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

Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma proposta focada na Resolução de Problemas

Débora Danielle Alves Moraes Priebe

Goiânia

2016

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS 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: Débora Danielle Alves Moraes Priebe

Título do trabalho: Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma Proposta focada na Resolução de Problemas

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.

Débora Danielle Alves Moraes Priebe

Assinatura do (a) autor (a) [2] Data: 08/12/2016

[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.

[2] A assinatura deve ser escaneada.

Débora Danielle Alves Moraes Priebe

Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma proposta focada na Resolução de Problemas

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: Profª Drª Lidiane dos Santos Monteiro Lima

Goiânia

2016

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

Priebe, Débora Danielle Alves Moraes
Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma proposta focada na Resolução de Problemas [manuscrito] / Débora Danielle Alves Moraes Priebe. - 2016.
LXXIV, 74 f.: il.

Orientador: Profa. Dra. Lidiane dos Santos Monteiro Lima.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), Programa de Pós-Graduação em Matemática, Goiânia, 2016.
Bibliografia.
Inclui símbolos, tabelas, lista de figuras.

1. Teoria dos Números. 2. Ensino Fundamental. 3. Divisibilidade. 4. Congruência. 5. Resolução de Problemas. I. Lima, Lidiane dos Santos Monteiro, orient. II. Título.

CDU 511

Débora Danielle Alves Moraes Priebe

"Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma Proposta focada na Resolução de Problemas"

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 07 de dezembro de 2016, pela Banca Examinadora constituída pelos professores:

Profª. Drª. Lidiane dos Santos Monteiro Lima
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Mário José de Souza
Instituto de Matemática e Estatística - UFG

Prof. Dr. José Eder Salvador de Vasconcelos
Membro Externo – IFG/GOIÂNIA

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 da aluna Débora Danielle Alves Moraes Priebe – Aos sete dias do mês de dezembro do ano de dois mil e dezesseis (07/12/2016), às 09:30 horas, reuniram-se os componentes da Banca Examinadora: Prof.ª. Drª. Lidiane dos Santos Monteiro Lima – Orientadora; Prof. Dr. Mário José de Souza e José Eder Salvador de Vasconcelos, para, sob a presidência do primeiro, e em sessão pública realizada no Auditório do IME, procederem a avaliação da defesa intitulada: **"Tópicos de Aritmética para as séries finais do Ensino Fundamental: Uma proposta focada na Resolução de Problemas"**, em nível de Mestrado, área de concentração Matemática do Ensino Básico, de autoria de Débora Danielle Alves Moraes Priebe discente do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás. A sessão foi aberta pela Presidente da banca, Prof.ª. Drª. Lidiane dos Santos Monteiro Lima, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida a autora do TCC que, em 30 minutos procedeu a 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 a avaliação da defesa. Tendo-se em vista o que consta na Resolução nº. 1075/2012 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 11:00 horas a presidência da mesa encerrou a sessão e para constar, eu, Sonia Maria de Oliveira, secretária do PROFMAT/UFG, lavrei a presente Ata que, depois de lida e aprovada, é assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Prof.ª. Drª. Lidiane dos Santos Monteiro Lima
Presidente – IME/UFG

Prof. Dr. Mário José de Souza
Membro – IME/UFG

Prof. Dr. José Eder Salvador de Vasconcelos
Membro – IFG/GOIÂNIA

Débora Danielle Alves Moraes Priebe graduou-se em Matemática pela Faculdade Alfredo Nasser no ano de 2012.

Dedico este trabalho ao Senhor Deus em nome do seu filho Jesus e aos meus pais.

Agradecimentos

Agradeço primeiramente ao Senhor Deus, o pai da Matemática, que criou um Universo perfeito e precisamente calculado e deu ao ser humano a luz de Sua sabedoria para compreender os mistérios dessa incrível ferramenta por Ele utilizada na criação de tudo. A Deus agradeço pela oportunidade de ter cursado este mestrado e mesmo diante das dificuldades que apareceram no caminho, agradeço por ter me carregado em Seus braços, por ter me dado forças e sabedoria para vencer cada etapa e ter permitido que eu chegasse ao fim dessa jornada como vencedora.

Agradeço a minha melhor e verdadeira amiga, minha mãe, por sua proteção e companhia em todos os momentos de minha vida. Agradeço a ela por todo apoio que sempre me deu nessa trajetória, em qualquer que fosse minha decisão; pela confiança que sempre pude encontrar nela e pela tranquilidade que me passa em saber que sempre posso contar com seu auxílio. Agradeço por ter participado dessa caminhada ao meu lado e por toda ajuda e compreensão que despendeu em meu favor. Enquanto muitos chamavam seus cuidados de desnecessários ou exagerados, ela os chamava de amor, e é esse amor que me trouxe até aqui e que me torna cada dia melhor. Posso dizer que olhando para o tamanho de seu amor por mim, consigo imaginar a grandeza do amor de Deus. Mãe, esta vitória também é sua!

Agradeço ao meu pai, que sempre esteve disposto a ajudar, muitas vezes sacrificando seu tempo. Agradeço pela compreensão com os longos dias de estudo e silêncio em casa, pela sua força e presença durante esta batalha.

Aos meus colegas da turma 2015 do PROFMAT de Goiânia agradeço por terem me mostrado a importância da união. Neste mestrado tive a oportunidade de conhecer pessoas incríveis, nobres e que foram muito importantes no decorrer desta caminhada. Agradeço especialmente ao colega Marcelo Rigonatto por sua nobreza de espírito em praticar a caridade e ao colega Davi Lessa de Oliveira por compartilhar seus conhecimentos, dispendendo de seu tempo para auxiliar nos momentos mais difíceis de nosso aprendizado.

Ao mestre Bruno César Sá da Silva (Bruno Glasses) um agradecimento especial por todas as contribuições feitas aos alunos do PROFMAT no intuito de auxiliar na

árdua tarefa de tornarmos mestres. Agradeço também aos colegas José Ivelton Siqueira Lustosa (Bonito de Santa Fé - PB), João Mendes Barroso Filho (Fortaleza - CE), Mariel de Paula Chaves, Walas da Silva Santos, Bruno Astrolino e Silva, e todos aqueles que mesmo sem me conhecer estavam sempre dispostos a ajudar, resolvendo problemas, disponibilizando materiais e trocando informações. Vocês foram meus professores virtuais.

À minha orientadora, Profª. Drª. Lidiane dos Santos Monteiro Lima, agradeço por ter aceitado a tarefa de me orientar no desenvolvimento deste trabalho e por toda paciência e sabedoria demonstrados durante este período.

Ao Prof. Dr. Mário José de Souza agradeço por todo o incentivo, apoio e demonstração de fé, que me tornaram mais forte e confiante.

Agradeço a todos os professores que tive a oportunidade de conhecer durante este curso pelo excelente trabalho desenvolvido.

A teoria dos números é uma pedra angular que sustenta uma apreciável porção do edifício matemático. E, claro, também é divertida.

Terence Tao

Os professores são os melhores embaixadores para o belo reino da matemática.

Alfred Posamentier

Resumo

Este trabalho tem como objetivo apresentar uma proposta de ensino de alguns tópicos de Aritmética, também denominada de Teoria dos Números, às séries finais do Ensino Fundamental, com foco na resolução de problemas, visando desafiar e fascinar os alunos com a gama de possibilidades oriunda das propriedades da Teoria dos Números e desenvolver sua capacidade de raciocínio através de problemas interessantes que darão uma nova vida ao assunto. O leitor encontrará neste trabalho tópicos de divisibilidade, primos, Máximo Divisor Comum, Mínimo Múltiplo Comum, Algoritmo de Euclides, congruências, representação decimal, testes de divisibilidade, além de diversos exemplos, problemas desafiadores e também curiosidades acerca da congruência módulo 9.

Palavras-chave

Teoria dos Números, Aritmética, Ensino Fundamental, Resolução de Problemas, Divisibilidade, Congruência Modular

Abstract

This paper aims to present an educational proposal of some topics of arithmetic, also called Number Theory, for the final grades of elementary school, focusing on solving problems to challenge and entertain students with the range of possibilities arising from properties of Number Theory and develop their thinking skills through interesting problems that will give a new life to the subject . The reader will find in this work topics of divisibility, primes, Greatest Common Divisor, Least Common Multiple, Euclidean Algorithm, congruences, decimal representation, divisibility tests, as well as several examples, challenging problems and also curiosities about the congruence module 9.

Keywords

Number Theory , Arithmetic, Elementary Education, Problem Solving, Divisibility, Congruence Modular

Lista de Figuras

Sumário

Introdução

A Teoria dos Números, também denominada de Aritmética, é considerada por muitos a rainha da matemática e é um ramo antigo e importante que estuda as propriedades dos números inteiros.

Todavia, como pode ser observado em algumas escolas, nas séries finais do Ensino Fundamental o ensino de tópicos de Aritmética é feito de maneira superficial e mecânica, não permitindo que os alunos desenvolvam sua capacidade de raciocínio na resolução de problemas. A falta de contextualização e aplicação em questões incomuns também contribuem para desestimular os alunos com relação ao gosto pela Aritmética.

Conforme [11], usar os números sem nunca parar para observar algumas de suas propriedades incomuns é como caminhar em um jardim sem parar para cheirar as flores. Apresentar aos alunos algumas dessas propriedades permitirá que tenham um maior apreço por esses símbolos. O autor afirma que muitas vezes a matemática é ensinada como um campo seco e necessário de instrução. Como professores, temos a obrigação de torná-la interessante. Apresentar algumas propriedades e curiosidades darão uma nova vida ao assunto.

Os professores devem seduzir os jovens em direção a um amor por este assunto magnífico, afirma [11]. Todavia os professores precisam de ideias para motivar os seus alunos através de um material apropriado e divertido.

A Revista Eureka! ([12]), reconhecendo a importância de um material que estimule a criatividade dos alunos através da resolução de problemas, afirma que

> *A cada ano, livros novos são editados repetindo quase sempre o mesmo estilo e os mesmos conteúdos dos anteriores. Existem hoje no Brasil bons livros de Matemática dedicados aos alunos tanto do ensino fundamental quanto do ensino médio. Entretanto, o que lhes falta é um ingrediente que, no mundo de hoje, é fundamental: o estímulo à criatividade. Entendemos que não é suficiente para a formação do futuro cidadão um aprendizado burocrático da Matemática e percebemos a importância de estimular os alunos desde a tenra idade a resolver problemas novos e desafiantes, propiciando o desenvolvimento da imaginação e da criatividade.*

Com este trabalho pretende-se contribuir com uma proposta para o ensino de tópicos de Aritmética nas séries finais do Ensino Fundamental de modo a estimular nos alunos a capacidade de resolver problemas, estruturando seu pensamento algébrico de forma a evitar a prática repetitiva, muito comum em alguns livros textos. Com isso, a proposta deste trabalho é quebrar o ciclo historicamente praticado de ensinar aritmética de forma superficial e mecanicista. Mesmo que alguns estudantes dominem e memorizem os algoritmos para cálculos que atualmente são ensinados, o que realmente torna-se importante para o aprendizado é a real compreensão do significado dos conceitos, que desenvolve-se através da interpretação de problemas.

Segundo [14], "as aplicações que derivam dos conceitos básicos de inteiro e divisibilidade são de um poder e diversidade espantosos". Com isso, buscaremos explorar esta diversidade no intuito de aguçar a curiosidade e o interesse dos estudantes e buscar a interação entre a teoria e suas aplicações aos mais diversos problemas, demonstrando a beleza inerente à Matemática e em particular, à Aritmética, e levando os alunos a apreciá-la também por sua beleza e não só por sua utilidade.

O trabalho foi estruturado em dois capítulos, cada um dividido em algumas seções. No Capítulo 1 trabalhamos com o conceito de divisibilidade e resto, apresentando inicialmente a noção de fatoração juntamente com a definição de número primo, conceitos que são atinentes. Em seguida são apresentadas as definições de Máximo Divisor Comum e Mínimo Múltiplo Comum. A noção de restos é introduzida previamente à

divisão euclidiana e ao final do capítulo é apresentado o Algoritmos de Euclides, para o cálculo do M.D.C.. No Capítulo 2 trabalhamos com a definição de congruência e algumas de suas aplicações. O conceito de congruência pode ser naturalmente inserido no conteúdo programático do ensino fundamental, desde que os alunos tenham trabalhado de forma satisfatória o conceito de restos na divisão euclidiana. Neste mesmo capítulo, apresentamos a ideia de bases numéricas para, em seguida, discutirmos acerca da representação decimal e dos testes de divisibilidade, já utilizando-se de congruências. Dentro desta seção são apresentados alguns critérios de divisibilidade e damos ênfase à divisibilidade por 9, que gera uma série de curiosidades como os truques numéricos ou "matemágicas"e a famosa prova dos "noves fora". Ao final são feitas as considerações finais acerca deste trabalho.

A escolha dos temas a serem abordados neste trabalho e dos que seriam deixados de fora reflete uma análise pessoal do que seria realmente importante para ser apresentado a alunos do Ensino Fundamental, de forma que buscou-se cobrir os aspectos mais relevantes da teoria.

Os teoremas, definições, corolários, etc., foram, em grande parte, baseados em autores consagrados da Teoria dos Números como [2], [6], [8] e [13]. Os exercícios trabalhados foram elaborados, extraídos ou adaptados de diversas fontes, como [3], [5], [4], [9] e [7].

A seleção dos exercícios que foram trabalhados em cada unidade foi feita de maneira criteriosa, englobando exercícios de diversos níveis, inclusive olímpicos, pertinentes ao conteúdo em questão. Procurou-se apresentar exercícios interessantes com caráter interpretativo que visem desenvolver nos alunos a compreensão do significado dos conceitos apresentados na forma de teoremas e definições e torná-los aptos a manipular as expressões algébricas. Em alguns casos, tornou-se mais interessante apresentar um problema antes da definição formal, para que o aluno possa familiarizar-se preliminarmente com o conceito que será trabalhado, verificando de imediato sua necessidade e aplicação. As soluções dos problemas foram elaboradas de maneira clara e detalhada e as justificativas e explicações são apresentadas de forma simples e adequadamente inteligível a alunos das séries finais do Ensino Fundamental, abrindo caminho para que o aluno realize suas explorações individuais, que ocorre quando ele realmente começa a apreciar a matemática envolvida.

Capítulo 1

Divisibilidade e resto

Neste capítulo serão apresentados os principais conceitos acerca de divisibilidade e resto, tais como números primos e compostos, Máximo Divisor Comum e Mínimo Múltiplo Comum, divisão euclidiana e algoritmo de Euclides, bem como diversos exercícios pertinentes.

1.1 Números primos e compostos

O conjunto dos números naturais é formado por números primos e compostos. Um número natural maior que 1 é considerado primo se possui como divisores positivos apenas 1 e ele mesmo. Desta forma, podemos considerar como composto o número que for igual ao produtos de dois naturais menores que ele. Tomemos o número 130 que pode ser representado como a multiplicação dos números 13 e 10, pois $130 = 13 \cdot 10$. O número 13 não pode ser representado pela multiplicação entre outros naturais diferentes de 1 e 13, logo $13 = 1 \cdot 13$ é a única decomposição possível de 13 como produto de números naturais e, portanto, 13 é primo. Entretanto, notemos que $10 = 2 \cdot 5$ e assim 10 é composto. Notemos que os fatores presentes na decomposição de 10, os números 2 e 5, são primos e, do mesmo modo, podemos representar o número 130, que é composto, como um produto de primos da seguinte maneira: $130 = 13 \cdot 10 = 13 \cdot 5 \cdot 2$.

E se tentarmos fatorar o número 130 de outro modo? Por exemplo, $130 = 26 \cdot 5$. Como 5 é primo e 26 é composto, podemos fatorar o número 26 da seguinte forma: $26 = 13 \cdot 2$, e assim $130 = 26 \cdot 5 = 13 \cdot 2 \cdot 5$. Com isto, terminamos com as mesma

representação em fatores primos, diferindo apenas na ordem dos fatores.

Este fato leva-nos a inferir o Teorema Fundamental da Aritmética, enunciado abaixo. O leitor interessado em outras demonstrações do referido teorema pode consultar [6], [8] e [13].

Teorema 1.1 (Teorema Fundamental da Aritmética)**.** Todo número natural a maior do que 1 ou é primo ou pode ser escrito de forma única (a menos da ordem dos fatores) como um produto de números primos.

Demonstração. Provaremos a existência e a unicidade utilizando o segundo princípio de indução, que parte da ideia de que o resultado é válido para todo natural menor que a para provar que vale para a. Para a demonstração dos princípios de indução, o leitor interessado pode consultar [2], [6] ou [13].

Existência:

Para $a = 2$ o teorema é válido, pois 2 é primo.

Se a é primo, não há nada a demonstrar. Suponhamos que a seja composto, assim existem números a_1 e a_2 tais que $a = a_1 \cdot a_2$, com $1 < a_1 < a$ e $1 < a_2 < a$. Pela hipótese indutiva, existem primos p_1, p_2,...,p_r e q_1, q_2,...,q_s tais que $a_1 = p_1 \cdot p_2 \cdots p_r$ e $a_2 = q_1 \cdot q_2 \cdots q_s$, ou seja, a_1 e a_2 se decompõem como produto de primos. Assim, juntando as fatorações de a_1 e a_2 e reordenando os fatores, obtemos a fatoração de a: $a = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s$

Unicidade: Para $a = 2$ a afirmação é válida.

Se a é primo não há nada a provar. Suponhamos então que a seja composto e que possua duas fatorações, ou seja,

$a = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$

Provemos que $r = s$ e que cada p_i é igual a algum q_j. Como p_1 pertence a fatoração do número $q_1 \cdot q_2 \cdots q_s$, pelo menos um dos fatores q_j é divisível por p_1. Suponhamos, sem perda de generalidade, que q_1 seja divisível por p_1. Como ambos são primos, temos que $p_1 = q_1$. Logo $\frac{a}{p_1} = p_2 \cdot p_3 \cdots p_r = q_2 \cdot q_3 \cdots q_s$. Como $1 < \frac{a}{p_1} < a$, pela hipótese indutiva, as fatorações são iguais, ou seja, $r = s$ e, a menos da ordem dos fatores, as fatorações $p_1 \cdot p_2 \cdots p_r$ e $q_1 \cdot q_2 \cdots q_s$ são iguais.

□

Exemplo 1.2. Escreva 2670 como um produto de números primos.

Solução: Para realizar este procedimento, também denominado de fatoração, escrevemos o número 2670 ao lado de uma barra vertical, conforme pode ser verificado abaixo.

Do lado direito da barra, escrevemos os divisores primos de 2670 em ordem crescente e do lado esquerdo os resultados das sucessivas divisões por estes fatores primos. Vejamos abaixo:

2670	2
1335	3
445	5
89	89
1	$2 \cdot 3 \cdot 5 \cdot 89 = 2670$

Figura 1.1: Fatoração do número 2670

Multiplicando os números primos do lado direito da barra obtemos a fatoração de 2670 como um produto de fatores primos: $2670 = 2 \cdot 3 \cdot 5 \cdot 89$.

Abaixo vejamos a sugestão de alguns problemas a serem propostos aos alunos para auxiliar na construção dos conceitos de fatoração.

Problema 1.3. O número $3^5 \cdot 7$ é divisível por 3?

Solução: Sim, visto que 3 é um dos fatores na decomposição do número dado.

Problema 1.4. O número $2^7 \cdot 3^2$ é divisível por 5?

Solução: Não, pois o primo 5 não faz parte da decomposição do número.

Problema 1.5. O número $3^5 \cdot 5$ é divisível por 9?

Solução: Sim, já que $9 = 3^2$ e existem cinco fatores iguais a 3 na decomposição do número dado: $3^5 \cdot 5 = 3^2 \cdot 3^3 \cdot 5 = 9 \cdot 3^3 \cdot 5 = 9^2 \cdot 3 \cdot 5$

Problema 1.6. Se um número natural for divisível por 6 e por 9 ele tem que ser divisível por $6 \cdot 9 = 54$?

Solução: Vejamos, se o número é divisível por 6, possui os primos 2 e 3 em sua decomposição. Como também é divisível por 9, possui dois fatores iguais a 3 em sua decomposição. Todavia, podemos ter certeza que a decomposição tem dois fatores iguais a 3 (mas não necessariamente três fatores), e um igual a 2, assim só podemos garantir a divisibilidade por 18.

Problema 1.7. Dê a fatoração em números primos dos números 620, 1024 e 30030.

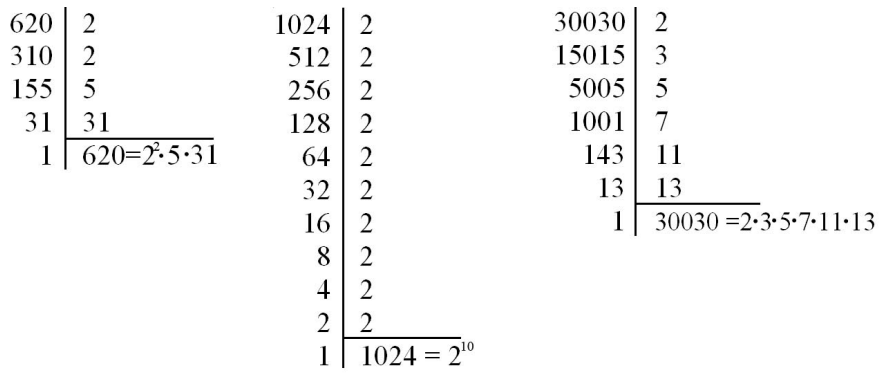

Figura 1.2: Fatorações dos números 620, 1024 e 30030

Problema 1.8. O número $7 \cdot A$ é divisível por 3. É verdade que A é divisível por 3?

Solução: Sim, pois a decomposição de $7 \cdot A$ contém 3, mas a decomposição de 7 não.

Vejamos abaixo um famoso problema extraído de [5] :

Problema 1.9. Portas abertas e fechadas
Uma nova escola acaba de ser construída. Nela há 1000 armários numerados de 1 a 1000. Durante o recesso, os estudantes decidem tentar uma experiência. Cada estudante irá andar pela escola, um de cada vez. O primeiro aluno irá abrir as portas de todos os armários. O segundo aluno irá fechar as portas dos armários de números pares. O terceiro aluno irá alterar a posição das portas de números múltiplos de 3: as que estiverem abertas ele irá fechá-las e as que estiverem fechadas ele irá abri-las. O quarto aluno irá mudar a posição das portas de número múltiplo de 4, e assim por diante. Depois que 1000 alunos entrarem na escola, a porta de qual armário ainda estará aberta?

Solução. Para simplificar o problema, é possível construir uma tabela para as primeiras 20 portas, onde a = aberto e f = fechado:

Tabela 1.1: Tabela para as 20 primeiras portas

Estudantes																				
Número do armário	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	a																			
2	a	f																		
3	a		f																	
4	a	f		a																
5	a				f															
6	a	f	a			f														
7	a						f													
8	a	f		a				f												
9	a		f						a											
10	a	f			a					f										
11	a										f									
12	a	f	a	f		a						f								
13	a												f							
14	a	f					a							f						
15	a		f		a										f					
16	a	f		a				f								a				
17	a																f			
18	a	f	a			f			a									f		
19	a																		f	
20	a	f		a	f					a										f

Com a tabela é possível observar o seguinte:

1. Todas as portas são abertas pelo primeiro estudante. Depois que o primeiro estudante abriu a primeira porta, ela não foi mais alterada. Depois o segundo estudante fechou a segunda porta e ela retornou à sua posição. Quando o n-ésimo estudante entra, ela altera a posição do armário de ordem n e a posição desta porta não será alterada mais. A diagonal na tabela indica a posição final das portas.

2. As únicas portas da diagonal que estão abertas são as portas 1, 4, 9 e 16. Se esse padrão continuar, o próximo armário que ficará aberto é o de número 25. Esta conclusão pode ser verificada. A porta 25 será aberta pelo primeiro aluno, fechada pelo quinto aluno e finalmente aberta pelo vigésimo quinto estudante. Os números 1, 5 e 25 são os únicos divisores de 25.

Para cada porta de armário, considere que os alunos irão abrir ou fechar a porta.

Os únicos estudantes que irão mudar a porta de um armário são aqueles cujos números de ordem são divisores do número da porta do armário. Por exemplo, o armário 12 só será alterado pelos estudantes 1, 2, 3, 4, 6 e 12.

Agora a atenção virou-se para os divisores correspondentes de um número e as mudanças que ocorrem na porta do armário. É possível observar que todas as portas com um número par de divisores são mantidas fechadas.

Vejamos a porta 12:

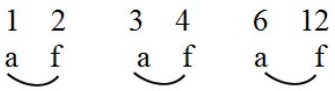

Figura 1.3: Divisores de 12

Os divisores de 12 também podem ser emparelhados como:

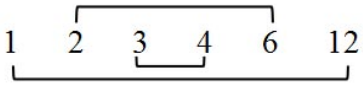

Figura 1.4: Emparelhamento dos divisores de 12

No emparelhamento, cada par de fatores distintos, quando multiplicados, produz o número do armário. O emparelhamento de todos os fatores implica em um número par de fatores.

Apenas armários com número ímpar de fatores serão deixados abertos. Um número quadrado tem um fator (que é sua raiz quadrada) que quando multiplicado por si mesmo resulta no número quadrado, conforme pode ser verificado na Figura 1.5. Assim, todos os números quadrados tem um número ímpar de fatores. Os únicos armários que ficarão abertos são aqueles cujos números são quadrados perfeitos.

Nota aos professores: O Teorema Fundamental da Aritmética foi crucial para a solução deste problema, bem como o conceito de número de divisores. Neste momento seria interessante apresentar o problema seguinte, que induz os alunos à determinação de uma fórmula para o número de divisores.

Problema 1.10. Determine todos os divisores positivos do número $a = 2^3 \cdot 3$. Generalize a questão determinando todos os divisores positivos do número $n = p_1^{x_1} \cdot p_2^{x_2} \cdots p_s^{x_s}$, com p_i primo.

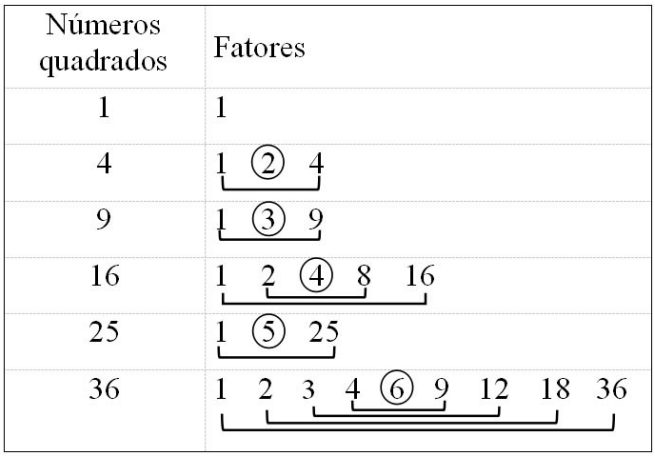

Figura 1.5: Fatores emparelhados de alguns números quadrados

Solução: Se d é um divisor de a, os únicos fatores primos de d serão 2 e 3. Logo, $d = 2^x \cdot 3^y$. Mas a é múltiplo de d, então podemos escrever $a = k \cdot d$, implicando que as potências x e y dos primos 2 e 3 devem ser menores ou iguais às potências de 2 e 3 na fatoração de a. Veja que o número $2^4 \cdot 3$ não pode ser divisor de a, pois a não possui em sua fatoração quatro fatores 2. Logo, devemos ter $x \leq 3$ e $y \leq 1$. Desta forma, $x \in \{0, 1, 2, 3\}$ e $y \in \{0, 1\}$. Para encontrar todos os divisores de a devemos realizar todas as combinações possíveis dos expoentes x e y. Logo, a questão pode ser resolvida utilizando-se da Combinatória. Cada um dos fatores primos de a pode ser usado para formar um divisor de 0 até o número de vezes indicado no expoente. Construímos então a árvore de possibilidades para os divisores de a, onde o número de ramos no final da árvore indica o número de modos de selecionar os fatores primos.

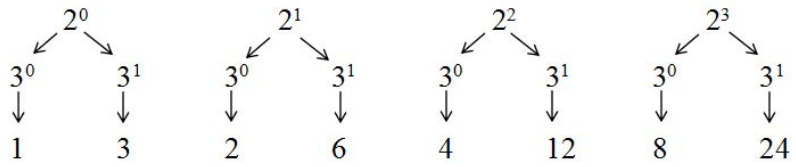

Figura 1.6: Árvore de possibilidades dos divisores de $a = 2^3 \cdot 3$

Logo, a possui $(3 + 1) \cdot (1 + 1) = 8$ divisores.

Generalizando, seja m um divisor positivo de $n = p_1^{x_1} \cdot p_2^{x_2} \cdots p_s^{x_s}$ e p^y a potência de um

primo na decomposição de m. Como n é divisível por m, p^y deve dividir algum fator $p_i^{x_i}$, por ser primo com os demais fatores $p_j^{x_j}$, assim $p = p_i$ e $0 \leq y \leq x_i$.

Logo, $m = p_1^{y_1} \cdot p_2^{y_2} \cdots p_s^{y_s}$, onde $0 \leq y_i \leq x_i$.

Seja $d(n)$ o número de divisores positivos de $n = p_1^{x_1} \cdot p_2^{x_2} \cdots p_s^{x_s}$, segue por contagem que $d(n) = (x_1 + 1) \cdot (x_2 + 1) \cdots (x_s + 1)$.

Problema 1.11. (Extraído de [6]) Ache os possíveis valores de $n, m \in \mathbb{N} \cup \{0\}$ de modo que o número $9^m \cdot 10^n$ tenha: a) 27 divisores b) 243 divisores.

Solução. Observemos primeiramente que $9^m \cdot 10^n = 3^{2m} \cdot (2 \cdot 5)^n = 3^{2m} \cdot 2^n \cdot 5^n$. Assim, o número de divisores é $(2m + 1)(n + 1)(n + 1)$.

a) Para que o número tenha 27 divisores, devemos ter $(2m + 1)(n + 1)^2 = 27$. Mas $27 = 3^3$, logo 27 pode ser escrito como produto de dois fatores, sendo um deles quadrado, das seguintes formas:

i) Se $(2m + 1)(n + 1)^2 = 3 \cdot 3^2$

$$\begin{cases} (2m + 1) = 3 \longrightarrow m = 1 \\ (n + 1) = 3 \longrightarrow n = 2 \end{cases}$$

ii) Se $(2m + 1)(n + 1)^2 = 27 \cdot 1^2$

$$\begin{cases} (2m + 1) = 27 \longrightarrow m = 13 \\ (n + 1) = 1 \longrightarrow n = 0 \end{cases}$$

Assim, os possíveis valores para m e n são $\{1, 2\}$ e $\{13, 0\}$.

b) De modo análogo ao item anterior, para que o número tenha 243 divisores, devemos ter $(2m + 1)(n + 1)^2 = 243$. Mas $243 = 3^5$, logo 243 pode ser escrito como produto de dois fatores, sendo um deles quadrado, das seguintes formas:

i) Se $(2m + 1)(n + 1)^2 = 27 \cdot 3^2$

$$\begin{cases} (2m + 1) = 27 \longrightarrow m = 13 \\ (n + 1) = 3 \longrightarrow n = 2 \end{cases}$$

ii) Se $(2m + 1)(n + 1)^2 = 3 \cdot 9^2$

$$\begin{cases} (2m+1) = 3 \longrightarrow m = 1 \\ (n+1) = 9 \longrightarrow n = 8 \end{cases}$$

iii) Se $(2m+1)(n+1)^2 = 243 \cdot 1^2$

$$\begin{cases} (2m+1) = 243 \longrightarrow m = 121 \\ (n+1) = 1 \longrightarrow n = 0 \end{cases}$$

Assim, os possíveis valores para m e n são $\{13, 2\}$, $\{1, 8\}$ e $\{121, 0\}$.

1.1.1 Números primos - O Crivo de Eratóstenes

Ao trabalharmos com números primos surge a necessidade de um método para determinar se um número é primo ou não. Para isso, apresentaremos um método antigo, mas eficaz para verificação da primalidade de um número e obtenção de uma lista de todos os primos menores ou iguais a algum número dado: o Crivo de Eratóstenes.

O método parte da utilização de uma tabela com todos os números naturais de 2 até n, a partir da qual vão-se eliminando os números compostos até que restem apenas os números primos menores ou iguais a n, como uma peneira; daí origina-se o nome Crivo (Peneira) de Eratóstenes. Vejamos primeiramente o seguinte teorema:

Teorema 1.12. Se $n \in \mathbb{N}$ é composto, então n é divisível por algum fator primo $p \leq \sqrt{n}$.

Demonstração. Como n é composto, ele pode ser decomposto da seguinte forma:

$$n = ab \ (1 < a \leq b < n)$$

Disso, decorre que $n = ab \geq a^2$. Seja p um número primo divisor de a, então $a = kp$ e isso implica que $a^2 = k^2p^2$ e assim, p^2 é um divisor de a^2 e portanto $p^2 \leq a^2$. Como $a^2 \leq n$, então $p^2 \leq n$ implica $p \leq \sqrt{n}$.

□

Para visualizar outras demonstrações deste teorema, o leitor interessado pode consultar [8] e [13].

Este resultado possui grande importância prática e sua aplicação determina o processo utilizado no Crivo de Eratóstenes. Ele afirma que para testarmos se um número é

primo, basta verificarmos a divisibilidade pelos primos menores ou iguais a $\sqrt{n}$. Desta forma, para obtermos uma lista com todos os primos menores que n devemos riscar dentre os números de 2 a n os múltiplos dos primos menores ou iguais a $\sqrt{n}$.

Por exemplo, para determinarmos se 67 é primo, basta testarmos a divisibilidade de 67 pelos primos 2, 3, 5, 7, que são os primos menores que $\sqrt{67}$. Como 67 não é divisível por nenhum desses primos, então 67 é número primo.

Vejamos na tabela abaixo o processo de determinação de todos os primos menores que 50. Para construí-la, escrevemos os naturais de 2 a 50 e riscamos os múltiplos dos primos menores que $\sqrt{50}$, ou seja, os múltiplos de 2, 3, 5 e 7.

	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~~

1.2 Máximo Divisor Comum e Mínimo Múltiplo Comum

1.2.1 Máximo Divisor Comum

Antes de visualizarmos a definição formal de Máximo Divisor Comum (MDC) vejamos o seguinte problema:

Problema 1.13. Um prédio tem duas escadas diferentes, todas começando da base do prédio e terminando no topo. Uma escada tem 780 degraus e a outra 700 degraus. Sempre que os degraus das duas escadas estão na mesma altura há um andar. Quantos andares têm o prédio?

Solução. Vamos verificar as possibilidades:

-Podemos dividir o prédio em dois andares, assim, quando a escada nº 1 tiver passado por 390 degraus e a escada nº 2 por 350 degraus, temos um andar.

-Mas também podemos dividir o prédio em quatro andares, assim a cada 195 degraus da escada nº 1 e a cada 175 degraus da escada nº 2 temos um andar.

-Todavia, podemos obter ainda mais andares, bastando dividir 195 e 175 por algum número em comum de suas fatorações. Mas vejamos que queremos o maior dos divisores comuns de 780 e 700. Para encontrá-lo, podemos fatorar os dois números e verificar os fatores primos em comum:

$780 = 2^2 \cdot 3 \cdot 5 \cdot 13$

$700 = 2^2 \cdot 5^2 \cdot 7$

Representando na forma de diagramas de Venn, conforme a Figura 1.7, podemos ver quais são os fatores comuns na fatoração de 780 e 700:

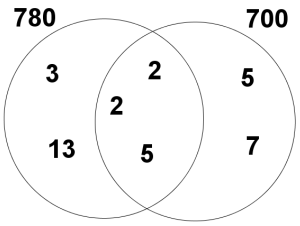

Figura 1.7: Diagramas com as fatorações de 780 e 700

Logo, o maior divisor comum entre 780 e 700 é o número composto pelos fatores 2, 2 e 5, ou seja, $2 \cdot 2 \cdot 5 = 20$

Desta forma, podemos concluir que o prédio tem 20 andares.

Definição 1.2.1. O Máximo Divisor Comum (MDC ou $mdc(x, y)$) de dois naturais x e y é o maior número natural que divide ambos os números.

Vejamos um exemplo:

Exemplo 1.14. Dados os números $x = 2^2 \cdot 3 \cdot 5^3 \cdot 7^2$ e $y = 2 \cdot 3 \cdot 5^2 \cdot 13$, encontre o $mdc(x, y)$.

Solução: Notemos que os termos comuns na fatoração de x e y são 2, 3 e 5^2, logo o $mdc(x, y) = 2 \cdot 3 \cdot 5^2 = 150$ Visualizemos abaixo através dos diagramas de Venn:

1.2.2 Mínimo Múltiplo Comum

Vamos verificar como o conceito de Mínimo Múltiplo Comum (MMC) aparece naturalmente na resolução de problemas:

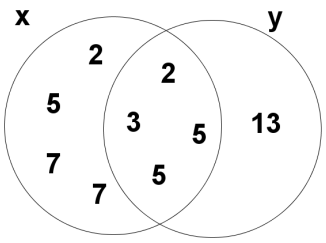

Figura 1.8: Diagramas com as fatorações de x e y

Problema 1.15. Em um ponto de ônibus, os ônibus da linha A passam a cada 12 minutos, os que fazem a linha B passam a cada 15 minutos e os que fazem a linha C passam a cada 20 minutos. A cada quantos minutos os ônibus das três linhas chegarão juntos ao ponto?

Solução: Vamos começar a anotar os horários, em minutos, de cada ônibus a partir do instante 0 onde os três ônibus passam ao mesmo tempo no ponto:

$A = \{0, 12, 24, 36, 48, 60, 72, 84, 96, 108, 120, ...\}$

$B = \{0, 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, ...\}$

$C = \{0, 20, 40, 60, 80, 100, 120, 140, 160, 180, ...\}$

Notemos que os três ônibus chegam ao ponto após 60 minutos. Dentre os múltiplos comuns dos horários de A, B e C, 60 é o menor deles; logo, podemos concluir que os ônibus se encontram no ponto a cada 60 minutos.

Definição 1.2.2. O Mínimo Múltiplo Comum (MMC ou $mmc(x, y)$) de dois naturais x e y é o menor número natural divisível por ambos os números.

Exemplo 1.16. Encontre o Mínimo Múltiplo Comum entre os números $a = 3^2 \cdot 7 \cdot 11^2$ e $b = 2 \cdot 3 \cdot 7^2$.

Solução. Como o $mmc(a, b)$ é o menor múltiplo simultâneo de a e b, ele é composto por todos os fatores primos de a e b. Logo, também podemos representar o $mmc(a, b)$ através de diagramas, onde o mmc é a união dos fatores primos de a e b. Veja a representação através de diagramas de Venn (Figura 1.9) do $mmc(3^2 \cdot 7 \cdot 11^2, 2 \cdot 3 \cdot 7^2)$:

Assim, o $mmc(3^2 \cdot 7 \cdot 11^2, 2 \cdot 3 \cdot 7^2) = 2 \cdot 3 \cdot 3 \cdot 7 \cdot 7 \cdot 11 \cdot 11 = 2 \cdot 3^2 \cdot 7^2 \cdot 11^2 = 106722$
Vejamos abaixo um exemplo do cálculo do mmc e do mdc dadas as fatorações:

Exemplo 1.17. Encontre o mdc e o mmc dos números 24 e 36.

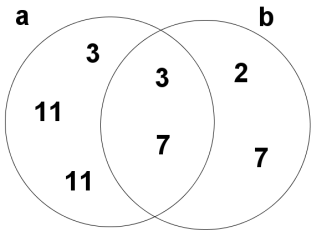

Figura 1.9: Diagramas com as fatorações de a e b

Solução. Vamos primeiramente fatorar os números. Através o método descrito no Exemplo 1.2 encontramos as seguintes fatorações: $24 = 2^3 \cdot 3$ e $36 = 2^2 \cdot 3^2$. Podemos representar os números em sua forma fatorada através de diagramas, conforme figura 1.10:

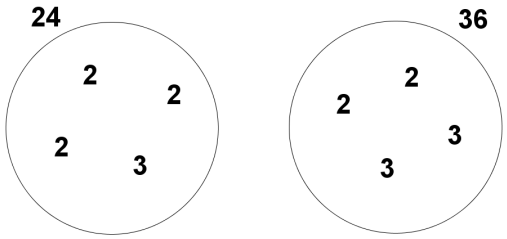

Figura 1.10: Diagramas com as fatorações de 24 e 36

Conforme observamos anteriormente, no problema 1.13 e no exemplo 1.16, o *mdc* é a intersecção das fatoraçãoes e o *mmc* é a união das fatorações do números, o que pode ser verificado na Definição 1.2.3.

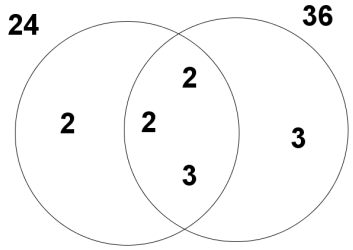

Figura 1.11: Intersecção das fatorações de 24 e 36

Logo, pela observação dos diagramas da Figura 1.11 podemos concluir que o $mdc(24, 36) =$

$2 \cdot 2 \cdot 3 = 12$ e o $mmc(24, 36) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$.

1.2.3 Método da fatoração simultânea

Visto que, para o cálculo do mmc e do mdc utilizamos as fatorações dos números envolvidos, podemos utilizar um único cálculo para determinar simultaneamente o mdc e o mmc. Trata-se da fatoração simultânea, descrito como segue:

Listemos os números dos quais desejamos encontrar o mmc e o mdc, lado a lado, separados por vírgulas e, semelhantemente ao procedimento normal de fatoração descrito no Exemplo 1.2, tracemos uma barra vertical à direita do último número e do lado direito da barra escrevemos o menor número primo que divide algum dos números à esquerda. Devemos tentar dividir todos os números da esquerda pelo número primo da direita; se o número for divisível pelo primo à direita da barra, escrevemos abaixo do número o quociente da divisão, se não for, repetimos o mesmo número da linha anterior. Devemos repetir esse procedimento até que restem apenas números 1 do lado esquerdo da barra. Vamos realizar a fatoração simultânea dos números 24 e 36 do exemplo 1.17:

1º passo		2º passo		3º passo		4º passo		5º passo		6º passo	
24, 36	2	24, 36	2	24, 36	2	24, 36	2	24, 36	2	24, 36	2
		12,18	2	12, 18	2	12, 18	2	12, 18	2	12, 18	2
				6, 9	2	6, 9	2	6, 9	2	6, 9	2
						3, 9	3	3, 9	3	3, 9	3
								1, 3	3	1, 3	3
										1,1	

O que podemos observar com o resultado da fatoração simultânea? Podemos notar que a mesma corresponde à união dos termos das decomposições dos números 24 e 36 e a união das fatorações nada mais é que o mínimo múltiplo comum entre os números. Logo, o mmc será o produto dos primos encontrados na fatoração simultânea, que no caso é igual a $mmc(24, 36) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$.

Através da mesma fatoração simultânea podemos determinar o mdc entre os números, bastando recordar que o mdc é a intersecção das fatorações dos números desejados, ou seja, é o produto dos primos que dividem simultaneamente todos os números. Desta forma, podemos observar todos os primos que dividem todos os números à esquerda ao mesmo tempo e sublinhá-los; o produto de todos os primos sublinhados é o mdc procurado. Vejamos:

24, 36	$\underline{2}$	
12, 18	$\underline{2}$	
6, 9	2	$\Longrightarrow$2 não divide 9, logo não sublinharemos
3, 9	$\underline{3}$	
1, 3	3	$\Longrightarrow$3 não divide 1, logo não sublinharemos
1,1		

Desta forma o $mdc(24, 36)$ é igual a $2 \cdot 2 \cdot 3 = 12$.

Ao final deste capítulo veremos outro método para o cálculo do mdc através das divisões sucessivas, o Algoritmo de Euclides.

Vejamos abaixo a definição de MMC e MDC que utiliza as fatorações:

Definição 1.2.3. Seja $a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ e $b = p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n}$ dois naturais e suas decomposições em fatores primos, tais que $p_1, p_2, ...p_n$ são primos e $r_1, r_2, ...r_n, s_1, s_2, ...s_n \in \mathbb{N} \cup \{0\}$. Definimos o Máximo Divisor Comum de a e b como

$$mdc(a, b) = p_1^{t_1} \cdot p_2^{t_2} \cdots p_n^{t_n}, \text{ onde } t_i = min\{r_i, s_i\}$$

Definimos o Mínimo Múltiplo Comum de a e b como

$$mmc(a, b) = p_1^{v_1} \cdot p_2^{v_2} \cdots p_n^{v_n}, \text{ onde } v_i = max\{r_i, s_i\}$$

Definição 1.2.4. Dois (ou mais) naturais são considerados primos entre si quando o mdc entre eles é 1.

Problema 1.18. Prove que, dados dois números naturais a e b, eles satisfazem a equação $mdc(a, b) \cdot mmc(a, b) = a \cdot b$.

Solução. Sendo $a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ e $b = p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n}$, pela Definição 1.2.3, temos que $mdc(a,b) = p_1^{t_1} \cdot p_2^{t_2} \cdots p_n^{t_n}$ e $mmc(a,b) = p_1^{v_1} \cdot p_2^{v_2} \cdots p_n^{v_n}$, com $t_i = min\{r_i, s_i\}$ e $v_i = max\{r_i, s_i\}$. Desta forma,

$$mdc(a,b) \cdot mmc(a,b) = p_1^{t_1} \cdot p_2^{t_2} \cdots p_n^{t_n} \cdot p_1^{v_1} \cdot p_2^{v_2} \cdots p_n^{v_n}$$

E assim, o produto do $mdc(a,b)$ com $mmc(a,b)$ contém todos os fatores primos de a e b.

Problema 1.19. Se a é múltiplo de b, determine o $mdc(a,b)$ e o $mmc(a,b)$.

Solução. Como a é múltiplo de b, temos que $a = kb$. Das definições de mdc e mmc podemos concluir que $mmc(a,b) = a$ e que $mdc(a,b) = b$.

Podemos notar que o $mmc(a,b)$ é um múltiplo do $mdc(a,b)$. Verifiquemos a validade desta afirmação através do argumento seguinte:

Sejam a e b dois números naturais. Temos que o $mdc(a,b)$ divide a, logo $a = k_1 \cdot mdc(a,b)$. Sabemos também que $mmc(a,b)$ é múltiplo de a, assim $mmc(a,b) = k_2 \cdot a$. Disso segue que

$$mmc(a,b) = k_2 a = k_2(k_1 \cdot mdc(a,b)) = (k_1 k_2) mdc(a,b)$$

Como k_1 e k_2 são inteiros, segue que o $mmc(a,b)$ é um múltiplo do $mdc(a,b)$.

Proposição 1.20. Para quaisquer $a, b \in \mathbb{Z}$ não nulos e $t \in \mathbb{N}$ tem-se que

$$mdc(ta, tb) = t \cdot mdc(a,b)$$

Demonstração. No processo das divisões sucessivas (descrito na seção 1.4) que leva ao $mdc(a,b)$ partindo de a e b, multipliquemos por t cada uma das igualdades obtidas:

$$\begin{aligned} ta &= (tb)q_1 + tr_1 \\ tb &= (tr_1)q_2 + tr_2 \\ &\vdots \\ tr_{n-2} &= (tr_{n-1})q_n + tr_n \\ tr_{n-1} &= (tr_n)q_{n+1} \end{aligned}$$

Logo, temos que $t \cdot mdc(a,b) = tr_n = mdc(tr_{n-1}, tr_n) = \cdots = mdc(tb, tr_1) = mdc(ta, tb)$.

□

Corolário 1.21. Dados a e b naturais não nulos, se $d = mdc(a, b)$ então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.

Demonstração. Pela Proposição 1.20, temos que

$$d \cdot mdc(\tfrac{a}{d}, \tfrac{b}{d}) = mdc(d \cdot \tfrac{a}{d}, d \cdot \tfrac{b}{d}) = mdc(a, b) = d$$

o que prova o resultado. □

Problema 1.22. Encontre dois números naturais a e b tais que $mdc(a, b) = 12$ e $mmc(a, b) = 180$.

Solução. Sabemos, pelo que foi demonstrado anteriormente, que $mdc(a, b) \cdot mmc(a, b) = a \cdot b$. Temos também que, se $d = mdc(a, b)$, então $1 = mdc(\frac{a}{d}, \frac{b}{d})$. Logo, como $mdc(a, b) = 12$, então $mdc(\frac{a}{12}, \frac{b}{12}) = 1$ Assim, a e b são múltiplos de 12 e $\frac{a}{12}$ e $\frac{b}{12}$ são primos entre si.

$a \cdot b = mdc(a, b) \cdot mmc(a, b)$

$a \cdot b = 12 \cdot 180$

$\frac{a}{12} \cdot \frac{b}{12} = 15$

Como $mdc(\frac{a}{12}, \frac{b}{12}) = 1$, então $\frac{a}{12} = 1$ e $\frac{b}{12} = 15$ ou $\frac{a}{12} = 3$ e $\frac{b}{12} = 5$.

As possíveis soluções são, portanto $a = 12$ e $b = 180$ ou $a = 36$ e $b = 60$.

Problema 1.23. (UERJ/00) O número de fitas de vídeo que Marcela possui está compreendido entre 100 e 150. Agrupando-as de 12 em 12, de 15 em 15 ou de 20 em 20, sempre resta uma fita. A soma dos três algarismos do número total de fitas que ela possui é igual a:

a) 3 b) 4 c) 6 d) 8 e) 10

Solução. O número de fitas menos 1 é múltiplo de 12, 15 e 20. Temos que o $mmc(12, 15, 20) = 2 \cdot 2 \cdot 3 \cdot 5 = 60$. Sabemos assim que o número de fitas é um múltiplo de 60 mais 1 que está entre 100 e 150. Logo, o número procurado de fitas é $60 \cdot 2 + 1 = 121$, visto que $60 \cdot 1 + 1 < 100$ e $60 \cdot 3 + 1 > 150$. A soma dos algarismos de 121 é $1 + 2 + 1 = 4$. Resposta: letra b) 4

Problema 1.24. Prove que o produto de três números naturais consecutivos quaisquer é divisível por 6.

Solução. Sejam a, $a+1$ e $a+2$ os três números consecutivos e consideremos o produto dos mesmos. Provemos por indução sobre a que o produto supracitado é divisível por 6.

i) Se $a = 1$, temos $1 \cdot 2 \cdot 3 = 6$ que é divisível por 6, logo a afirmação é válida para $a = 1$.

ii) Suponhamos, por hipótese, que $k(k+1)(k+2)$ é divisível por 6, para algum $k \in \mathbb{N}$. Provemos que $(k+1)(k+2)(k+3)$ também é divisível por 6.

Temos que $(k+1)(k+2)(k+3) = k^3+6k^2+11k+6 = (k^3+3k^2+2k)+3(k+1)(k+2)$

Por hipótese, k^3+3k^2+2k é divisível por 6, agora resta provarmos que $3(k+1)(k+2)$ também o é. Como $6 = 2 \cdot 3$, um número divisível por 6 possui em sua decomposição os fatores 2 e 3. Se k for par, $k+2$ também é par, e se k for ímpar, $k+1$ será par. Então, para qualquer valor de k, $3(k+1)(k+2)$ é múltiplo de 2 e de 3, sendo desta forma, múltiplo de 6. Portanto, $(k+1)(k+2)(k+3)$ é múltiplo de 6.

Outra solução: Sejam a, $a+1$ e $a+2$ os três números consecutivos. Mostremos que o produto entre eles é múltiplo de 2 e de 3. Consideremos os seguintes casos:

- Se a for ímpar, $a+1$ é par e o produto $a(a+1)(a+2)$ é múltiplo de 2;
- Se a for par, $a+2$ é par e o produto $a(a+1)(a+2)$ é múltiplo de 2.

Assim, em qualquer caso, o produto $a(a+1)(a+2)$ é múltiplo de 2.

Verifiquemos a divisibilidade por 3:

- Se $a = 3k$, $a(a+1)(a+2)$ é múltiplo de 3;
- Se $a = 3k+1$, então $a+2 = 3k+1+2 = 3k+3 = 3(k+1)$ e $a(a+1)(a+2)$ é múltiplo de 3;
- Se $a = 3k+2$, então $a+1 = 3k+2+1 = 3k+3 = 3(k+1)$ e $a(a+1)(a+2)$ é múltiplo de 3.

Logo, em qualquer caso o produto $a(a+1)(a+2)$ é múltiplo de 2 e de 3 e, desta forma é divisível por 6.

Problema 1.25. Prove que o produto de cinco números naturais consecutivos quaisquer é divisível por 30.

Solução. Primeiramente devemos fatorar o número 30: $30 = 2 \cdot 3 \cdot 5$.

Sejam a, $a+1$, $a+2$, $a+3$ e $a+4$ cinco números consecutivos. Pelo problema 1.24 verificamos que o produto de três naturais consecutivos é múltiplo de 2 e de 3, desta forma o produto $a(a+1)(a+2)(a+3)(a+4)$ também é múltiplo de 2 e 3.

Verifiquemos agora que o produto $a(a+1)(a+2)(a+3)(a+4)$ é múltiplo de 5:

- Se $a = 5k$, $a(a+1)(a+2)(a+3)(a+4) = 5k(5k+1)(5k+2)(5k+3)(5k+4)$ sendo assim, múltiplo de 5;

- Se $a = 5k+1$, então $a+4 = 5k+1+4 = 5k+5 = 5(k+1)$ e $a(a+1)(a+2)(a+3)(a+4) = (5k+1)(5k+2)(5k+3)(5k+4)5(k+1)$ sendo assim, múltiplo de 5;

- Se $a = 5k+2$, então $a+3 = 5k+2+3 = 5k+5 = 5(k+1)$ e $a(a+1)(a+2)(a+3)(a+4) = (5k+2)(5k+3)(5k+4)5(k+1)(5k+6)$ sendo assim, múltiplo de 5;

- Se $a = 5k+3$, então $a+2 = 5k+3+2 = 5k+5 = 5(k+1)$ e $a(a+1)(a+2)(a+3)(a+4) = (5k+3)(5k+4)5(k+1)(5k+6)(5k+7)$ sendo assim, múltiplo de 5;

- Se $a = 5k+4$, então $a+1 = 5k+4+1 = 5k+5 = 5(k+1)$ e $a(a+1)(a+2)(a+3)(a+4) = (5k+4)5(k+1)(5k+6)(5k+7)(5k+8)$ sendo assim, múltiplo de 5.

Assim, em qualquer caso, o produto $a(a+1)(a+2)(a+3)(a+4)$ é múltiplo de 2, 3 e 5 e, portanto, é divisível por 30.

Problema 1.26. (Bélgica-90) Seja n o número de inteiros (≥ 0) menores ou iguais a 10000, que são divisíveis por todos os inteiros positivos menores ou iguais a 10. Então: a) $n = 0$ b) $1 \leq n \leq 5$ c) $5 < n \leq 10$ d) $10 < n \leq 15$ e) $15 < n$

Solução. Um número k é divisível por todos os inteiros positivos menores ou iguais a 10 se possuir em sua fatoração em primos os números: 2, 3, $4 = 2^2$, 5, $6 = 2 \cdot 3$, 7, $8 = 2^3$, $9 = 3^2$ e $10 = 2 \cdot 5$. Notemos que k deve possuir em sua fatoração os primos 2, 3, 5 e 7, em certas quantidades mínimas para garantir a divisibilidade por todos os naturais menores ou iguais a 10. São necessários três fatores 2 para garantir a divisibilidade por 8 e dois fatores 3 para ser divisível por 9. Os primos 5 e 7 podem aparecer apenas uma vez na fatoração, pois não há nenhum número inteiro positivo menor ou igual a 10 que possua em sua fatoração alguma potência de 5 e 7 maior que 1.

Essa análise equivale a encontrar o Mínimo Múltiplo Comum entre os números 2, 3, 4, 5, 6, 7, 8, 9 e 10.

Logo, devemos ter $k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot a = 2520a$, sendo a natural.

Desta forma, n é a quantidade de múltiplos de 2520 menores que 10000. São eles:

$2520 \cdot 1 = 2520$

$2520 \cdot 2 = 5040$

$2520 \cdot 3 = 7560$

Assim, $n = 3$. Resposta: b) $1 \leq n \leq 5$

Problema 1.27. (Argentina-2000) Dos números naturais A e B sabe-se que $B = \frac{(A^2-1)}{8}$ e que o mínimo múltiplo comum entre A e B é igual 3720. Determinar A e B.

Solução. Notemos que se A é par, A^2 é par, e assim A^2-1 é ímpar, logo não é divisível por 8. Verifiquemos a hipótese de que se A é ímpar, A^2-1 é divisível por 8.

Se A é ímpar, é da forma $A = 4p+1$ ou $A = 4p+3$, daí

se $A = 4p+1 \Longrightarrow A^2-1 = (4p+1)^2-1 = 8(2p^2+p)$

se $A = 4p+3 \Longrightarrow A^2-1 = (4p+3)^2-1 = 8(2p^2+3p+1)$

Como A é ímpar, não possui em sua decomposição nenhum fator 2, o que indica que o fator 2^3 da decomposição de 3720 pertence a B.

Resta-nos os fatores 3, 5 e 31 que podem compor A, que é ímpar. Testando as possíveis combinações, temos:

se $A = 3, B = 1$, logo $mmc(3,1) = 3 \neq 3720$

se $A = 5, B = 3$, logo $mmc(5,3) = 15 \neq 3720$

se $A = 31, B = 120$, logo $mmc(31,120) = 3720$

Logo, $A = 31$ e $B = 120$

Problema 1.28. (Austrália-91) Seja M_n o mínimo múltiplo comum dos números $1, 2, 3, \ldots, n$, isto é, $M_1 = 1$, $M_2 = 2$, $M_3 = 6$, $M_4 = 12$, $M_5 = 60$, $M_6 = 60$. Para quais inteiros positivos $M_{n-1} = M_n$ é válido?

Solução. Observemos que M_n, por ser o mínimo múltiplo comum de todos os naturais menores ou iguais a n, deve conter todos os fatores primos que compõem os naturais menores ou iguais a n. Logo, teremos $M_{n-1} = M_n$ quando os primos que compõem n em sua fatoração já aparecem, na devida quantidade, entre os naturais menores que n. Vejamos alguns exemplos:

$M_9 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 2^2 \cdot 3^2 \cdot 7 = 10 \cdot 2^2 \cdot 3^2 \cdot 7$

$M_{10} = 10 \cdot 2^2 \cdot 3^2 \cdot 7$

Logo, $M_9 = M_{10}$.

$M_{11} = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 2^2 \cdot 3 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 12 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

$M_{12} = 12 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

Logo, $M_{11} = M_{12}$.

Problema 1.29. Encontre o menor número natural n tal que $n!$ é divisível por 990.

Solução. Temos que $990 = 2 \cdot 3^2 \cdot 5 \cdot 11$. Logo, para que $n!$ seja divisível por 990, $n!$ deve conter os fatores $2, 3^2, 5$ e 11. Como 11 é primo, ele mesmo deve estar contido no produto e $n = 11$ é o menor valor possível.

Problema 1.30. Quantos zeros existem no final da representação decimal do número 100!?

Solução: A quantidade de zeros no final de um número reflete a quantidade de fatores 10 que estão em sua decomposição. Se um número possui n zeros em seu final, ele é divisível por 10^n. Queremos saber então quantos fatores iguais a 10 estão contidos em 100!. Mas $10 = 2 \cdot 5$, então precisamos saber quantos fatores 2 e 5 estão contidos em 100!. Entre 5 números consecutivos quaisquer, que podem ser escritos da forma $5k$, $5k+1$, $5k+2$, $5k+3$ e $5k+4$ (não necessariamente nesta ordem), sempre haverá um múltiplo de 5 ($5k$) e, pelo menos, dois números pares, pois se k for par, também serão pares os números $5k$, $5k+2$ e $5k+4$ e, se k for ímpar, serão pares os números $5k+1$ e $5k+3$. Desta forma, para qualquer fator igual a 5 haverá fatores suficientes iguais a 2 para formar um fator igual a 10. Logo, basta contar os fatores 5.

Como $100 = 20 \cdot 5$, existem 20 múltiplos de 5 no produto $1 \cdot 2 \cdot 3 \cdots 99 \cdot 100$. Mas este número tem mais fatores iguais a 5, já que os números 25, 50, 75 e 100 contêm dois fatores iguais a 5, formando quatro "extras". Existem, portanto, 24 fatores iguais a 5, logo 24 fatores iguais a 10 e assim 24 algarismos finais iguais a 0 no produto 100!.

Outro método para descobrir o expoente de 5 na decomposição em fatores primos de 100!, encontrado em [7], consiste em usar o símbolo ˜ para significar a igualdade dos expoentes de 5 na decomposição.

$100! = 1 \cdot 2 \cdot 3 \cdots 100 \tilde{} 5 \cdot 10 \cdot 15 \cdots 100 = 5^{20}(1 \cdot 2 \cdot 3 \cdots 20) \tilde{} 5^{20}(5 \cdot 10 \cdot 15 \cdot 20) = 5^{20} \cdot 5^4(1 \cdot 2 \cdot 3 \cdot 4) \tilde{} 5^{24}$

Logo, 100! termina por 24 zeros.

Observação 1.31. O referido exercício também pode ser solucionado utilizando-se do Teorema de Legendre, conforme é explanado em [6].

Problema 1.32. Encontre todas as soluções de números naturais das equações:

a)$x^2 - y^2 = 31$ b)$x^2 - y^2 = 303$

Dica: $x^2 - y^2 = (x - y)(x + y)$

Solução: Temos que $x^2 - y^2 = 31$. Como 31 é primo, devemos ter o menor fator igual

a 1 e o maior igual a 31. Temos a seguinte equação:

$$\begin{cases} x - y = 1 \\ x + y = 31 \end{cases}$$

Da qual encontramos $x = 16$ e $y = 15$

b) Temos que $303 = 1 \cdot 303 = 3 \cdot 101$, logo temos dois sistemas de equações que podem fornecer os valores de x e y:

$$\begin{cases} x - y = 3 \\ x + y = 101 \end{cases}$$

$$\begin{cases} x - y = 1 \\ x + y = 303 \end{cases}$$

Dos quais encontramos os valores $x = 52$ e $y = 49$, e $x = 152$ e $y = 151$.

1.3 Restos

Iniciemos esta seção analisando a resolução dos seguintes problemas:

Problema 1.33. Desde que mudou de cidade José visita sua mãe a cada 8 dias. Se a primeira visita ocorreu em uma segunda-feira, a segunda visita será numa terça-feira, a terceira visita numa quarta-feira e assim sucessivamente. Em que dia da semana ocorrerá a 50ª visita?

Solução. Notemos que, como o intervalo entre uma visita e outra é de 8 dias, a próxima visita sempre ocorre no dia da semana posterior ao dia da visita anterior. Isto ocorre porque a semana possui 7 dias e o intervalo entre as visitas é de 8 dias. Como $8 = 7 \cdot 1 + 1$, o resto da divisão de 8 por 7 é 1 e assim, a cada 8 visitas o dia da visita volta a ser numa segunda-feira.

Logo, basta descobrir o resto da divisão de 50 por 8 para encontrar o dia em que ocorre a 50ª visita.

Como $50 = 6 \cdot 8 + 2$, devemos avançar dois dias da segunda-feira e assim descobrimos que a 50ª visita ocorrerá numa quarta-feira.

Problema 1.34. O ano de 2016 teve início numa sexta-feira. Em que dia cairá o último dia deste ano?

Solução. O objetivo desta questão é resolvê-la sem consultar o calendário.

Primeiramente vejamos que o ano de 2016 é bissexto e assim possui 366 dias. Se o 1º dia do ano caiu numa sexta-feira, também cairão numa sexta o 8º, 15º, 22º,... dias do ano, basta somar 7 aos dias que cairem numa sexta-feira. Notemos que os dias que cairão em sexta-feira deixam resto 1 na divisão por 7, logo, os dias que caem em sábado deixam resto 2, os que caem no domingo deixam resto 3 e assim por diante.

Dividindo 366 por 7 encontramos um resto 2, logo o último dia do ano de 2016 será sábado.

Nos problemas anteriores pudemos perceber a utilização dos restos na resolução de problemas, como os de fenômenos periódicos.

O conceito de resto surge quando um número natural $m \neq 0$ não divide o número N.

Teorema 1.35 (Divisão Euclidiana)**.** Sejam N e m dois números naturais com $m \neq 0$. Existem dois únicos números inteiros q e r tais que

$$N = mq + r, \text{ com } 0 \leq r < m$$

Os números q e r são denominados de quociente e resto da divisão.

Demonstração. Seja m um número natural não nulo. Se $N \in \mathbb{N}$, ou N é múltiplo de m ou está entre dois múltiplos consecutivos de m, isto é, $mq \leq N < m(q+1)$.

Como $mq \leq N$, existe um $r \in \mathbb{N}$ tal que $N = mq + r$. Provemos que $r < m$. Se r for maior ou igual a m, teremos $r = N - mq \geq m$, então $(N - mq) + mq \geq m + mq$ e assim, $N \geq m(q+1)$, o que não é possível. Logo, $N = mq + r$ com $r < m$.

Provemos agora a unicidade de q e r. Suponhamos que $N = q_1 m + r_1 = q_2 m + r_2$, com $r_1 \neq r_2$ e admitindo que $r_1 < m$ e $r_2 < m$ (conforme provamos anteriormente). Sem perda de generalidade, suponhamos ter $r_1 < r_2$, então $0 < r_1 - r_2 < m$. Da igualdade $q_1 m + r_1 = q_2 m + r_2$ decorre que $q_1 m + (r_1 - r_2) = q_2 m$, logo $r_1 - r_2$ é

divisível por m e disso segue que $m \leq r_1 - r_2$, o que é um absurdo. Portanto $r_1 = r_2$ e desta forma $q_1 = q_2$.

□

Exemplo 1.36. Na divisão de 23 por 6, o quociente e o resto são respectivamente 3 e 5, pois $23 = 6 \cdot 3 + 5$.

Problema 1.37. Encontre quantos múltiplos de 7 se encontram entre 1 e 423.

Solução. Pelo algoritmo da divisão euclidiana, $423 = 60 \cdot 7 + 3$. Logo, o maior múltiplo de 7 que cabe em 423 é $60 \cdot 7$, onde 60 é o quociente da divisão de 423 por 7. Desta forma, os múltiplos de 7 entre 1 e 423 são

$$1 \cdot 7, 2 \cdot 7, 3 \cdot 7, \ldots, 60 \cdot 7$$

que, em número, são 60 múltiplos.

Problema 1.38. Em um determinado país, cuja unidade monetária é a Merreca, existem notas de diversos valores, inclusive de 3 merrecas (M$3,00). Uma pessoa possui trinta e uma notas de M$50,00 e quarenta e sete notas de M$10,00; ela deseja trocar este dinheiro por notas de M$3,00. Qual vai ser o troco depois da pessoa receber as notas de 3 merrecas?

Solução. Basta encontrar o resto da divisão de $x = 31 \cdot 50 + 47 \cdot 10$ por 3. Todavia, não precisamos calcular a soma dos produtos, bastando substituir cada um dos números pelo resto obtido na divisão por 3. Então o número x fica $1 \cdot 2 + 2 \cdot 1 = 4$ que tem resto 1 na divisão por 3. Notemos que o resto da divisão de $x = 31 \cdot 50 + 47 \cdot 10 = 1550 + 470 = 2020$ por 3 é 1.

Este resultado nos leva a inferir o seguinte teorema que pode nos auxiliar na solução de diversos problemas:

Teorema 1.39. O resto da divisão por $m \neq 0$ da soma ou do produto de dois números naturais N_1 e N_2 é igual ao resto da divisão por $m \neq 0$ da soma ou do produto dos restos de N_1 e N_2, individualmente, na divisão por $m \neq 0$.

Demonstração. Vamos verificar o teorema acima para a soma e produto separadamente.

Provemos primeiramente que o resto da soma é a soma dos restos.

Consideremos dois números naturais N_1 e N_2, tais que sua soma $N_1 + N_2$ deixa resto r quando dividida por $m \neq 0$, e $0 \leq r < m$, isto é $N_1 + N_2 = mq + r$. Os restos das

divisões de N_1 e N_2 por m são respectivamente r_1 e r_2, com $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Desta forma, existem naturais q_1 e q_2 tais que $N_1 = mq_1 + r_1$ e $N_2 = mq_2 + r_2$. Temos assim:

$$N_1 + N_2 = mq_1 + r_1 + mq_2 + r_2 = m(q_1 + q_2) + r_1 + r_2$$

Consideremos agora $r_1 + r_2 = mq' + r'$ e $q_1 + q_2 = q"$, com $0 \leq r' < m$. Assim, $N_1 + N_2 = m(q_1 + q_2) + (r_1 + r_2) = mq" + mq' + r' = m(q" + q') + r'$. Logo, pela unicidade do resto $r = r'$.

Provemos agora que o resto do produto é o produto dos restos.

Consideremos dois números naturais N_1 e N_2, tais que o produto $N_1 \cdot N_2$ quando dividido por $m \neq 0$ deixa resto r, com $0 \leq r < m$, isto é $N_1 \cdot N_2 = mq + r$. Os restos das divisões de N_1 e N_2 por m são respectivamente r_1 e r_2, com $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Desta forma, existem naturais q_1 e q_2 tais que $N_1 = mq_1 + r_1$ e $N_2 = mq_2 + r_2$. Temos então,

$$N_1 \cdot N_2 = (mq_1 + r_1)(mq_2 + r_2) = m^2 q_1 q_2 + mq_1 r_2 + mq_2 r_1 + r_1 r_2 = m(mq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2$$

Consideremos agora $r_1 r_2 = mq' + r'$ e $mq_1 q_2 + q_1 r_2 + q_2 r_1 = q"$, com $0 \leq r' < m$. Assim, $N_1 \cdot N_2 = m(mq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 = mq" + mq' + r' = m(q' + q") + r'$. Pela unicidade do resto, $r = r'$.

□

Problema 1.40. Encontre o resto da divisão de

a) $1989 \cdot 1990 \cdot 1991 + 1995^3$ por 7

b) 9^{100} por 8

Solução

a) Calculemos separadamente os restos das divisões por 7 de 1989, 1990, 1991 e 1995^3 que são respectivamente 1, 2, 3 e 0. Conforme verificamos com o Teorema 1.39, o resto da divisão de $1989 \cdot 1990 \cdot 1991 + 1995^3$ por 7 é o mesmo resto da divisão de $1 \cdot 2 \cdot 3 + 0^3$ por 7, que é 6.

b) Como 9 deixa resto 1 na divisão por 8, e pelo Teorema 1.39, o resto da divisão do produto $\underbrace{9 \cdot 9 \cdots 9}_{100\ vezes} = 9^{100}$ por 8 é o produto dos restos $\underbrace{1 \cdot 1 \cdots 1}_{100\ vezes} = 1^{100} = 1$. Logo, o resto é 1.

Problema 1.41. Prove que, para qualquer número natural n, $n^3 + 2n$ é divisível por 3.

Solução. O resto da divisão de n por 3 pode ser 0, 1 ou 2. Analisemos então os três casos dos possíveis restos de n, utilizando o Teorema 1.39:

- Se o resto for 0, $n = 3k$ então $n^3 = 27k^3$ e $2n = 6k$. Logo, $n^3 + 2n = 27k^3 + 6k = 3(9k^3 + 2k)$ é divisível por 3;
- Se o resto for 1, $n = 3k+1$ então $n^3 = (3k+1)^3 = 27k^3+27k^2+9k+1$ e $2n = 6k+2$. Logo, $n^3 + 2n = (27k^3 + 27k^2 + 9k + 1) + (6k + 2) = 3(9k^3 + 9k^2 + 5k + 1)$ é divisível por 3;
- Se o resto for 2, $n = 3k + 2$ então $n^3 = (3k + 2)^3 = 27k^3 + 54k^2 + 48k + 8$ e $2n = 6k+4$. Logo, $n^3+2n = (27k^3+54k^2+48k+8)+(6k+4) = 3(9k^3+18k^2+18k+4)$ é divisível por 3;

Desta forma, para qualquer valor de n, $n^3 + 2n$ é divisível por 3.

Observação 1.42. Notemos que a solução do problema acima envolveu uma análise de casos para verificar todos os possíveis restos da divisão por algum número natural. Este método é muito importante e os estudantes precisam compreender que esta análise fornece uma demonstração rigorosa e completa.

A análise de casos também pode ser usada em diversas outras áreas além da aritmética e seria ideal se os alunos aprendessem a verificar quando a análise de casos pode ser aplicada na resolução de um problema.

Problema 1.43. A soma dos quadrados de três números naturais é divisível por 9. Prove que podemos escolher dois desses quadrados de modo que sua diferença seja divisível por 9.

Dica: Se dois números tiverem o mesmo resto ao serem divididos por 9, então sua diferença é divisível por 9.

Solução. Devemos mostrar que podemos escolher dois números quadrados que possuem o mesmo resto na divisão por 9.

Os restos possíveis na divisão de um natural por 9 são, 0, 1, 2, 3, 4, 5, 6, 7 e 8. Analisemos quais são os possíveis restos na divisão do quadrado de um número $n = 9q + r$ por 9:

- se $r = 0$, n^2 deixa resto 0;
- se $r = 1$, n^2 deixa resto 1;
- se $r = 2$, n^2 deixa resto 4;
- se $r = 3$, n^2 deixa resto 0;
- se $r = 4$, n^2 deixa resto 7;
- se $r = 5$, n^2 deixa resto 7;
- se $r = 6$, n^2 deixa resto 0;
- se $r = 7$, n^2 deixa resto 4;
- se $r = 8$, n^2 deixa resto 1.

Logo, os possíveis restos da divisão do quadrado de um número por 9 são 0, 1, 4 e 7.

A questão afirma que a soma dos quadrados de três números naturais é divisível por 9, então devemos combinar os possíveis restos da divisão de um quadrado por 9, de modo que a soma entre três deles seja divisível por 9:

- $0 + 0 + 0 = 0$
- $4 + 4 + 1 = 9$
- $7 + 1 + 1 = 9$
- $7 + 7 + 4 = 18$

Pela observação das combinações possíveis elencadas acima, pelo menos dois dos quadrados deixam o mesmo resto na divisão por 9 e, assim sua diferença é divisível por 9.

Problema 1.44. Encontre o resto da divisão de 2^{100} por 3.

Solução. Notemos que $2^{100} = 2^{2 \cdot 50} = 4^{50}$. Mas 4 deixa resto 1 na divisão por 3, logo 4^{50} também deixa resto 1.

Problema 1.45. Encontre o último algarismo do número 1989^{1989}.

Dica: O último algarismo de um número é o resto da divisão por 10 deste número.

Solução. Observemos que 1989 deixa resto 9 na divisão por 10, logo 1989^{1989} deixa o mesmo resto que 9^{1989} na divisão por 10, pelo Teorema 1.39.

$9^2 = 81$ e 81 deixa resto 1 na divisão por 10. Então podemos escrever $9^{1989} = (9^2)^{994} \cdot 9^1$, mas 9^2 deixa resto 1 na divisão por 10, logo $(9^2)^{994} \cdot 9^1$ deixa resto $1^{994} \cdot 9 = 9$. Assim, o último algarismo do número 1989^{1989} é 9.

Outra solução. Já concluímos anteriormente que o último algarismo de 1989^{1989} é igual ao último algarismo do número 9^{1989}. Analisemos os últimos algarismos das primeiras potências de 9:

- $9^1 = 9$
- $9^2 = 81$
- $9^3 = 729$
- $9^4 = 6561$

Para calcular o último algarismo de uma potência de 9, basta multiplicar por 9 o último algarismo da potência anterior de 9. Logo, o algarismo 9 é sempre seguido pelo algarismo 1 (pois $9 \cdot 9 = 81$), que por sua vez é seguido por 9 (porque $1 \cdot 9 = 9$).

Desta forma, as potências ímpares de 9 sempre têm seu último algarismo igual a 9. Assim, o último algarismo de 1989^{1989} é 9.

Observação 1.46. É interessante sugerir como exercício aos alunos a elaboração de tabelas de multiplicação para os restos das divisões pelos números mais utilizados: 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, ..., tentando encontrar todos os restos possíveis da divisão de quadrados e cubos perfeitos por esses números. Geralmente os problemas que envolvem quadrados podem ser solucionados usando os restos da divisão por 3 ou 4, pois os quadrados perfeitos quando divididos por 3 ou 4 deixam apenas os restos 0 e 1. Os problemas com cubos podem frequentemente ser resolvidos usando-se os restos das divisões por 7 ou 9, que só deixam três restos possíveis: $\{0, 1, 6\}$ e $\{0, 1, 8\}$, respectivamente.

Problema 1.47. Prove que o número $6n^3 + 3$ não pode ser a sexta potência de um natural, qualquer que seja o número natural n.

Solução. Devemos provar que $6n^3+3$ não pode ser o quadrado ou o cubo de um natural qualquer.

Para verificar que $6n^3 + 3$ não pode ser um cubo, basta analisar os restos possíveis na divisão por 7 e verificar que $6n^3+3$ deixa os restos $\{2, 3, 4\}$, enquanto cubos perfeitos deixam restos $\{0, 1, 6\}$ na divisão por 7. Logo, $6n^3 + 3$ não pode ser o cubo de um natural e assim não pode ser a sexta portência de um natural.

Problema 1.48. 1. Mostre que nenhum quadrado ou soma de dois quadrados é da forma $4n + 3$

2. Mostre que nenhum elemento da sequência $11, 111, 1111, \ldots$ é um quadrado ou soma de dois quadrados.

3. Idem para nenhum elemento das sequências seguintes:

$$44, 444, 4444, \ldots, \; 55, 555, 5555, \ldots, \; 99, 999, 9999, \ldots$$

Solução.

a) Os números naturais podem ser representados em alguma das seguintes formas, de acordo com seu resto na divisão por 4: $4k$, $4k + 1$, $4k + 2$ ou $4k + 3$. Logo,

- $(4k)^2 = 4(4k^2) = 4n_1$
- $(4k + 1)^2 = 16k^2 + 8k + 1 = 4n_2 + 1$
- $(4k + 2)^2 = 16k^2 + 16k + 4 = 4n_3$
- $(4k + 3)^2 = 16k^2 + 24k + 9 = 4n_4 + 1$

Logo, todo quadrado perfeito é da forma $4n$ ou $4n + 1$.

Consideremos todas as possíveis somas de quadrados:

- $4n + 4n' = 4(n + n') = 4a$
- $4n + 4n' + 1 = 4(n + n') + 1 = 4a + 1$
- $4n + 1 + 4n' + 1 = 4(n + n') + 2 = 4a + 2$

Desta forma, as somas de dois quadrados podem assumir as formas $4a$, $4a + 1$ ou $4a + 2$.

Portanto, nenhum quadrado ou soma de quadrados é da forma $4n + 3$.

b) Qualquer número M da sequência $11, 111, 1111, \ldots$ pode ser escrito na forma

$$M = 111\ldots100 + 11 = 4\alpha + 8 + 3 = 4n + 3,\ \alpha, n \in \mathbb{N}$$

Como M é da forma $4n + 3$, ele não é um quadrado perfeito nem soma de dois quadrados, conforme o item anterior.

c) Seja $N = 444\ldots4$, $P = 555\ldots5$ e $Q = 999\ldots9$.

$N = 444\ldots4 = 4 \cdot 111\ldots1 = 2^2 \cdot 111\ldots1$

Pelo item anterior o número $111\ldots1$ não é um quadrado perfeito, logo N não será quadrado de nenhum número natural.

$P = 555\ldots5 = 555\ldots500 + 55 = 4\beta + 52 + 3 = 4n + 3$, com $\beta, n \in \mathbb{N}$

Como P é da forma $4n + 3$, não é quadrado de nenhum número natural.

$Q = 999\ldots9 = 9 \cdot 111\ldots1 = 3^2 \cdot 111\ldots1$

Como $111\ldots1$ não é quadrado, logo Q também não o é.

Problema 1.49. Mostre que todo número natural possui um múltiplo que se escreve apenas com os algarismos 0 e 1.

Solução. Considere os $n+1$ primeiros números da sequência $11, 111, 1111, \ldots$. Divida-os por n e considere os restos dessas divisões. Esses restos só podem ser iguais a $0, 1, 2, \ldots n-1$. Pensando nos $n+1$ números como pombos e nos n possíveis restos como casas, temos mais pombos do que casas. O Princípio da Casa dos Pombos nos garante que haverá pelo menos dois números que deixam o mesmo resto na divisão por n, suponhamos que sejam $11\ldots1$ (com x algarismos) e $111\ldots1$ (com y algarismos), tal que $x < y$.

A diferença entre esses números é múltipla de n e é escrita como

$$111\ldots1 - 11\ldots1 = 11\ldots100\ldots0, \text{ com } x \text{ algarismos iguais a } 0 \text{ e } y - x \text{ algarismos iguais a } 1.$$

1.4 Algoritmo de Euclides

Na seção 1.2.1 apresentamos o conceito de Máximo Divisor Comum e dois métodos para encontrá-lo utilizando a decomposição dos números: a fatoração simultânea e a intersecção das decomposições através de diagramas de Venn, métodos que são equivalentes. Agora apresentaremos um método para o cálculo do *mdc* denominado Algoritmo de Euclides e estudaremos algumas propriedades.

Este algoritmo é baseado na seguinte propriedade:

Se d é um divisor comum de dois números naturais a e b $(a < b)$, d também divide o número $b - na$. Reciprocamente, se d divide a e $b - na$, então d também divide b.

Que pode ser sintetizada no seguinte lema:

Lema 1. Seja $a, b, n \in \mathbb{N}$. Se existe o $mdc(a, b - na)$, então existe o $mdc(a, b)$ e $mdc(a, b - na) = mdc(a, b)$.

Demonstração. Seja $d = mdc(a, b - na)$. Como d é divisor de a e de $b - na$, d também é divisor de $b = b - na + na$. Segue que d é um divisor comum de a e b. Seja c um outro divisor comum de a e b, então c também é um divisor comum de a e $b - na$ e assim c é divisor de $d = mdc(a, b)$. Portanto, $d = mdc(a, b)$, pois d é o maior de todos os divisores comuns de a e $b - na$. □

Apresentamos agora uma prova construtiva da existência do mdc aplicando sucessivamente, a partir de a e b, o algoritmo da divisão da seguinte maneira:

$$\begin{gathered} a = bq_1 + r_1 \text{ com } (r_1 < b) \\ b = r_1q_2 + r_2 \text{ com } (r_2 < r_1) \\ r_1 = r_2q_3 + r_3 \text{ com } (r_3 < r_2) \\ \vdots \end{gathered}$$

Se tivermos $r_1 = 0$, então $b = mdc(a, b)$ e o processo se encerra na primeira etapa. De qualquer forma, na sequência $b > r_1 > r_2 > r_3 > \ldots$ para algum r_n teremos $r_{n+1} = 0$, pois caso contrário, a sequência de números naturais $b > r_1 > r_2 > r_3 > \ldots$ não teria mínimo, o que não é possível. Logo, para algum n:

$$\begin{gathered} r_{n-2} = r_{n-1}q_n + r_n \\ r_{n-1} = r_nq_{n+1} \end{gathered}$$

Desta forma, podemos obter o seguinte:

$$\begin{gathered} r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \cdots = mdc(b, r_1) = mdc(a, b) \\ \text{Logo, } r_n = mdc(a, b) \end{gathered}$$

Esse dispositivo prático utilizado para a demonstração construtiva da existência do mdc é denominado *processo das divisões sucessivas.*

O uso desta propriedade nos fornece um método eficaz para o cálculo do mdc, pois em vez de utilizar a fatoração dos números, como os métodos apresentados anteriormente, ele permite que possamos reduzir sucessivamente através da subtração, o cálculo do mdc de dois números naturais para o cálculo do mdc de números cada vez menores.

Exemplo 1.50. Calcule e $mdc(257, 39)$.

Solução.

$$\begin{aligned} mdc(257, 39) &= mdc(257 - 6 \cdot 39, 39) \\ &= mdc(23, 39) = mdc(23, 39 - 1 \cdot 23) \\ &= mdc(23, 16) = mdc(23 - 1 \cdot 16, 16) \\ &= mdc(7, 16) = mdc(7, 16 - 2 \cdot 7) \\ &= mdc(7, 2) = mdc(7 - 3 \cdot 2, 2) \\ &= mdc(1, 2) = 1 \end{aligned}$$

Vejamos abaixo como utilizar o Algoritmo através de um diagrama.

Primeiramente realizamos a divisão $a = bq_1 + r_1$ e colocamos os números em uma tabela da seguinte maneira:

	q_1
a	b
r_1	

Em seguida, realizamos a divisão $b = r_1q_2 + r_2$ e completamos a tabela conforme consta abaixo:

	q_1	q_2
a	b	r_1
r_1	r_2	

Repetimos este processo enquanto for possível até que se tenha:

	q_1	q_2	q_3	$\ldots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-2}	r_{n-1}	$r_n = mdc(a, b)$
r_1	r_2	r_3	r_4	$\ldots$	r_n		

Vejamos como ficaria o exemplo anterior utilizando-se da estrutura do diagrama:

	6	1	1	2	3	2
257	39	23	16	7	2	$1 = mdc(257, 39)$
23	16	7	2	1	0	

Capítulo 2

Congruências

Após o aprendizado do conceito de restos e sua ampla utilização na resolução de exercícios, é possível introduzir com naturalidade o conceito de congruência através da seguinte definição:

Definição 2.1. Dois inteiros a e b são congruentes módulo m quando eles deixam o mesmo resto na divisão por m, escrevendo-se

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

Exemplo 2.2. $22 = 7 \cdot 3 + 1$ e $37 = 12 \cdot 3 + 1$

Como 22 e 37 deixam o mesmo resto na divisão por 3, podemos dizer que 22 é congruente com 37 módulo 3, ou seja $22 \equiv 37 \pmod{3}$

Depois da apresentação da definição de congruência, é interessante que os alunos demonstrem as propriedades como forma de exercícios, o que pode ser realizado com razoável facilidade através da utilização dos conceitos anteriormente aprendidos de restos e divisão euclidiana.

Problema 2.3. Mostre que $a \equiv b \pmod{m}$, se e somente se, $a - b$ é divisível por m.

Solução. Seja r o resto comum da divisão de a e b por m. Assim podemos escrever

$$a = mk_1 + r \text{ e } b = mk_2 + r$$

Portanto, $a - b = mk_1 + r - mk_2 - r = m(k_1 - k_2)$ e com isso, $a - b$ é divisível por m.

Reciprocamente, se $a-b$ é divisível por m, a e b deixam algum resto na divisão por m, digamos r_1 e r_2. Temos então

$$a = mk_1 + r_1 \text{ e } b = mk_2 + r_2$$

Mas $a - b = mk_1 + r_1 - mk_2 - r_2 = m(k_1 - k_2) + r_1 - r_2$ é divisível por m, logo $r_1 - r_2$ também é divisível por m, como $\mid r_1 - r_2 \mid < m$, temos que $r_1 = r_2$ e assim $a \equiv b \pmod{m}$.

Problema 2.4. Prove que se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:
i) $a + c \equiv b + d \pmod{m}$ ii) $a - c \equiv b - d \pmod{m}$
iii) $ac \equiv bd \pmod{m}$ iv) $a^n \equiv b^n \pmod{m}$

Solução.
i) Como $a \equiv b \pmod{m}$, então $a-b \equiv 0 \pmod{m}$, conforme demonstrado no problema anterior. Assim, temos também que $c - d \equiv 0 \pmod{m}$. Desta forma, podemos escrever $(a-b)+(c-d) \equiv 0 \pmod{m} \iff (a+c)-(b+d) \equiv 0 \pmod{m} \iff a+c \equiv b+d \pmod{m}$.

ii) Analogamente ao item anterior, podemos escrever $(a-b)-(c-d) \equiv 0 \pmod{m} \iff (a-c)-(b-d) \equiv 0 \pmod{m} \iff a-c \equiv b-d \pmod{m}$

iii) Notemos que $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d)$. Como $a-b$ e $c-d$ são divisíveis por m, então $ac - bd$ também o é.

iv) Podemos provar por indução sobre n.

1) Para $n = 1$ é válido pois, por hipótese, $a^1 \equiv b^1 \pmod{m}$.

2) Suponhamos que $a^n \equiv b^n \pmod{m}$. Queremos provar que $a^{n+1} \equiv b^{n+1} \pmod{m}$.

Como $a^n \equiv b^n \pmod{m}$ e $a \equiv b \pmod{m}$, pelo que foi demonstrado no item iii) desta questão, podemos multiplicar as congruências do seguinte modo: $a^n \cdot a \equiv b^n \cdot b \pmod{m}$. Assim, $a^{n+1} \equiv b^{n+1} \pmod{m}$ e a propriedade é válida para todo $n \in \mathbb{N}$, com $n > 1$.

Podemos sintetizar as propriedades já demonstradas e acrescentar outras na proposição abaixo:

Proposição 2.5. Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:

i) $a + c \equiv b + d \pmod{m}$
ii) $a - c \equiv b - d \pmod{m}$
iii) $ac \equiv bd \pmod{m}$
iv) $a^n \equiv b^n \pmod{m}$, $\forall n \in \mathbb{N}$
v) $ka \equiv kb \pmod{m}$, $\forall k \in \mathbb{Z}$
vi) Se $mdc(n, m) = d > 0$, então $na \equiv nb \pmod{m} \iff a \equiv b \pmod{\frac{m}{d}}$

Em síntese, podemos realizar quase todas as operações elementares envolvendo a igualdade de inteiros, com excessão da divisão. Vejamos abaixo a demonstração do item vi).

Demonstração. (Item vi) Por hipótese, $na \equiv nb \pmod{m}$, logo $na - nb = mk \iff n(a - b) = mk$, para algum $k \in \mathbb{Z}$. Daí, $\frac{n}{d}(a - b) = \frac{m}{d}k$, onde $mdc(\frac{n}{d}, \frac{m}{d}) = 1$. Disso temos que $a - b$ é divisível por $\frac{m}{d}$ e portanto, $a \equiv b \pmod{\frac{m}{d}}$. □

Corolário 2.6. Se $na \equiv nb \pmod{m}$ e $mdc(n, m) = 1$, então $a \equiv b \pmod{m}$.

Problemas de análise de casos como os vistos no capítulo anterior também podem ser resolvidos através de congruências. Vejamos um exemplo:

Problema 2.7. Mostre que, para qualquer inteiro n, $n^2 + 1$ não é divisível por 3.

Solução. Qualquer inteiro n deixa resto 0, 1 ou 2 na divisão por 3. Então podemos ter $n \equiv 0 \pmod{3}$, $n \equiv 1 \pmod{3}$ ou $n \equiv 2 \pmod{3}$. Com isso podemos analisar as possibilidades:

- Se $n \equiv 0 \pmod{3}$, então $n^2 + 1 \equiv 1 \pmod{3}$;
- Se $n \equiv 1 \pmod{3}$, então $n^2 + 1 \equiv 2 \pmod{3}$;
- Se $n \equiv 2 \pmod{3}$, então $n^2 + 1 \equiv 2 \pmod{3}$.

Portanto, em qualquer caso, $n^2 + 1$ nunca é divisível por 3.

Problema 2.8. Encontre o resto da divisão de 5^{100} por 6.

Solução. Como $5 - (-1) = 5 + 1 = 6$, temos que $5 \equiv -1 \pmod{6}$. Elevando a 100, $5^{100} \equiv (-1)^{100} \pmod{6} \Longrightarrow 5^{100} \equiv 1 \pmod{6}$.

Logo, 5^{100} deixa resto 1 na divisão por 6.

Problema 2.9. Mostre que $30^{99} + 61^{100}$ é divisível por 31.

Solução.

$$30 \equiv -1 \pmod{31}, \text{ logo } 30^{99} \equiv (-1)^{99} = -1 \pmod{31}$$
$$61 \equiv -1 \pmod{31}, \text{ logo } 61^{100} \equiv (-1)^{100} = 1 \pmod{31}$$

Desta forma, $30^{99} + 61^{100} \equiv -1 + 1 = 0 \pmod{31}$.

Problema 2.10. Se n é ímpar, prove que $1^n + 2^n + \cdots + (n-1)^n$ é divisível por n.

Solução. Sendo n ímpar, os restos das divisões de k^n e $(n-k)^n$ possuem sinais opostos. Como de 1^n a $(n-1)^n$ temos uma quantidade par de fatores e os restos dos fatores k^n e $(n-k)^n$ se anulam, o número $1^n + 2^n + \cdots + (n-1)^n$ é divisível por n.

Problema 2.11. Encontre o algarismo das unidades dos números 7^{7^7} e 9^{9^9}.

Solução. 1ª parte. Como $7 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^3 \equiv 3 \pmod{10}$ e $7^4 \equiv 1 \pmod{10}$, temos que $7^n \equiv 7, 9, 3 \text{ ou } 1 \pmod{10}$, quando $n \equiv 1, 2, 3 \text{ ou } 0 \pmod{4}$, respectivamente.

Temos também que $7 \equiv 3 \pmod{4}$, $7^2 \equiv 1 \pmod{4}$, $7^3 \equiv 3 \pmod{4}$, $7^4 \equiv 1 \pmod{4}$,.... Isto é, $7^m \equiv 3 \text{ ou } 1 \pmod{4}$, conforme m seja ímpar ou par. Como 7 é ímpar, $7^7 \equiv 3 \pmod{4}$. Então, $7^{7^7} \equiv 3 \pmod{10}$.

Desta forma, o algarismo das unidades de 7^{7^7} é 3.

2ª parte. Temos que:

$$\begin{aligned} 9^1 &\equiv 9 \pmod{10} \\ 9^2 &\equiv 1 \pmod{10} \\ 9^3 &\equiv 9 \cdot 1 = 9 \pmod{10} \\ 9^4 &\equiv 1 \pmod{10} \\ &\vdots \end{aligned}$$

Logo, $9^r \equiv 9 \text{ ou } 1 \pmod{10}$, se r for respectivamente ímpar ou par. Como 9 é ímpar, $9^9 \equiv 9 \pmod{10}$ e assim, 9^9 é ímpar, o que implica que $9^{9^9} \equiv 9 \pmod{10}$, ou seja, o algarismo das unidades de 9^{9^9} é o 9.

2.1 Bases Numéricas

Em nossa cultura, a utilização da base decimal está inserida de tal maneira que qualquer estudante compreende a quantidade representada por um número, por exemplo 5462, e sabe descrevê-lo da seguinte forma: o último algarismo representa o número

de unidades, o penúltimo, o número de dezenas, o antepenúltimo, a quantidade de centenas e assim sucessivamente. E este modo de representar os números é chamado de sistema de base numérica decimal. Desta forma, ao escrevermos 5462, pensamos no número $5 \cdot 1000 + 4 \cdot 100 + 6 \cdot 10 + 2 \cdot 1 = 5 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10^1 + 2 \cdot 10^0$, e assim podemos observar que qualquer número pode ser escrito como uma soma de diferentes potências de dez com coeficientes que assumem valores de 0 até 9. Como utilizamos dez símbolos para escrever um número, 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9, esse sistema é denominado decimal.

Mas também podemos utilizar outros números como base, por exemplo o 8 e assim precisaremos de apenas oito símbolos: 0, 1, 2, 3, 4, 5, 6 e 7. O número 8 será a unidade do próximo nível e por isso será escrito como 10. Vejamos abaixo como alguns números na base decimal são escritos no sistema de base 8 (utilizaremos a simbologia $[ab]_x$ para dizer que o número ab está escrito na base x, quando $x \neq 10$):

$$9 = 1 \cdot 8^1 + 1 \cdot 8^0 = [11]_8$$
$$64 = 1 \cdot 8^2 + 0 \cdot 8^1 + 0 \cdot 8^0 = [100]_8$$
$$15 = 1 \cdot 8^1 + 7 \cdot 8^0 = [17]_8$$

Podemos construir um sistema numérico com qualquer número natural n maior que 1 como base desse sistema, onde relacionamos os algarismos com sua representação como soma de múltiplos de potências de n.

Um número em um sistema de base n é representado da seguinte forma

$$a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n^1 + a_0 n^0$$

Com a_k assumindo valores de 0 a $n - 1$.

Podemos descobrir a representação de um número que está na base decimal para outra base através do método das divisões sucessivas. Vejamos abaixo a representação do número 27 na base binária (base 2):

$$27 = 13 \cdot 2 + 1$$
$$13 = 6 \cdot 2 + 1$$
$$6 = 3 \cdot 2 + 0$$
$$3 = 1 \cdot 2 + 1$$
$$1 = 0 \cdot 2 + 1$$

Logo, $27 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = [11011]_2$

Exemplo 2.12. Represente o número 2584 na base 11.

Solução. Como o sistema pedido é maior que 10, precisaremos de mais de 10 símbolos para representar todos os algarismos, então podemos utilizar a para representar o "algarismo"10, tendo assim os seguintes algarismos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 e a. Assim, o número 2584 será escrito como

$$\begin{aligned} 2584 &= 234 \cdot 11 + 10 \\ 234 &= 21 \cdot 11 + 3 \\ 21 &= 1 \cdot 11 + 10 \\ 1 &= 0 \cdot 11 + 1 \end{aligned}$$

Assim, $2584 = [1a3a]_{11}$.

Podemos realizar operações como somar e multiplicar números escritos em qualquer base, do mesmo modo que fazemos na base decimal, atendo-se ao fato de que "vai um"sempre que o resultado da soma em uma coluna for maior ou igual à base do sistema numérico dado.

Vejamos como somar os números $[1203]_4$ e $[101]_4$, que estão na base 4:

$$\begin{array}{cccc} & & {\scriptstyle 1} & \\ 1 & 2 & 0 & 3 \\ + & 1 & 0 & 1 \\ \hline 1 & 3 & 1 & 0 \end{array}$$

Assim $[1203]_4 + [101]_4 = [1310]_4$.

Realizemos agora a multiplicação entre os números $[112]_4$ e $[13]_4$.

$$\begin{array}{cccc} & {\scriptstyle 1} & {\scriptstyle 1} & \\ & 1 & 1 & 2 \\ & \mathrm{x} & 1 & 3 \\ \hline & 1 & 0 & 0 & 2 \\ + & 1 & 1 & 2 & \\ \hline & 2 & 1 & 2 & 2 \end{array}$$

Portanto, $[112]_4 \cdot [13]_4 = [2122]_4$.

Para realizar com maior facilidade as operações de soma e multiplicação é necessário consultar as tabelas de adição e subtração dos números menores que a base do sistema. Para a base 10, as crianças aprendem a construí-las e memorizá-las logo nas séries iniciais. Vejamos a tabela de multiplicação na base 4:

$0 \times 0 = 0$	$1 \times 1 = 1$	$2 \times 0 = 0$	$3 \times 0 = 0$	$4 \times 0 = 0$
$0 \times 1 = 0$	$1 \times 2 = 2$	$2 \times 1 = 2$	$3 \times 1 = 3$	$4 \times 1 = 10$
$0 \times 2 = 0$	$1 \times 3 = 3$	$2 \times 2 = 10$	$3 \times 2 = 12$	$4 \times 2 = 20$
$0 \times 3 = 0$	$1 \times 4 = 10$	$2 \times 3 = 12$	$3 \times 3 = 21$	$4 \times 3 = 30$

Ao propor aos alunos atividades que envolvam a adição ou a multiplicação em alguma base arbitrária, seria interessante sugerir-lhes que construam as tabelas de adição e multiplicação na respectiva base.

2.2 Representação decimal e testes de divisibilidade

Antes mesmo de desenvolver o algoritmo da divisão é possível saber se um número escrito na base decimal é divisível por outro apenas através da observação e análise dos algarismos que o compõe. Por exemplo, sabemos que um número é divisível por 2 se o seu último algarismo o for; sabemos que é divisível por 5 se seu último algarismo for 0 ou 5. Esses critérios de divisibilidade foram obtidos através da expansão decimal dos números, por meio da qual também é possível obter critérios de divisibilidade por vários outros números. O uso das congruências é uma grande ferramenta para trabalhar com os critérios de divisibilidade.

Com o advento da calculadora, tornou-se muito mais simples detectar se um número é ou não divisível por outro, bastando simplesmente fazer a divisão na calculadora. Entretanto, para uma maior apreciação da matemática, os critérios de divisibidade são uma janela interessante para que os alunos explorem a natureza dos números e suas propriedades. Por esta razão, este tema ainda encontra espaço no espectro do ensino da matemática e deve ser apresentado aos alunos, não como algo a ser memorizado, mas como um tópico de "diversão", onde o aluno deve tentar compreender as bases desses critérios e até mesmo obter novos critérios de divisibilidade além dos apresentados.

Com esta seção, os alunos não terão apenas uma lista de critérios de divisibilidade, mas terão também uma visão interessante sobre a Teoria dos Números.

Primeiramente é necessário compreender a seguinte identidade:

$$\overline{a_n \dots a_1 a_0} = a_n \cdot 10^n + \cdots + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

Onde o número com um traço, à esquerda da igualdade, está representado na base decimal de modo usual e à direita encontra-se a expansão decimal do número. Por exemplo, $\overline{abc} = 100a + 10b + c$.

O traço usado sobre os números servirá para diferenciar o número $\overline{a_n \dots a_1 a_0}$ do produto $a_n \cdots a_1 \cdot a_0$.

Vejamos o exemplo seguinte que explora a representação descrita acima.

Exemplo 2.13. (OBMEP - Banco de Questões 2015) Sejam a e b dois dígitos diferentes de zero não necessariamente diferentes. O número de dois dígitos $\overline{ab}$ é chamado de curioso se ele for um divisor do número $\overline{ba}$, que é formado pela troca de ordem dos dígitos de $\overline{ab}$. Ache todos os números curiosos.

Solução. Os números $\overline{ab}$ e $\overline{ba}$ são escritos respectivamente como $\overline{ab} = 10a + b$ e $\overline{ba} = 10b + a$. O número $\overline{ab}$ será curioso se existir $k \in \mathbb{N}$ tal que $k \cdot \overline{ab} = \overline{ba}$, ou seja, $k(10a + b) = 10b + a$. Notemos que, como $\overline{ab}$ e $\overline{ba}$ possuem dois dígitos, k deve ser menor ou igual a 9.

$$\begin{gathered} k(10a + b) = 10b + a \\ 10ak + bk = 10b + a \\ 10ak + bk + 10a + b = 10b + a + 10a + b \\ (10a + b)(k + 1) = 11(a + b) \end{gathered}$$

Pela última equação podemos concluir que o número $(10a + b)(k + 1)$ é múltiplo de 11, mas $k \leq 9$, então $k + 1 \leq 10$ e não possui nenhum fator 11. Logo $10a + b$ é múltiplo de 11. Todos os múltiplos de 11 com dois dígitos possuem dígitos repetidos, logo $a = b$. Se $a = b$, então $\overline{ab} = \overline{ba}$ e um divide o outro. Então, o conjunto dos números curiosos é:

$$\{11, 22, 33, 44, 55, 66, 77, 88, 99\}$$

A seguir, vamos enunciar e demonstrar alguns critérios de divisibilidade. Alguns deles podem ser deixados como exercícios para os alunos.

Divisibilidade por 2: Um número natural é divisível por 2, se e somente se, o algarismo das unidades do número for 0, 2, 4, 6 ou 8.

Demonstração. Como $10 \equiv 0 \pmod 2$, segue que $10^i \equiv 0 \pmod 2$ e $a_i 10^i \equiv 0 \pmod 2$ e assim $a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \equiv 0 + 0 + \ldots 0 + 0 + a_0 \pmod 2$, ou seja, $\overline{a_n a_{n-1} \ldots a_1 a_0} \equiv a_0 \pmod 2$ Assim, o número $\overline{a_n a_{n-1} \ldots a_1 a_0}$ será divisível por 2 se a_0 for divisível por 2 ou for igual a 0. □

Divisibilidade por 4: Um número natural é divisível por 4 se o número formado pelos seus dois últimos dígitos o for.

Demonstração. Como $100 \equiv 0 \pmod 4$, todas as potências de 10 acima de 100 também são divisíveis por 4, assim $a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \equiv 0 + 0 + \ldots 0 + a_1 10 + a_0 \pmod 4$, ou seja, $\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv \overline{a_1 a_0} \pmod 4$. Desta forma, $\overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$ será divisível por 4 se $\overline{a_1 a_0}$ for igual a $\{00, 04, 08, 12, 16, 20, \ldots, 92, 96\}$. □

Problema 2.14. Prove que, se o último algarismo do quadrado de um número natural é 6, então seu penúltimo algarismo é ímpar.

Solução. O quadrado de um número par também é par, bem como o quadrado de um número ímpar também é ímpar. Com isso podemos concluir que o número é par, pois é terminado em 6. Sendo um número múltiplo de 2, seu quadrado será múltiplo de 4. Assim, pelo critério de divisibilidade por 4 acima descrito, o número formado pelos dois últimos algarismos pode ser $\{16, 36, 56, 76, 96\}$, que são mútilplos de 4 terminados em 6. E em todos eles o algarismo das centenas é ímpar.

Divisibilidade por potências de 2 e 5: Um número natural é divisível por 2^n ou 5^n se o número formado por seus n últimos algarismos for divisível por 2^n ou 5^n, respectivamente.

Demonstração. Temos que $10 = 2 \cdot 5$, logo $10^n = 2^n \cdot 5^n$. Dado um número natural a, seja p o número formado por seus n últimos algarismos. Assim, $a = k10^n + p$ e como 10^n é divisível por 2^n e por 5^n, a também será divisível por 2^n ou por 5^n se p o for. □

Por exemplo, um número é divisível por $8 = 2^3$ se o número formado pelos três últimos algarismos deste número for divisível por 8.

Divisibilidade por 7, 11 ou 13: Um número natural $a = \overline{a_n a_{n-1} \dots a_2 a_1 a_0}$, escrito na base 10, é divisível por 7, 11 ou 13 se, e somente se,

$$\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots \equiv 0 \pmod 7, \pmod{11}, \pmod{13}$$

Demonstração. Usaremos o fato de que $10^3 \equiv -1 \pmod 7, \pmod{11}, \pmod{13}$. Logo, $10^{3k} \equiv (-1)^{3k} \equiv (-1)^k \pmod 7, \pmod{11}, \pmod{13}$.

Com isso, temos que

$$\begin{cases} 10^{3k} \equiv -1 \pmod 7, \pmod{11}, \pmod{13} & \text{se } k \text{ é ímpar;} \\ 10^{3k} \equiv 1 \pmod 7, \pmod{11}, \pmod{13} & \text{se } k \text{ é par} \end{cases}$$

Observemos que

$$a = a_k 10^k + \dots + a_8 10^8 + a_7 10^7 + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 =$$
$$a_k 10^k + \dots + (a_8 10^2 + a_7 10 + a_6)10^6 + (a_5 10^2 + a_4 10 + a_3)10^3 + (a_2 10^2 + a_1 10 + a_0).$$

Daí temos $\begin{cases} k \cdot 10^{3k} \equiv -k \pmod 7, \pmod{11}, \pmod{13} & \text{se } k \text{ é ímpar;} \\ k \cdot 10^{3k} \equiv k \pmod 7, \pmod{11}, \pmod{13} & \text{se } k \text{ é par;} \end{cases}$

Assim,

$$a \equiv \dots + (a_8 10^2 + a_7 10 + a_6) - (a_5 10^2 + a_4 10 + a_3) + (a_2 10^2 + a_1 10 + a_0) \pmod 7, \pmod{11}, \pmod{13}$$
$$a \equiv \dots + \overline{a_8 a_7 a_6} - \overline{a_5 a_4 a_3} + \overline{a_2 a_1 a_0} \pmod 7, \pmod{11}, \pmod{13}$$

□

Podemos encontrar critérios de divisibilidade para vários números primos, como 2, 3, 5, 7, 11, 13,... E também podemos estender esta lista com números compostos. É divertido e pode ampliar a percepção matemática dos alunos. Todavia, devemos ressaltar que os números primos possuem critérios de divisibilidade independentes, ao passo que os números compostos não. Um número dado é divisível por um número composto se for divisível por cada um de seus fatores primos.

Divisibilidade por 6: Um número natural é divisível por 6 se for divisível por 2 e 3 ao mesmo tempo.

Divisibilidade por 3 ou 9: Um número natural é divisível por 3 (ou por 9) se o número formado pela soma de seus dígitos for divisível por 3 (ou por 9).

Demonstração. Como $10 \equiv 1 \pmod 3, \pmod 9$, temos que $a_i 10^i \equiv a_i \pmod 3, \pmod 9$. Seja $a = \overline{a_n \dots a_2 a_1 a_0}$, então

$$a = \overline{a_n \dots a_2 a_1 a_0} \equiv a_n + \dots + a_2 + a_1 + a_0 \pmod 3, \pmod 9$$

□

Problema 2.15. O número $a15b$ é divisível por 15. Encontre os valores de a e b.

Solução. Para que um número seja divisível por 15 é necessário que o mesmo seja divisível por 3 e por 5. Para ser divisível por 5 o número deverá terminar em 0 ou em 5 e para ser divisível por 3 a soma dos dígitos do número deve ser múltipla de 3. Analisemos as possibilidades:

- Se $b = 0$, devemos ter $a + 1 + 5 + 0 = 3k$ podendo obter $a = 3$, $a = 6$ ou $a = 9$
- Se $b = 5$, devemos ter $a + 1 + 5 + 5 = 3k$ podendo obter $a = 1$, $a = 4$ ou $a = 7$

Assim, temos seis possibilidades diferentes para formar o número $a15b$:

$$3150,\ 6150,\ 9150,\ 1155,\ 4155 \text{ ou } 7155.$$

O critério de divisibilidade por 9 mostra-se muito útil para diversas aplicações que podem fascinar os alunos, conforme veremos mais adiante.

2.3 Raiz digital

Para os tópicos que veremos à frente, será necessário utilizarmos o conceito de raiz digital, definido em [4].

O resultado da soma recursiva dos dígitos de um número inteiro até que reste apenas um dígito é conhecido como raiz digital do número.

O procedimento de somar os algarismos de um número resulta no resto da divisão do referido número por 9, conforme vimos acima. Logo, a raiz digital de um inteiro a também pode ser definida como o resto da divisão de a por 9. Dizer que um número possui raiz digital 0 ou 9 é o mesmo que dizer que o número é múltiplo de 9.

Exemplo 2.16. $2016 \equiv 2 + 0 + 1 + 6 \pmod 9$

$2016 \equiv 9 \equiv 0 \pmod 9$

Logo, a raiz digital de 2016 é 0.

A maneira mais rápida de se chegar a uma raiz digital é suprimindo os noves na soma dos dígitos do número dado, visto que $9 \equiv 0 \pmod 9$.

Por exemplo, vamos encontrar a raiz digital do número 892991.

$$892991 \equiv 8 + 2 + 1 \pmod 9$$
$$892991 \equiv 11 \pmod 9, \text{ mas } 11 \equiv 2 \pmod 9, \text{ daí}$$
$$892991 \equiv 2 \pmod 9$$

Com base nessa propriedade, existe uma grande quantidade de truques numéricos (também conhecidos como matemágicas) onde aparentemente chega-se a um número aleatório, mas na realidade chega-se a um número com raiz digital 9.

2.3.1 Truques numéricos ou Matemágicas

Utilizando-se do fato de que todo número é congruente a soma de seus algarismos módulo 9, pode-se criar truques onde o "mágico"aparenta adivinhar o número oculto resultante de operações aparentemente aleatórias, mas que na verdade chegam a um número com raiz digital 9. Com o número de raiz digital 9, o "mágico"pode pedir a pessoa que oculte um dígito do número, exceto 0, e fale ao "mágico"os dígitos restantes em qualquer ordem. O "mágico", sabendo que o número original possuía raiz digital 9, irá acrescentar ao número fornecido o algarismo necessário para que a soma dos dígitos volte a ter raiz digital 9. Por exemplo, se a pessoa, após ocultar um algarismo, fornece o número 82731, notaremos que $8+2+7+3+1 \equiv 3 \pmod 9$, e assim concluímos que o número ocultado foi o 6, pois $3 + 6 = 9$.

Para se chegar a um número com raiz digital 9 existem vários procedimentos. Vejamos alguns deles.

1. Anote um número qualquer e reorganize aleatoriamente os dígitos formando um novo número. Subtraia o menor do maior e o número obtido será múltiplo de 9.

   Demonstração. Seja $\overline{a_n \dots a_1 a_0}$ o número escolhido. Sua raiz digital será $a_n + \cdots + a_1 + a_0$, pois $\overline{a_n \dots a_1 a_0} \equiv a_n + \cdots + a_1 + a_0 \pmod 9$. Reacomodando os dígitos do número original obtemos um novo número, mas cuja raiz permanece a mesma do número original, por exemplo, $\overline{a_2 a_n \dots a_{n-1} a_0} \equiv a_2 + a_n + \dots a_{n-1} + a_0 = a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 9$, logo, a subtração entre os números implica na subtração das raízes digitais, que são iguais, logo a subtração dessas raízes será 0 e assim a diferença entre os números será um múltiplo de 9. □

Exemplo: Número escolhido: 67231

Embaralhamento: 17263

Subtraindo o menor do maior: $67231 - 17263 = 49968$

$49968 \equiv 4 + 6 + 8 = 18 \equiv 0 \pmod 9$

2. Anote um número qualquer, some todos os seus dígitos e subtraia o resultado do número original. O número obtido será múltiplo de 9.

   Demonstração. Sabemos que todo número é congruente à soma de seus dígitos módulo 9. Pelo que foi demonstrado na resolução do problema 2.3, a subtração de dois números congruentes módulo m é múltipla de m. Assim, um número subtraído da soma de seus algarismos é múltiplo de 9.

   Também é possível observar a veracidade deste método para obter um número com raiz digital 9 da seguinte maneira:

   Seja $\overline{a_n \dots a_1 a_0}$ o número escolhido. Sabemos que $\overline{a_n \dots a_1 a_0} \equiv a_n + \cdots + a_1 + a_0 \pmod 9$. Subtraindo do número original a soma dos seus dígitos teremos

   $$\overline{a_n \dots a_1 a_0} - (a_n + \cdots + a_1 + a_0) \equiv (a_n + \cdots + a_1 + a_0) - (a_n + \cdots + a_1 + a_0) \pmod 9$$

   $$\overline{a_n \dots a_1 a_0} - (a_n + \cdots + a_1 + a_0) \equiv 0 \pmod 9$$

   Logo, um número menos a soma de seus dígitos resulta em um número com raiz digital 9. □

   Exemplo: Número escolhido: 8135

   Soma dos dígitos: $8 + 1 + 3 + 5 = 17$

   Subtração: $8135 - 17 = 8118$

   $8118 \equiv 8 + 1 + 1 + 8 = 18 \pmod 9 \equiv 0 \pmod 9$

3. Anote um número qualquer, some seus dígitos, multiplique essa soma por 8 e some o resultado ao número original. O número obtido será múltiplo de 9.

   Demonstração. Seja $\overline{a_n \dots a_1 a_0}$ o número escolhido. Partiremos do fato de que $\overline{a_n \dots a_1 a_0} \equiv a_n + \cdots + a_1 + a_0 \pmod 9$. Somando $8(a_n + \cdots + a_1 + a_0)$ teremos

$$\overline{a_n \dots a_1 a_0} + 8(a_n + \cdots + a_1 + a_0) \equiv a_n + \cdots + a_1 + a_0 + 8(a_n + \cdots + a_1 + a_0) \pmod 9$$

$$\overline{a_n \dots a_1 a_0} + 8(a_n + \cdots + a_1 + a_0) \equiv 9a_n + \cdots + 9a_1 + 9a_0 \pmod 9$$

$$\overline{a_n \dots a_1 a_0} + 8(a_n + \cdots + a_1 + a_0) \equiv 9(a_n + \cdots + a_1 + a_0) \pmod 9$$

$$\text{Mas } 9(a_n + \cdots + a_1 + a_0) \equiv 0 \pmod 9\text{, daí}$$

$$\overline{a_n \dots a_1 a_0} + 8(a_n + \cdots + a_1 + a_0) \equiv 0 \pmod 9$$

Logo, a soma de um número com a soma de seus dígitos multiplicada por 8 resulta em um número com raiz digital 9. □

Exemplo: Número escolhido: 26374

Soma dos dígitos multiplicada por 8: $8(2 + 6 + 3 + 7 + 4) = 176$

Soma: $26374 + 176 = 26550$

$26550 \equiv 2 + 6 + 5 + 5 = 18 \pmod 9 \equiv 0 \pmod 9$

4. Anote um número qualquer, reorganize seus dígitos aleatoriamente gerando dois outros números. Some os três números e eleve o resultado ao quadrado. O número obtido será múltiplo de 9.

Demonstração. Seja $a = \overline{a_n \dots a_1 a_0}$ o número escolhido. Sabemos que, independente da ordem de seus dígitos, sua raiz digital será sempre a mesma. Digamos que, sem perda de generalidade, os números $\overline{a_1 \dots a_n a_0}$ e $\overline{a_0 \dots a_1 a_n}$ sejam gerados pela permutação dos dígitos de a. Assim,

$$\overline{a_n \dots a_1 a_0} + \overline{a_1 \dots a_n a_0} + \overline{a_0 \dots a_1 a_n} \equiv$$
$$(a_n + \cdots + a_1 + a_0) + (a_1 + \cdots + a_n + a_0) + (a_0 + \cdots + a_1 + a_n) \pmod 9$$

$$\overline{a_n \dots a_1 a_0} + \overline{a_1 \dots a_n a_0} + \overline{a_0 \dots a_1 a_n} \equiv 3(a_n + \cdots + a_1 + a_0) \pmod 9$$

Elevando ao quadrado temos

$$(\overline{a_n \dots a_1 a_0} + \overline{a_1 \dots a_n a_0} + \overline{a_0 \dots a_1 a_n})^2 \equiv [3(a_n + \cdots + a_1 + a_0)]^2 =$$
$$9(a_n + \cdots + a_1 + a_0)^2 \pmod 9$$

Mas $9(a_n + \cdots + a_1 + a_0)^2 \equiv 9 \equiv 0 \pmod 9$. Daí,

$(\overline{a_n \ldots a_1 a_0} + \overline{a_1 \ldots a_n a_0} + \overline{a_0 \ldots a_1 a_n})^2 \equiv 0 \pmod 9$.

Portanto, a soma de um número com outros dois números gerados do reordenamento dos dígitos do número original, elevada ao quadrado, resulta em um número múltiplo de 9.

□

Exemplo: Número escolhido: 1782

Números embaralhados: 2187 e 8271

Soma elevada ao quadrado: $(1782 + 2187 + 8271)^2 = 149817600$

$149817600 \equiv 1 + 4 + 8 + 1 + 7 + 6 = 27 \equiv 0 \pmod 9$

2.3.2 Adivinhando a idade

Um outro truque numérico muito interessante e que utiliza-se da propriedade da raiz digital é o truque de "adivinhar"a idade de uma pessoa. Começa-se pedindo que a pessoa realize qualquer uma das operações que resulte em um número com raiz digital 9, em seguida a pessoa deve somar a este número a sua idade e anunciar o total, podendo ser em qualquer ordem, visto que o "mágico"precisa saber somente a raiz digital do número fornecido pela pessoa. Com a raiz digital, o "mágico"deve seguir somando 9 até alcançar o número que esteja mais próximo da idade da pessoa, pois não é difícil estimar a idade de uma pessoa em lapsos de 9 anos.

Vejamos um exemplo:

Pede-se a uma criança que pense em um número qualquer e o multiplique por 9. Ao resultado, a criança deve somar sua idade e falar os números do resultado em qualquer ordem. Suponhamos que a criança diga os números 277858. A raiz digital deste número é 1 e a ele devemos somar 9 até alcançar uma idade que a pessoa aparente ter: 10, 19, 28, 37,... Como se trata de uma criança, sua idade é de 10 anos.

2.3.3 Prova dos noves fora

A prova dos noves fora é um método utilizado antigamente para revisar cálculos de adição, subtração, multiplicação e divisão e utiliza-se basicamente da propriedade da

congruência módulo 9, a raiz digital. Apesar de não ser mais utilizada atualmente, é interessante apresentá-la aos alunos como uma curiosidade, que os fará refletir sobre as propriedades da teoria dos números, em especial a gama de possibilidades de uso da congruência módulo 9.

Tirar os "noves fora"significa subtrair de um número natural n o maior múltiplo de 9 menor do que n, o que é equivalente a encontrar o resto da divisão de n por 9. Conforme vimos anteriormente, este procedimento equivale a obtenção da raiz digital do número, bastando somar seus dígitos recursivamente até que reste apenas um algarismo.

Vejamos como proceder para verificar os resultados dos cálculos nas quatro operações aritméticas.

Adição, subtração ou multiplicação: Some os dígitos que compõe os números de cada uma das parcelas da adição (subtração ou multiplicação) e, sempre que a soma exceder 9, subtrai-se 9 da mesma antes de continuar somando os demais algarismos. Esse procedimento é equivalente a somar os algarismos dos números resultantes sempre que se chegar a um número maior que 9, até encontrar um número de apenas um algarismo, se este algarismo for o nove, tiramos o "nove fora"e ficamos com 0, que é o resto da divisão de 9 por 9. O mesmo procedimento deve ser realizado com o resultado da soma (subtração ou multiplicação). Se a raiz digital desse resultado diferir da soma (subtração ou multiplicação) das raízes digitais das parcelas, então há erro na operação.

Exemplo 2.17. Verifiquemos a soma 7213+684=7897:

$$\begin{aligned} 7213 &\implies 7+2+1+3=13 \implies 1+3=4 \text{ ou } 13-9=4 \\ +\ 684 &\implies 6+8+4=18 \implies 1+8=9\equiv 0 \pmod 9 \text{ ou } 18-9-9=0 \\ \hline 7897 &\implies 7+8+9+7=31 \implies 3+1=4 \text{ ou } 31-9-9-9=4 \end{aligned}$$

Observemos que a soma das raízes digitais da 1ª e da 2ª parcela é igual a $4+0=4$ que corresponde a raiz digital do número 7897, dado resultado da soma $7213+684$. Com isso, é provável que o resultado esteja correto.

Divisão: Calculemos a raiz digital do dividendo a, do divisor b, do quociente q e do resto r da divisão. Como devemos ter $a=bq+r$, então $a\equiv bq+r \pmod 9$, logo, o resto do divisor b multiplicado pelo resto do quociente q e somado ao resto de r deve ser igual ao resto do dividendo.

Exemplo 2.18. Suponhamos que encontramos na divisão de $a=25461$ por $b=273$ o quociente $q=93$ e o resto $r=72$. Temos que $a\equiv 2+5+4+6+1\equiv 0 \pmod 9$, $b\equiv 2+7+3\equiv 3 \pmod 9$, $q\equiv 9+3\equiv 3 \pmod 9$ e $r\equiv 7+2\equiv 0 \pmod 9$

$$bq + r \equiv 3 \cdot 3 + 0 \equiv 0 \equiv a \pmod 9$$

Como $bq + r \equiv a \pmod 9$, provavelmente a divisão esteja correta.

Mas, seria a prova dos nove totalmente eficaz? Vejamos:

Se a raiz digital do resultado for diferente da soma das raízes das parcelas, temos a certeza de que o resultado do cálculo está errado. Mas, se a raiz digital do resultado for igual à soma das raízes digitais das parcelas, nada podemos afirmar, visto que números diferentes podem ter o mesmo resto na divisão por 9. Por exemplo, se a resposta dada à soma $7213 + 684$ fosse 8113, teríamos que a raiz digital de 8113 é $8 + 1 + 1 + 3 = 13$ e $1 + 3 = 4$ que equivale à soma das raízes digitais das parcelas da soma, todavia o resultado está incorreto.

Em princípio, prova dos nove baseia-se no fato de que

$$a = b \pm c \Longrightarrow a \equiv b \pm c \pmod 9$$
$$a = bc \Longrightarrow a \equiv bc \pmod 9$$

Cujas implicações não valem no sentido contrário. Portanto, a prova dos "noves fora"é capaz de detectar se há um erro em uma operação aritmética, mas não pode garantir se o resultado é realmente correto.

Vejamos o problema abaixo que apresenta mais uma "matemágica"utilizando a congruência módulo 9.

Problema 2.19. (Extraído de [6]) Escolha um número abc de três algarismos no sistema decimal, de modo que os algarismo das centenas a e o das unidades c difiram de, pelo menos, duas unidades. Considere os números $\overline{abc}$ e $\overline{cba}$ e subtraia o menor do maior, obtendo o número $\overline{xyz}$. A soma de $\overline{xyz}$ e $\overline{zyx}$ vale 1089. Justifique este fato.

Observação 2.20. Vejamos que este problema se aplica também ao caso em que a diferença entre a e c é igual a 1. A única exigência é que tenhamos $a \neq c$.

Solução. Sabemos que, pela propriedade da congruência módulo 9, todo número é congruente à soma de seus algarismos módulo 9, logo,

$$\overline{abc} \equiv a + b + c \pmod 9 \text{ e}$$
$$\overline{cba} \equiv c + b + a \pmod 9$$

Suponhamos, sem perda de generalidade que $a > c$, daí

$$\overline{abc} - \overline{cba} \equiv a + b + c - (c + b + a) \pmod 9 \text{ e}$$
$$\overline{abc} - \overline{cba} \equiv 0 \pmod 9$$

Seja $\overline{xyz} = \overline{abc} - \overline{cba}$, logo $\overline{xyz}$ é múltiplo de 9.

Observemos que, na subtração $abc - cba$, o algarismo b não muda de posição, permanecendo na casa das dezenas e que $a > c$, logo podemos concluir que $y = 9$, em razão do "tira 1"realizado no algoritmo da subtração. Veja abaixo:

$$\begin{array}{cccc} & & {\scriptstyle b-1+10} & \\ & {\scriptstyle a-1} & {\scriptstyle b-1} & {\scriptstyle c+10} \\ & a & b & c \\ - & c & b & a \\ \hline & a-1-c & 9 & c+10-a \end{array}$$

1º passo - Como $c < a$, "pedimos 1 emprestado"ao b, que se torna $b - 1$ enquanto c se torna $c + 10$;

2º passo - Como $b-1 < b$, "pedimos 1 emprestado"ao a, que se torna $a-1$ enquanto b se torna $b - 1 + 10 = 9$;

3º passo - Logo, $b + 9 - b = 9$.

Como concluímos que $\overline{xyz}$ é múltiplo de 9, temos que a soma $x + y + z$ deve ser múltipla de 9; como $y = 9$, devemos ter $x + z = 9$. Não é possível termos $x + z = 18$, pois para isso deveríamos ter $\overline{xyz} = 999$, o que não é possível pelo fato de que $\overline{xyz}$ é o resultado da subtração entre um número de três algarismos e seu "inverso", e o maior número de três algarismos que podemos ter é o próprio 999.

Sabendo que $y = 9$ e que $x + z = 9$, podemos escrever o resultado S da soma da diferença pelo seu "inverso":

$$S = \overline{xyz} + \overline{zyx}$$
$$S = 100x + 10y + z + 100z + 10y + x$$
$$S = 100(x + z) + 20y + (x + z) = 100 \cdot 9 + 20 \cdot 9 + 9 = 900 + 180 + 9 = 1089$$

Como queríamos demonstrar.

Também podemos encontrar todos os valores possíveis de xyz. Vejamos:

$$\overline{abc} - \overline{cba} = 100a + 10b + c - 100c - 10b - a$$
$$\overline{abc} - \overline{cba} = 99a - 99c$$
$$\overline{abc} - \overline{cba} = 99(a - c)$$
$$\overline{xyz} = 99(a - c)$$

Logo, $\overline{xyz}$ é sempre um múltiplo de 99 multiplicado pela diferença entre a e c.

- Se $a - c = 1$, $\overline{xyz} = 099$ e $\overline{zyx} = 990$, assim $\overline{xyz} + \overline{zyx} = 99 + 990 = 1089$
- Se $a - c = 2$, $\overline{xyz} = 198$ e $\overline{zyx} = 891$, assim $\overline{xyz} + \overline{zyx} = 198 + 891 = 1089$
- Se $a - c = 3$, $\overline{xyz} = 297$ e $\overline{zyx} = 792$, assim $\overline{xyz} + \overline{zyx} = 297 + 792 = 1089$
- Se $a - c = 4$, $\overline{xyz} = 396$ e $\overline{zyx} = 693$, assim $\overline{xyz} + \overline{zyx} = 396 + 693 = 1089$
- Se $a - c = 5$, $\overline{xyz} = 495$ e $\overline{zyx} = 594$, assim $\overline{xyz} + \overline{zyx} = 495 + 594 = 1089$
- Se $a - c = 6$, $\overline{xyz} = 594$ e $\overline{zyx} = 495$, assim $\overline{xyz} + \overline{zyx} = 594 + 495 = 1089$
- Se $a - c = 7$, $\overline{xyz} = 693$ e $\overline{zyx} = 396$, assim $\overline{xyz} + \overline{zyx} = 693 + 396 = 1089$
- Se $a - c = 8$, $\overline{xyz} = 792$ e $\overline{zyx} = 297$, assim $\overline{xyz} + \overline{zyx} = 792 + 297 = 1089$
- Se $a - c = 9$, $\overline{xyz} = 891$ e $\overline{zyx} = 198$, assim $\overline{xyz} + \overline{zyx} = 891 + 198 = 1089$

Capítulo 3

Considerações finais

A Aritmética é uma área muito rica da Matemática, caracterizada pela simplicidade dos métodos e pela variedade de problemas; mas que infelizmente é uma área pouco explorada nas séries finais do Ensino Fundamental. Com este trabalho, apresentamos uma proposta de inserção deste tão importante conteúdo na grade curricular do Ensino Fundamental, apresentando os aspectos mais importantes da teoria, ilustrando com exemplos e desafiando os alunos com problemas de diversos níveis de dificuldade.

Na Aritmética, o pilar central são os problemas e neste trabalho buscou-se, com sucesso, a inserção de problemas como parte do processo de ensino. Cabe agora aos professores, exortar os alunos a resolvê-los, visto que são uma parte importante do aprendizado de qualquer novo assunto, e com isso, estimular nos estudantes o prazer em solucionar desafios utilizando-se dos conhecimentos aprendidos, de métodos diversos e de uma boa dose de imaginação.

Os problemas relacionados à Aritmética são amplamente cobrados em olimpíadas, por ser um tema fundamental, de bases teóricas que podem ser facilmente assimiladas por estudantes do Ensino Fundamental e mesmo Ensino Médio. Entretanto, os alunos não têm a oportunidade de visualizar tal conteúdo, que não consta de forma completa em suas grades curriculares, havendo a necessidade da realização de estudos complementares, como nos grupos de estudo PIC-OBMEP e POTI-IMPA, pelos alunos interessados a tornarem-se aptos a participar de olimpíadas de matemática que explorem esse assunto.

Durante o desenvolvimento deste trabalho, apesar da ênfase nos exemplos e problemas, não foram deixados de lado os teoremas, corolários, definições, proposições e suas

demonstrações, apresentados de forma clara e na medida ideal para que os alunos comecem a habituar-se com os procedimentos de abstração matemática. Tão importante como apresentar demonstrações de propriedades é instigar os alunos a realizá-las também, conforme foi realizado neste trabalho em diversos momentos em que foi proposta a demonstração ou generalização de propriedades na forma de problemas.

Acreditamos que com este trabalho possamos inspirar professores que tenham interesse em inserir os conceitos aqui apresentados em sua prática pedagógica com o objetivo de impulsionar a curiosidade e a criatividade dos seus alunos; e também inspirar futuros pesquisadores que possam complementar, aperfeiçoar ou desenvolver outros trabalhos espelhados nesta linha.

Referências Bibliográficas

[1] Cadar, Luciana; Dutenhefner, Francisco *Encontros de Aritmética*, Rio de Janeiro: IMPA, (2015).

[2] Domingues, Hygino H., *Fundamentos de Aritmética*, São Paulo: Atual, (1991).

[3] Fomin, Dmitri; Genkin, Sergey; Itenberg, Ilia *Círculos Matemáticos - A experiência russa*, Tradução de Valéria de Magalhães Iório - Rio de Janeiro: IMPA, (2012).

[4] Gardner, Martin, *Matemática, Magia y Misterio*, RBA, (2011).

[5] Greenes, Carole E.; Spugin, Rika; Dombrowski, Justine M. *Problem-Mathics: Mathematical challenge problems with solutions strategies*, Palo Alto, Califórnia: Creative Publications, (1977).

[6] Hefez, Abramo, *Aritmética*, Coleção PROFMAT. Rio de Janeiro: SBM, (2014).

[7] Lima, Elon Lages; Carvalho, Paulo Cezar P.; Wagner, Eduardo; Morgado, Augusto César, *A Matemática do Ensino Médio*, Volume 4, Enunciados e Soluções dos Exercícios. Rio de Janeiro: SBM, (2007).

[8] Martinez, Fábio E. B.; Moreira, Carlos G. T. de A.; Saldanha, Nicolau C.; Tengan, Eduardo, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, Rio de Janeiro: IMPA, (2010).

[9] Oliveira, Marcelo Rufino de; Pinheiro, Márcio Rordrigo da Rocha, *Coleção Elementos da Matemática*, Volume 1. 3ed. Fortaleza: Editora VestSeller, (2010).

[10] Papa Neto, Angelo, *Critérios de Divisibilidade*, Material Teórico - Módulo de Divisibilidade, Sexto Ano. Portal da Matemática - OBMEP. Disponível em: `http://matematica.obmep.org.br/uploads/material_teorico/5obdvodxmnk8c.pdf`. Acessado em: julho de 2016.

[11] Posamentier, Alfred S., *Math wonders to inspire teachers and students*, ASCD - Association for Supervision and Curriculum Development. Alexandria, Virginia USA, (2003).

[12] Revista Eureka!, *Eureka! Nº1*, Sociedade Brasileira de Matemática - SBM, (1998).

[13] Santos, José Plínio de O., *Introdução à Teoria dos Números*, Rio de janeiro: SBM. (1998).

[14] Tao, Terence, *Como resolver problemas matemáticos - uma perspectiva pessoal*, Tradução de Paulo Ventura - Rio de Janeiro: SBM, (2013).