmc: por decomposição em fatores primos, método do algoritmo de Euclides e o método da divisão sucessiva. Executaremos alguns exercícios para concluir o seguinte fato: “dados dois números naturais, seu produto é igual ao produto do seu mmc e pelo seu mdc."Por fim aproveitaremos para mostrar aos alunos uma análise gráfica do mmc e mdc com o uso do software livre GEOGEBRA.

Recursos Didáticos: Folha de papel e caneta.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula III

Data:04/10/2017

Sequência Didática: Múltiplos, divisores e fatores

Máximo Divisor Comum (mdc) e Mínimo Divisor Comum (mmc).

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Resolução de exercícios de vestibulares para a fixação de conteúdos propostos nos encontros anteriores.

Recursos Didáticos: Folha de papel e caneta.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula IV

Data:11/10/2017

Sequência Didática: Aritmética Modular.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Durante a semana que antecede a aula, os alunos serão alertados da importância dessa aula para o decorrer do curso. Após a correção de exercícios propostos na aula passada, discutiremos a seguinte afirmação matemática: $7 + 6 = 1$.Enunciaremos e demosntraremos os conceitos de congruência modular e classe de equivalência, por fim resolveremos vários exercícios do tipo : 47 é congruente à 43 (mod 4) ? Qual o resto da divisão $7^{12} : 4$?

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula V

Data:18/10/2017

Sequência Didática: Aritmética Modular;

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Será trabalhado uma lista de exercícios composta por exercícios de nível olímpico e questões dos vestibulares das principais universidades do país como FUVEST, UNB, UFG, além de questões do ENEM.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula VI

Data:25/10/2017

Sequência Didática: Equações Diofantinas.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Iniciaremos a aula com uma equação diofantina (sem citar tal nomenclatura) com o intuito que os alunos descubram algumas soluções. Depois disso discutiremos outra equação diofantina, porém essa uma equação sem solução.Feito isso demosntraremos o motivo pelo qual uma equação diofantina tem ou não solução. Discutiremos a exeistência de solução de algumas equações.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e para preparação para a Olimpíada do Estado de Goiás (OMEG).

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula VII

Data:01/11/2017

Sequência Didática: Equações diofantinas.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Resolveremos exercícios como por exemplo: De quantas maneiras é possível comprar selos de 10 reais e de 14 reais gastando ao todo 100 reais? Determine o formato das soluções da equação : $56x + 72y = 40$.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e para preparação para a Olimpíada do Estado de Goiás (OMEG).

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula VIII

Data:08/11/2017

Sequência Didática: Criptografia.

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Correção das atividades da aula anterior de equação Diofantina. Iniciaremos o estudo lendo a mensagem que aparece quando se inicia uma nova conversa no aplicativo "whatsapp".Depois disso execreveremos no quadro uma mensagem criptografada – 112422 131810 – Bom dia. Em seguida conceituaremos criptografia citando vários exemplos. Assim iremos decifrar a mensagem inicial.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula IX

Data:22/11/2017

Sequência Didática: Criptografia (Cifra de César).

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Apresentaremos alguns códigos como: Código de César, Código de Chave Pública e Criptografia RSA. Apresentaremos técnicas de decodificação desses códigos. Concluiremos o projeto com uma atividade criptografada pelos alunos que será apresentada à escola.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

Plano de Aula X

Data:29/11/2017

Sequência Didática: Criptografia (Método RSA.)

Competências e Habilidades: A atividade proposta visa promover a integração dos alunos de todas as séries do Ensino Fundamental II. Em todo o curso buscaremos contemplar aspectos originais da Matemática que por diversos motivos não se encontram nos livros didático. Além do que, com a realização de tal atividade espera-se que os alunos desenvolvam a rapidez e o raciocínio lógico na realização de problemas matemáticos de nível olímpico.

Metodologia: Mostraremos alguns vídeos explicando o método RSA, em seguida iremos criptografar a mensagem OMEG (olimpíada do estado de Goiás) e na sequência decifrar a mensagem criptograda. Por fim mostraremos o porque do método funcionar com tanta precisão.

Recursos Didáticos: Folha de papel, caneta, data show e notebook.

Avaliação: O material produzido servirá como base para o desenvolvimento do aluno no decorrer do curso e não como uma forma de avaliação.

Bibliografia: Programa de Iniciação Científica da OBMEP – Módulo 1 – Divisibilidade e números inteiros. Vídeo aulas – Portal da Matemática - https://matematica.obmep.org.br.

Assinatura do Professor	Assinatura da Coordenação

1) (IFPE/2016) Mariana estava na casa de sua amiga, Karine, e precisou ter acesso a sua rede wifi. Na parede da sala, encontrava-se uma plaquinha com a senha de 6 dígitos que ela precisaria para ter esse acesso.

Senha WIFI:
214_37

Mariana percebeu que faltava um dos dígitos na senha e perguntou a Karine que dígito seria esse. Sua amiga, então, lhe lançou um desafio, dizendo-lhe que a senha completa é múltiplo de nove. Assim, Mariana descobriu que o número que faltava seria:

a)9. b)1. c)3. d)2. e)6.

2) (UNITAU SP/2015) Sabendo-se que n é um número natural e diferente de zero, e que sua divisão por 3 não é exata, é CORRETO afirmar que o resto da divisão de n^2 por 3 é

a)0 b)1 c)2 d)3 e)não é possível determinar

3) (FGV /2016) O resto da divisão do número 6^{2015} por 10 é igual a

a)4. b)5. c)6. d)8. e)9.

4) (IFMA/2016) Dadas as afirmativas:

I. Todo número par é divisível por 2.
II. Todo número ímpar é divisível por 3.
III. Todo número é divisível por 10 quando termina em 0 ou 5.
IV. No calendário do mês de maio há mais números divisíveis por 9 do que por 10.
V. Existe um número natural que é divisível por 2, 3, 5 e 9 ao mesmo tempo.
Quais as afirmativas verdadeiras?

a) III e IV b)II e V c)I e V d)II e IV e)III e V

5) Calcule mmc (15,20), a partir da informação de que mdc (15,20) = 5

6) Se o MMC (A,B)=90 e A.B=1350, então o MDC (A,B) é igual a?

7) (Unicamp) Sejam a e b dois números inteiros positivos tais que mdc(a,b) = 5 e o mmc(a,b) = 105.

a) Qual é o valor de b se a = 35?
b) Encontre todos os valores possíveis para (a,b).

8) (IFSC/2015)Em uma loja existe três relógios cucos desregulados. O primeiro toca o cuco a cada 12 min, o segundo a cada 22 min e o terceiro a cada 39 min. Se os três cucos tocaram juntos às quinze horas da tarde, é CORRETO afirmar que eles tocarão juntos novamente:

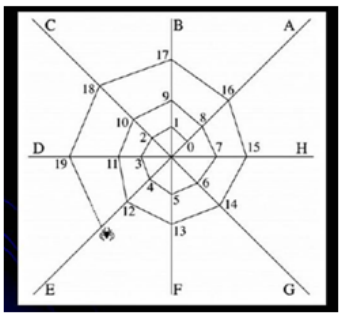
a) Às 19 horas e 32 minutos do mesmo dia.
b) Somente às 4 horas e 28 minutos do dia seguinte.
c) Às 16 horas e 32 minutos do mesmo dia.
d) Somente às 2 horas e 44 minutos do dia seguinte.
e) Somente às 19h e 36 min do dia seguinte.

9) (Unievangélica GO/2015) Três barras de alumínio medem, respectivamente, 8m, 96m e 112m. Um serralheiro deseja cortá-las em pedaços de mesmo comprimento.Qual deverá ser esse comprimento, em metros, para que os pedaços tenham o maior tamanho possível?

a) 8 b)2 c)4 d)6

10) (OBMEP) A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura abaixo. A aranha continua seu trabalho... As perguntas são: sobre qual fio de apoio estará o número 118? E o número 9.999?

Figura 21: Lista de exercícios - parte I



11) Vamos supor que você saiba em qual dia da semana caiu o dia 1º de janeiro de um determinado ano. Em 2006, por exemplo, foi um domingo. Imaginemos que você deseja saber quando cairá um outro dia qualquer (vale para qualquer ano). Verificamos (veja texto no final da lista) aqui que estamos diante de um caso de congruência, módulo 7 nesse caso. Digamos que estivéssemos interessados em descobrir em que dia da semana caiu o dia 5 de julho (e não temos um calendário em mãos, é claro).Qual dia da semana caiu então o dia 5 de julho?

12) Ache o resto da divisão de 4^{555} por 10.

13) Prove que : $2^{70} + 3^{70}$ divisível por 13.

14) O número 2^{255} é divisível por 3?

15) (OBM – 2003) Seja n = 9867 . Se você calculasse $n^3 - n^2$, você encontraria um número cujo algarismo das unidades é:

A) 0 B) 2 C) 4 D) 6 E) 8
Gab: C

16) Achar todos os inteiros x tais que $0 < x < 15$ e $3x \equiv 6 \pmod{15}$

17) Mostrar que $11^{10} \equiv 1 \pmod{100}$.

18) O ano de 2013, começou em uma terça-feira. Qual o dia da semana termina o ano?
R: Terça-feira

19) Sabendo que o 2013 começou em terça-feira, qual dia da semana será 1º de janeiro de 2016?
R: Sexta- feira

20) Sabendo que o 2013 começou em terça-feira, qual dia da semana será 31º de dezembro de 2016?
R: Sábado

Figura 22: Lista de exercícios - parte II

Referências

[1] Moreira, M.a. e Rosa, p,r,s. , *Pesquisa em ensino:métodos qualitativos e quantitativos.*, Porto Alegre 2009/2016.

[2] Franco, t.r.r., *Divisibilidade e Congruências: Aplicações no Ensino Fundamental II*, 2016, Profmat-UFG.

[3] Sa, I.p., *A aritmética modular e suas aplicações no cotidiano.*Disponivel em <amagiadamatematica.com.br>.

[4] Hefez, a., *Aritmética*, 1ª Edição. Rio de Janeiro: SBM,2013.

[5] Tripp, d., *Pesquisa-ação: uma introdução metodológica*, 2005, Universidade de Murdoch, pp 446.

[6] Jurkiewicz, s., *Divisibilidade e Números Inteiros: Introdução à Aritmética Modular.*Disponível em www.obmep.org.br .

[7] Rech, a.j.d e Freitas, s.n *O papel do professor junto ao aluno com Altas Habilidades*, Revista Educação Especial (2005) nº 25 disponível em https://periodicos.ufsm.br/educacaoespecial/article/view/4904.

[8] Giovanni, j.r , Giovanni Jr, j.r e Castrucci, b *A conquista da Matemática-9º Ano*, São Paulo, FTD, 2015.

[9] Giovanni, j.r , Giovanni Jr, j.r e Castrucci, b *A conquista da Matemática-8º Ano*, São Paulo, FTD, 2015.

[10] Giovanni, j.r , Giovanni Jr, j.r e Castrucci, b *A conquista da Matemática-7º Ano*, São Paulo, FTD, 2015.

[11] Giovanni, j.r , Giovanni Jr, j.r e Castrucci, b *A conquista da Matemática-6º Ano*, São Paulo, FTD, 2015.

[12] SHOKRANIAN, s., *Criptografia para Iniciantes.* , Brasília: UNB, 2005.