Universidade Federal de Goiás

Coordenação de Matemática

Programa de Mestrado Profissional em Matemática em Rede Nacional

Divisibilidade e Congruências: Aplicações no Ensino Fundamental II

Tânia Regina Rodrigues Franco

Jataí-GO

2016

Divisibilade e Congruências: Aplicações no Ensino Fundamentantal II

Tânia Regina Rodrigues Franco

Trabalho de Conclusão de Curso apresentado à coordenação de Matemática 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: Prof. Dr. Fernando Ricardo Moreira

Jataí-GO

2016

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

Franco, Tânia Regina Rodrigues
Divisibilidade e Congruências: Aplicações no Ensino Fundamental II [manuscrito] / Tânia Regina Rodrigues Franco. - 2016.
80 f.

Orientador: Prof. Dr. Fernando Ricardo Moreira; co-orientadora Dra. Adriana Araujo Cintra.
Dissertação (Mestrado) - Universidade Federal de Goiás, Regional Jataí , Jataí, Programa de Pós-Graduação em Matemática (PROFMAT - Profissional), Jataí, 2016.
Bibliografia.
Inclui siglas, abreviaturas, símbolos, tabelas, algoritmos.

1. Divisibilidade. 2. Congruência. 3. Aplicações. 4. Metodologias. I. Moreira, Fernando Ricardo, orient. II. Cintra, Adriana Araujo, co-orient. III. Título.

Tânia Regina Rodrigues Franco

Divisibilidade e Congruências: Aplicações no Ensino Fundamental II

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em rede Nacional – PROFMAT/UFG, Polo Jataí, 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 30 de março de 2016, pela banca examinadora constituída pelos professores abaixo:

Prof. Dr. Fernando Ricardo Moreira
Presidente da Banca
Coordenação de matemática – UFG/Jataí

Prof. Dr. Esdras Teixeira Costa
Membro – Coordenação de Matemática – UFG/Jataí

Prof. Dr. Paulo Freitas Gomes
Membro – Coordenação de Física – UFG/Jataí

Dedico este trabalho a todos que de forma direta ou indireta colaboraram para que eu pudesse cursar o PROFMAT, em especial a meus filhos Milena Gabriele e Vitor Gabriel que muitas vezes não tiveram minha presença em momentos importantes de suas vidas, visto a escassez de tempo pra assimilar profissional e pessoal, e a meu esposo Nelson que sempre esteve ao meu lado acreditando em minha capacidade e incentivando-me a crescer profissionalmente.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado força e ânimo pra jamais desistir.

Ao meu orientador Prof. Dr. Fernando Ricardo Moreira pelo apoio, incentivo, dedicação e principalmente, pela paciência e amizade, não só durante a elaboração deste trabalho, mas também durante aulas que ministrou a mim e a meus colegas.

Aos meus professores pela orientação durante todo o curso, e em especial, ao Prof. Dr. Esdras Teixeira Costa, pela orientação de uso do LATEX.

A todos os meus colegas, inclusive aqueles que no meio do percurso não puderam concluir este mestrado, mas que sempre ajudaram quando precisei.

Aos meus filhos Milena e Vitor por terem a paciência de me ver dedicando tanto aos estudos e às vezes os deixando sem mim.Ao meu esposo, que em nenhum momento duvidou de que eu iria conseguir e me acompanhou nas incansáveis viagens pra assistir as aulas, sem cobranças ou ressentimentos

Aos meus pais, Elma e Marciano, e principalmente meus queridos avós Eva e Matias(*in memorian*) que me criaram e me ensinaram que os estudos são a maior conquista que se pode ter e que é a unica coisa que ninguém pode nos tirar.

Aos meus irmãos, Dyeimys, Aderson, Juliana, Priscila e Marciano Filho, que sempre elogiaram pela garra e força de vontade.

A minha sogra Maria Aparecida e minha madrasta Soraia, que incansávelmente ajudaram a cuidar dos meus filhos que eu pudesse me dedicar aos estudos.

Ao PROFMAT, pela oportunidade e a CAPES, pelo apoio financeiro.

Enfim todos aqueles que sempre me incentivaram, e também aos que ao contrário o fizeram, levando-me a ter mais garra do que talvez teria e mostranto a mim mesmo que não temos limites.

Resumo

Esta dissertação, inicia-se com uma fundamentação teórica acerca do sistema posicional, divisibilidade, divisão euclidiana, máximo divisor comum, números primos e congruência modular. Através dos conceitos abordados, apresentaremos algumas aplicações, para alunos do ensino fundamental. O principal objetivo é apresentar os principais pontos da teoria e trazer noções da aplicabilidade da aritmética em situações cotidianas. Trabalharemos a resolução de Equações Diofantinas Lineares; determinaremos alguns critérios de divisibilidade, através da relação de congruência modular e aritmética dos restos; ainda com congruência modular proporemos atividades com códigos e outras numerações existentes em nosso país, finalizando com a resolução de problemas sobre calendários. Essas aplicações servirão de ferramentas e metodologias para que de forma contextualizada, o professor, motive seu aluno a entender um pouco mais sobre o conceito de Aritmética Modular, de maneira fácil, rápida e simples.
Palavras-chave: Divisibilidade. Congruência. Aplicações. Metodologias.

Abstract

This essay begins with a theoretical foundation about the positional system, divisibility, Euclidean division, maximum common divisor, prime numbers and modular congruence. Through the concepts discussed, we show some applications, for elementary school students. The main main points of the theory and bring notions of applicability of arithmetic in daily situations. We will work solving Diophantine linear equations; we will determine some criteria of divisibility; by the relationship of modular congruence and arithmetic of the rest; even with modular congruence we will propose activities with codes and other existing numbers in our country, ending solving problem on calendars. These applications will serve of tools and methodologies of contextualized form, the teachers, will motivate their students to understand a little more about the concept of Modular Arithmetic, easy, fast and simple way.
Key words: Divisibility. Congruence. Applicability. Methodologies.

Sumário

Capítulo 1

Introdução

Desde o seu surgimento até hoje o homem se desenvolveu, ou melhor, se modificou. A partir do momento em que passou a viver em grupos, sentiu a necessidade da comunicação. Então no decorrer de um longo processo surgiu a linguagem. A mesma coisa se repetiu com os números. Entretanto até chegar no modo que são atualmente, os números e os símbolos que os representam sofreram grandes transformações ao longo do tempo (MIYASCHITA. 2002).

Neste trabalho iremos abordar conceitos que envolvem a Teoria dos Números, em específico a Aritmética. Este é o ramo da matemática pura que se preocupa com as propriedades dos números inteiros. A Aritmética envolve muitos problemas facilmente compreendidos mesmo por não-matemáticos.

O termo "Aritmética" é um termo antigo, que não é mais tão popular como já foi. A Teoria dos Números foi também chamada de aritmética superior e faz parte da cultura dos povos desde os tempos antigos, tendo sido desenvolvida para atender às necessidades de comunicação e quantificação. Na história das civilizações, os povos a criaram e a recriaram sob roupagens diferentes, utilizando essencialmente os mesmos processos matemáticos modificados ao longo do tempo (LORENSATTI. 2012).

A Aritmética começou a ser desenvolvida a partir do surgimento da contagem, antes da definição formal dos números e operações aritméticas sobre eles por um sistema de axiomas, estando intimamente relacionada com álgebra e teoria dos números.

Tornou-se uma necessidade prática, a longo prazo, para medidas simples e cálculos. A primeira informação confiável sobre o conhecimento aritmética é encontrada nos monumentos históricos do Antigo Egito e na Babilônia, relativa ao 3°- 2° milênio a.C. (BOYER. 2003).

Segundo Boyer (2003) a disciplina em questão veio a ocupar-se com uma classe mais vasta de problemas que surgiram naturalmente a partir estudo dos números inteiros. Esta teoria pode ser subdividida em vários campos, de acordo com os métodos que são usados e das questões que são investigadas, sendo estes campos à:

- Teoria Elementar: que utiliza somente os métodos elementares da aritmética para a verificação e comprovação das propriedades essenciais do conjunto dos números inteiros e em particular as propriedades dos números primos;
- Teoria analítica dos números: que utiliza a análise real e análise complexa, especialmente para estudar as propriedades dos números primos;
- Teoria algébrica: que utiliza álgebra abstrata e estuda os números algébricos[1];
- Teoria geométrica: que utiliza métodos geométricos, algébricos e analíticos.

Escolhemos para nosso estudo a Teoria Elementar dos Números, em especial, a Aritmética modular , tendo em vista possuir um conjunto de conhecimentos indispensáveis a todo cidadão.

A congruência modulo m e aritmética modular têm muitas aplicações. Dentre elas, a justificativa para os critérios de divisibilidade, exemplificação de conceitos que envolvem as propriedades das operações, construção de códigos e no estudo de modelagem para fenômenos periódicos que envolvem diferentes campos do conhecimento. (SILVA, FRIEDMANN. 2011).

Percebemos ainda que, estuda-se de forma direta em álgebra muitos conceitos envolvendo congruência, porém não é muito comum o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas e na resolução de diversos problemas.

Exemplos do uso da aritmética modular no dia-a-dia das pessoas é o relógio de ponteiro, no qual o dia é divido em dois períodos de 12 horas cada; nos calendários que são divididos em meses semanas e dias. Além disso, diferentes códigos numéricos de identificação, como *International Standard Book Number*(ISBN), Código de Barras,

[1]Um número algébrico é qualquer número real ou complexo que é solução de alguma equação polinomial com coeficientes inteiros. Em um sentido mais amplo, diz-se que um número é algébrico sobre um corpo quando ele é raiz de um polinômio com coeficientes neste corpo.

Cadastro de Pessoas Físicas (CPF) e vários fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos alguns em nosso trabalho. Este é um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental II, que abrange do $6^{\underline{o}}$ ao $9^{\underline{o}}$ anos, gerando excelentes oportunidades de contextualização no processo de ensino/aprendizagem de matemática.

Inicialmente mostraremos elementos teóricos referentes a forma de um número na sua base decimal, divisibilidade a Aritmética Modular. Na sequência, através dos conceitos expostos, proporemos algumas aplicações importantes relacionadas ao tema. Tendo em vista a relevância desta no conjunto dos conhecimentos indispensáveis a todo cidadão, é justificável o interesse de se compreender como essa "disciplina" se instituiu.

O objetivo geral deste trabalho é apresentar algumas atividades e exemplos ao professor de matemática do ensino básico, tal que possa servir de fonte de pesquisa para aulas dinâmicas e atrativas. Além disso, servirá como norteador de novos conceitos para aqueles que pretendem fazer estudos nesse âmbito e ainda promover aulas prazerosas e vinculadas ao cotidiano. Já os objetivos específicos são: fazer com que o aluno entenda de maneira correta o conceito de divisibilidade; definir congruência modular; relacionar divisibilidade/congruência, incorporando ao currículo escolar um conteúdo novo e capaz de sanar frequentes dúvidas a respeito de conjuntos de regras apresentadas por livros didáticos

O ponto de referência do processo de ensino e aprendizagem da Matemática deve ser a abordagem de assuntos de interesse do aluno, que estimulem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos (GROENWALD, FRANKE, OLGIN. 2009). A Matemática torna-se interessante e motivadora para a aprendizagem quando desenvolvida de forma integrada e relacionada a outros conhecimentos, trazendo o desafio de desenvolver competências e habilidades formadoras do pensamento matemático. Desse modo, constituímos o corpo do trabalho em seis capítulos, incluindo esta introdução e nos demais abrangeremos um referencial teórico e atividades que nos proporcionarão apresentar uma metodologia diferenciada no ensino de vários conceitos para alunos do ensino fundamental II.

No capítulo 2, faremos um breve apanhado sobre sistema decimal posicional que ultilizamos e a importância da sua representação estendida no desenvolvimento de outros conceitos.

No capítulo 3, trateremos do tema, divisibilidade. Apresentaremos conceitos como: Divisão Eucidiana, Máximo Divisor Comúm, Números Primos e uma grande aplicação destes conceitos que são as Equações Diofantinas Lineares(EDL). As EDL nos auxiliam na resolução de problemas aparentemente difíceis, no entanto, se mode-

lados de forma correta podem se tornar bem mais compreensíveis para o aluno. Para tal nos baseamos nas definições e teoremas apresentados por Hefez (2013). Levamos também em consideração o fato de que, conceitos como o de divisor de um número, ampliam o entendimento sobre campo multiplicativo, correlacionando as duas operações (BRASIL. 1998). Contudo ainda é importante que tal trabalho não se resuma à apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar resultados de forma mecânica sem compreender as situações-problema que esses conceitos permitem resolver. Além disso, ao se trabalhar divisibilidade, é de suma importância explorar conceitos ligados aos números primos, pois uma lista de números primos é como se fosse a "tabela periódica" do matemático, sendo que eles são geradores de todos os outros não primos (SAUTOY.2007).

Inicaremos o capítulo 4, definindo congruência modular, suas propriedades básicas e operatótias e as generalizações do Pequeno Teorema de Fermat em termos de Congruência. Na sequência apresentaremos alguns exemplos de atividades com estas propriedades através da aritmética dos restos. Essas aplicações, além de trabalhar propriedades da congruência modular, envolvem também conceitos de potenciação, fazendo a conexão de ambos. Através desta conexão, o aluno poderá determinar o resto de divisões com potências de expoentes muito grandes por um número qualquer. Estes conceitos são bastante explorados em outras dissertações direcionadas ao PROFMAT, inclusive por Júnior (2013), Esquinca (2015) e Moura (2015) e de forma bem sutil entram em consonância com este trabalho, visto que as demais são direcionadas ao ensino médio e no nosso caso, restringimos ao fundamental II.

No capítulo 5, nos direcionamos a outras aplicações de divisibilidade e congruências no ensino fundamental II, além das já apresentadas nos capítulos anteriores, visto que a Aritmética mesmo sendo um conceito tido como importante pelos currículos nacionais de ensino, não se valoriza o conteúdo de congruências . Pretendemos apresentar atividades desafiadoras e simples através da correlação entre conceitos que são estudados, de forma que possamos incluir tal conceito na grade curricular. Proporemos algumas atividades onde aluno possa ser gerador de seu próprio conhecimento. O significado da atividade matemática para o aluno também resulta das conexões que ele estabelece entre os diferentes temas matemáticos e também entre estes e as demais áreas do conhecimento e as situações do cotidiano. O estabelecimento de relações é fundamental para que o aluno compreenda efetivamente os conteúdos matemáticos, pois, abordados de forma isolada, eles não se tornam uma ferramenta eficaz para resolver problemas e para a aprendizagem/construção de novos conceitos(BRASIL. 1998). Discutiremos e apresentaremos sugestões de atividades que envolvem:

- Critérios clássicos de divisibilidade por 2, 3 e 11, através da construção do processo. De acordo com os Parametros Curriculares Nacionais (1998) é relevante para o aprendizado que, além do trabalho com os significados das operações, desenvolva-se um processo sistematizado de cálculo que inclua a construção e análise de vários procedimentos, tendo em vista que eles relacionam-se e complementam-se;
- Digitos de verifação, os quais são números bastante utilizados no nosso país para validação de alguns códigos como: Código de Barras, ISBN, CPF, entre outras sequências que não serão abordadadas neste trabalho, porém não deixam de ser menos importantes;
- Calendários: que segundo Oliveira (2015) servem como estímulo ao desenvolvimento das operações básicas através da sua associação com algoritmos.

No último capítulo faremos uma abordagem geral dos temas propostos, bem como sua sua aplicabilidade e relevância no ensino fundamental. Esta relevânica se encontra explícita nas experiências de quantificação de objetos e fenômenos fazem parte da vida prática das pessoas, e o estudo da Aritmética é uma necessidade para prover a organização adequada da sociedade e oferecer oportunidades para o indivíduo desenvolver processos matemáticos inerentes à sua estrutura lógica mental. Portanto, cabe à escola, também, oportunizar o desenvolvimento das competências aritméticas, ou seja, contar, calcular e resolver problemas que exijam esses conhecimentos (LORENSATTI. 2012).

Capítulo 2

Sistema de Numeração

O sistema de numeração que utilizamos é chamado de decimal posicional. São, ao todo, dez os algarismos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Estes são geradores de qualquer número neste sistema, uma vez que por serem infinitos os números podem ser compostos por quantos dígitos se desejar. No sistema decimal posicional a representação por algarismos é bastante prática, pois cada dígito do algarismo representa uma quantidade. Os números são separados por grupos de três algarismos, da direita para a esquerda. Cada um desses grupos é chamado classe. Dessa forma temos a classe das unidades, a classe dos milhares, a classe dos milhões, a classe dos bilhões etc. Cada classe, por sua vez é dividida em três ordens, também da direita para a esquerda: unidades, dezenas e centenas (MIYASCHITA. 2002 ; HEFEZ. 2013). Veja como é feita esta distribuição:

Classes	Milhões			Milhares			Unidades		
Ordens	9^a	8^a	7^a	6^a	5^a	4^a	3^a	2^a	1^a
	C	D	U	C	D	U	C	D	U
	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
Ex:3 245						3	2	4	5
Ex:3 634						3	6	3	4
Ex:1 863 025			1	8	6	3	0	2	5

Figura 1: Classes e Ordens
Fonte:https://proftamira.files.wordpress.com/2012/03/sistnumerdecimal1.jpg

Segundo Hefez (2013) para generalizar o sistema posicional podemos dizer que sua base b, tem b dígitos diferentes. Cada um destes digítos, além do seu valor real, possui um peso definido pela posição que ele ocupa. Como no nosso sitema utilizamos base 10, a distribuição do valor de cada digíto distribui-se, através de potências de base 10 da seguinte maneira:

- O algarismo da extrema direita tem peso um(10^0);
- Seguindo da direita para a esquerda o seguinte tem peso $2(10^1)$ e assim sucessivamente, até que se distribua pesos para todos os digítos (10^{n-1}).

Quando escrevemos o número 374, sabemos que o algarismo 3 representa 300 unidades, 30 dezenas ou $3 \cdot 10^2$ unidades, o algarismo 7 representa 70 unidades, 7 dezenas ou $7 \cdot 10^1$ unidades e o 4 representa 4 unidades ou $4 \cdot 10^0$ unidades. Assim, podemos escrever :

$$374 = 3 \cdot 10^2 + 7 \cdot 10^1 + 4 \cdot 10^0.$$

Observação. A representação de um número dado em sua forma posicional é dita representação extendida.

Exemplo 1. Escreva o número 235698 na forma extendida.

Solução:

$$235698 = 2 \cdot 10^5 + 3 \cdot 10^4 + 5 \cdot 10^3 + 6 \cdot 10^2 + 9 \cdot 10 + 8.$$

Genericamente, podemos dizer que um número da forma $a_n a_{n-1} a_{n-2} ... a_2 a_1 a_0$, no sistema de numeração decimal, representa o número:

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

O próximo resultado generaliza a expansão de um número a em uma base $b > 1$ dada.

Teorema 1. Sejam dados os números a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geqslant 0$ e $0 \leqslant r_0, r_1, \cdots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que:

$$a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n.$$

Demonstração.

Demonstraremos por indução completa sobre a.

Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. A unicidade é clara.

Suponhamos o resultado válido para todo natural menor do que a, onde $a \geqslant b$.

Vamos prová-la para a.

Pela divisão Euclidiana, existem q e r, únicos, tais que:

$$a = bq + r, \ com \ 0 \leqslant r \leqslant b \tag{1}$$

Como $0 < q < a$, pela hipótese de indução, segue-se que existem números inteiros $n' \geq 0$ e $0 \leq r_1, \cdots, r_{n'+1} < b$, com $r_{n'} + 1 \neq 0$.

Univocamente determinados, tais que:

$$q = r_1 + r_2 b + \cdots + r_{n'+1} b^{n'}. \tag{2}$$

Substituindo a equação (2) em (1), temos que:

$$a = bq + r = b(r_1 + r_2 b + \cdots + r_{n+1} b^{n'}) + r,$$

donde o resultado segue-se pondo:

$$r_0 = r \text{ e } n = n' + 1.$$

□

Contudo podemos trabalhar com diferentes bases. Quando adquirimos uma dúzia de laranjas, duas dúzias de rosas, cinco dúzias de bananas ou uma grosa (doze dúzias) de parafusos estaremos trabalhando na base duodecimal (base 12) de numeração. Quando marcamos o tempo em dias, horas, minutos e segundos estamos trabalhando com a base 60 de numeração, ou na base sexagesimal. Os computadores utilizam a base 2 (sistema binário). Neste sistema contamos de 2 em 2.

Para transformarmos da base decimal para uma base qualquer devemos dividir sucessivamente o número e a seguir os quocientes obtidos pelo algarismo representativo dessa base até que a divisão não seja mais possível. A nossa base será formada pelos restos dessas divisões de cima para baixo. Dessa forma temos que o número 430 na base 2 é escrito da seguinte forma:

$$430 = 2 \cdot 215 + 0$$

$$215 = 2 \cdot 107 + 1$$

$$107 = 2 \cdot 53 + 1$$

$$53 = 2 \cdot 26 + 1$$

$$26 = 2 \cdot 13 + 0$$

$$13 = 2 \cdot 6 + 1$$

$$6 = 2 \cdot 3 + 0$$

$$3 = 2 \cdot 1 + 1$$

$$1 = 2 \cdot 0 + 1$$

Fazendo substituições sucessivas de trás para frente nos resultados anteriores teremos que:

$$430 = 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0.$$

Logo, $430 = [110101110]_{(2)}$.

Compreender a forma estendida de um número, seja ele em qualquer base nos auxilia muito na resolução de problemas e generalização de alguns conceitos que muitas vezes apresentamos aos alunos sem nos dar conta de ensinar o processo que há por tráz disso. Fecharemos o capítulo dando um exemplo de uma questão de avaliação do PROFMAT, a qual se o conceito de base e forma estendida de um número ficarem bem claros para o aluno é um exercício excelente e que pode ser trabalhado no final do ensino fundamental, sem nenhum problema.

Exemplo 2. (Questão 2 - Avaliação 1 - Profmat 2014)Perguntado sobre quantos alunos tinha naquele ano, o professor escreveu no quadro:

"733 alunos, dos quais 276 são meninos e 435 são meninas". Inicialmente a resposta pareceu estranha, mas logo notamos que o professor não empregou o sistema decimal. Qual foi o sistema utilizado pelo professor?

Solução:

No sistema de base b, temos que $733 = 276 + 435$. Assim:

$$7 \cdot b^2 + 3 \cdot b + 3 = (2 \cdot b^2 + 7 \cdot b + 6) + (4 \cdot b^2 + 3 \cdot b + 5),$$

donde:

$$b^2 - 7b - 8 = 0.$$

Agora, determinando as raízes da equação, obtemos $b = -1$ ou $b = 8$.

Portanto, a base utilizada foi $b = 8$.

Capítulo 3

Conceitos Fundamentais

Neste capítulo iremos explorar conceitos como divisibilidade e suas propriedades, Divisão Euclidiana, Números primos, Pequeno Teorema de Fermat e para finalizar trataremos das Equações Diofantinas Lineares que por sua vez é uma aplicação bastante importante e de fácil compreensão para o público alvo.

3.1 Divisibilidade

Nesta secão abordaremos um conceito bastante importante, a **divisibilidade.** Conceito este ligado a vários outros e desenvolvido por Euclides em sua obra "Os Elementos" (HEFEZ, 2013). Para compreender o que é divisibilidade entre dois números considere o conjunto dos inteiros, $\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$ tal que a relação entre dois deles é dada por:

Definição 1. Dados dois números naturais a e b, com com $a \neq 0$, diz-se que a divide b, quando existir um número natural k, tal que $b = a \cdot k$. Neste caso, podemos dizer que são equivalentes as afirmações:

(i) a é um divisor de b ou a divide b $(a|b)$;

(ii) a é um fator de b;
(iii) b é um múltiplo de a.

Proposição 1. Considere os números naturais a, b, c e $d \in \mathbb{Z}$, com $a \neq 0$. Temos:

(i) $1|a$;
(ii) $a|a$;
(iii) $a|0$;
(iv) Se $a|b$ e $b|c$, então $a|c$;
(v) Sejam a, b, c e d, números naturais, com $a \neq 0$ e $c \neq 0$, então, se $a|b$ e $c|d$, então $(ac) \mid (bd)$;
(vi) Se $a|b$ e $a|c$, então $a|b \pm c$;
(vii) Se $a|b$, então $a|bc$;
$(viii)$ Se $a|b$ e $a|c$, então $a|m \cdot b + n \cdot c$, quaisquer $m, n \in \mathbb{Z}$.
$(viii)$ Sejam a e b números naturais, ambos diferentes de zero, tem-se que se $a|b$, então $a \leqslant b$
(ix) Se $b|a$ e $a \neq 0$ então $|b| \leqslant |a|$. (Todo divisor de a é menor ou igual a $|a|$;
(x) Se $b|a$ e $a|b$, então $a = \pm b$;
(xi) Se $b|1$, então $b = \pm 1$;
(xii) $a|b \Leftrightarrow -a|b \Leftrightarrow a|-b \Leftrightarrow -a|-b$

Demonstração.
(i) De fato, $1|a$ pois $a = a.1$ para todo inteiro a.
(ii) De fato, $a|a$ pois $a = 1.a$ (Propriedade reflexiva).
(iii) De fato, $a|0$ pois $0 = a.0$
(iv) Se a é divisor de b então, existe um úmero natural k, tal que $b = ak$.
Da mesma forma, se b é divisor de c então, existe um natural q, tal que $c = b \cdot q$.
Logo:

$$c = b \cdot q \Rightarrow c = a \cdot k \cdot q \Rightarrow c = a \cdot (kq).$$

Ou seja, a é divisor de c.
(v) Se a divide b, então existe um número natural k, tal que $b = ak$.
Da mesma forma, se c divide d, então existe um número natural q, tal que $d = cq$.
Temos que:

$$bd = (ak) \cdot (cq) = (ac) \cdot (kq).$$

Ou seja,$(a \cdot c)$ é um fator de $(b \cdot d)$, demonstrando a preposição.

(vi) Se $a|b$ e $a|c$ então existem q_1 e q_2 inteiros tais que:

$b = a \cdot q_1$ e $c = a \cdot q_2$.

Somando as duas equações temos:

$$b + c = a(q_1 + q_2).$$

Portanto $a|b + c$.

Para a subtração demonstra-se de maneira análoga.

(vii) Se $a|b$ então existe um número inteiro q tal que, $b = aq$.

Multiplicando a equação por um inteiro c temos que, $bc = a \cdot (qc)$. Portanto $a|bc$.

$(viii)$ Se $a|b$ e $a|c$ temos pelo item anterior que $a|bm$ e $a|cn$ para quaisquer inteiros m e n.

Logo, pelo item (vi) segue que $a|bm + cn$

(ix) Se $a|b$ com $b \neq 0$, então existe um inteiro $q \neq 0$ tal que $b = aq$.

Logo:

$$|b| = |aq| = |b| \cdot |q| \geqslant |a|.$$

Portanto,$|a| \leqslant |b|$

(x) Suponhamos que $a|b$ e que $b|a$. Se $a = 0$ ou b =0, temos que $a = b = 0$.

No caso $a, b \neq$0 temos pelo item (ix) que $|a| \leqslant |b|$ e $|b| \leqslant |a|$.

Logo, $|a| = |b| \Rightarrow a = \pm b$

(xi) Suponhamos que $a|1$. Do item (i) temos que $1|a$ para todo inteiro a.

Logo pelo item anterior segue que $a = \pm 1$

$(xii) a|b \Leftrightarrow b = aq$, $q \in \mathbb{Z} \Leftrightarrow$

$b = (-a) \cdot (-q)$, $-q \in \mathbb{Z} \Leftrightarrow$

$-b = a.(-q)$, $q \in \mathbb{Z} \Leftrightarrow$

$-q \in Z \Leftrightarrow -b = (-a) \cdot q$, $-q \in \mathbb{Z}$

$\Leftrightarrow -b = (-a) \cdot q$, $q \in \mathbb{Z}$

□

3.1.1 Divisão Euclidiana

Todos nós aprendemos fazer a operação de divisão nas etapas iniciais da vida escolar, mas muitos não entendem o processo, realizam-no automaticamente como uma receita infalível (ESQUINCA. 2013) . Primeiramente, precisamos saber que cada elemento da divisão possui um nome. Observe que ao dividir 15 e 13 por três respectivamente teremos os seguintes resultados:

$$15 = 3 \cdot 5 + 0 \tag{3}$$

$$13 = 3 \cdot 4 + 1 \tag{4}$$

Cada número das respectivas divisões recebem um nome específico sendo que em ambas o divisor é o número três. Além do divisor o cálculo apresenta: dividendo (15 e 13), quociente (5 e 4) e resto (0 e 1).

Na equação (3) como o resto da divisão foi zero, dizemos que esta é uma divisão exata. Se quisermos verificar se nossa divisão está correta, podemos multiplicar o quociente pelo divisor, isto é, $5 \cdot 3 = 15$. O resultado deve ser exatamente o dividendo, no caso 15. Esse processo é conhecido como a prova real da divisão.

Quando o resto da divisão não for zero, como na equação(4), dizemos que a divisão é inexata ou, simplesmente, que a divisão não é exata, desse modo, o produto do quociente pelo divisor deverá ser acrescido do resto para se obter o dividendo.

Este processo nada mais é do que a aplicação do algoritmo de Euclides surgido na sua obra Os Elementos (c. 300 a.C.), que é um dos mais antigos algoritmos ainda em uso.

O processo exposto acima nada mais é do que uma aplicação da divisão euclidiana, pois foi desenvolvido e generalizado por Euclides de Alexandria em "Os Elementos". Nele podemos notar que a divisão está extramente ligada à multiplicação, ou seja, uma é o inverso da outra.

Euclides de Alexandria foi um matemático platônico e possível escritor grego conhecido como o "Pai da Geometria" (BOYER. 2003). Além da sua principal obra "Os Elementos" escreveu sobre perspectivas, secções cônicas, geometria esférica, teoria dos números e rigor. Existem poucas referências a respeito de Euclides, de tal forma que as datas de nascimento e local , morte e circunstâncias são desconhecidas. Nenhuma imagem ou descrição da aparência física de Euclides foi feita durante sua vida portanto as representações de Euclides em obras de arte são o produtos da imaginação artística. O que se sabe é que a morte de Alexandre, o Grande, levou a disputas entres os generais do exército grego. Em em 306 a.C. o controle da parte egípcia do império

estava nas mãos de Ptolomeu I [2], e esse governante pôde voltar à atenção para esforços construtivos. Após a criação de uma escola em Alexandria conhecida como Museu, chamaram um grupo de sábios de primeira linha, entre eles Euclides, que era um dos autores mais bem sucedidos da época (BOYER. 2003).

Ainda segundo Boyer (2003) "Os Elementos" não só constituem a mais antiga e importante obra matemática grega a chegar até nós, mas o texto mais influente de todos os tempos. Composto em 300 a.C. aproximadamente e copiado muitas vezes até chegarem em nós por traduções árabes, mais tarde traduzidas para o latim no século doze, e finalmente, no século XVI, em vernáculo. A primeira versão impressa de "Os elementos" apareceu em Veneza, em 1482, um dos primeiros livros de matemática impressos. Calcula-se, pois, que desde então pelo menos mil edições foram publicadas e certamente nenhuma obra matemática teve influência comparável à de Euclides.

O Algoritmo de Euclides é apresentado por vários autores de livros de aritmética, porém usaremos como referencial pra nosso trabalho Hefez (2013), que apresenta uma teoria direcionada ao curso do PROFMAT. Assim, na sequência serão apresentados e demostrados teoremas e proposições que tratam desse assunto, para que no capítulo de congruências e de aplicações das mesma possamos utilizá-los para desenvolver alguns procedimentos de maneira hábil.

Teorema 2. *(*Algoritmo de Euclides) Dados $a \in \mathbb{Z}_+^*$ *e* $b \in \mathbb{Z}^*$ Existem dois únicos inteiros q e r tais que $a = bq + r$, com $0 < r < q$, onde q é o maior número, tal que $b \cdot q \leqslant a \leqslant b \cdot (q + 1)$

Demonstração.

Inicialmente mostraremos a existência de q e r. Em seguida mostraremos suas unicidades.

Temos que ou a é um múltiplo de b ou a está situado entre dois múltiplos qb e $(q + 1)b$ de$b$, para algum $q \in \mathbb{Z}$.

Se a é múltiplo de b, digamos, $a = bk$, trivialmente temos $q = k$ e $r = 0$.

Caso a não seja múltiplo de b, é fato que teremos:

$$qb < n < (q + 1)b.$$

Nesta desigualdade podemos subtrair qb de todos os membros, tendo assim:

[2] Ptolomeu I Sóter foi um general macedónio de Alexandre, o Grande que se tornou sátrapa do Egito de 323 a.C. a 283 a.C., fundando a Dinastia Ptolemaica

$$0 < a - qb < b$$

Tomemos:

$$a - qb = r \Rightarrow a = bq + r;\ 0 < r < b.$$

Segue que, quando $r = 0$, a é múltiplo de b.

Para provar a unicidade de q e r, suponhamos que existam outros inteiros r_0 e q_0 tais que:

$$a = bq_0 + r_0 \text{ , com } 0 < r_0 < a.$$

Desta forma temos que:

$$a = bq + r = bq_0 + r_0 \Rightarrow (r - r_0) = (q - q_0)b.$$

Percebemos assim que $(r - r_0)$ é múltiplo de b e como $-b < r - r_0 < b$, o único valor possível é:

$$r - r_0 = 0 \Rightarrow r = r_0.$$

Desta forma, $q = q_0$.

□

Exemplificando, efetuaremos a divisão de 22 por 5 e -54 por 8. Desse modo temos que:

$$22 = 5 \cdot 4 + 2 \text{ e } 0 < 2 < 5,\ -54 = 8 \cdot (-7) + 2 \text{ e } 0 < 2 < 8.$$

Assim, pelo o Algoritmo de Euclides , temos que o resto e o quociente da divisão de 22 por 5, são 2 e 4 respectivamente. Já da divisão de -54 por 8, são 2 e -7.

3.1.2 Máximo Divisor Comum

Para facilitar o entendimento, antes de generalizar a definição de máximo divisor comum antes consideraremos os números 20 e 45. Indicando por $D_{(20)}$ os divisores de vinte e $D_{(45)}$ os divisores de 45, faremos uma listagem dos mesmos. Assim teremos:

$$D_{(20)} = \{1, 2, 4, 5, 10, 20\}$$

$$D_{(45)}=\{1,3,5,9,15,45\}$$

Da listagem acima, segue que $D_{(20)} \cap D_{(45)} = \{1,5\}$, sendo que Máx $D_{(20)} \cap D_{(45)} = 5$, ou seja, 5 é o maior número pertencente ao conjunto interseção de $D_{(20)}$ e $D_{(45)}$.

Definição 2. Dados $a, b \in \mathbb{Z}$, não ambos nulos, dizemos que $d \in \mathbb{Z}^*$ é divisor comum de a e b se $d|a$ e $d|b$.

Exemplo 3. Tem-se que 3 é divisor comum de 90 e 45 pois $3 \mid 90$ e $3 \mid 45$.

Definição 3. Dados $a, b \in \mathbb{Z}$, não ambos nulos, dizemos que $d \in \mathbb{Z}^*$, é Máximo Divisor Comum de a e b, quando d cumpre duas condições:

(i) $d|a$ e $d|b$;

(ii) Se $e \in \mathbb{Z}$, tal que $e|a$ e $e|b$, então $e|d$, ou seja, d é o maior divisor comum de a e b.

A definição anterior pode ser extendida para uma quantidade finita de números inteiros $a_1, a_2, a_3, ..., a_n$ e esta será denotada simplesmente por $mdc(a_1, a_2, a_3, ..., a_n)$.

Imagine agora fazer este processo para um número muito grande, ou um número com muitos divisores. Seria um tanto trabalhoso listar todos eles. Portanto definiremos e apresentaremos alguns teoremas e proposições que facilitarão determinar o Máximo Divisor Comum de números inteiros.

Lema 1. Dados $a, b, q, r \in \mathbb{Z}$ tais que, $a = bq + r$, então $mdc(a, b) = mdc(b, r)$.

Demonstração.

Sejam $d = mdc(a, b)$ e $d_0 = mdc(b, r)$.

Como $d|a$ e $d|b$ temos que $d|(a-qb)$.

Logo, $d|r$, pois $r = a-qb$. Uma vez que $d|b$ e$d|r$, pela Definição (3), então $d|d_0$.

Por outro lado, $d_0|r$ e $d_0|b$, segue que $d_0|(qb+r)$. Assim, $d_0|a$. Portanto, pela pela Definição(3), $d_0|d$.

Como d_0, d são positivos, concluímos que $d = d_0$.

□

Teorema 3. Dados $a, b \in \mathbb{Z}$, existe um inteiro positivo d, que é máximo divisor comum de a e b.

Demonstração.

Considere $a, b \in \mathbb{Z}$. Notemos que caso, $a|b$ ou $a = 1$, temos $mdc(a, b) = |a|$.

Assim podemos supor que $1 < a < b$ e que a não divide b.

Logo pelo Algoritmo de Euclides existem q_1, r_1, tais que:

$$b = aq_1 + r_1 \text{ , com } 0 < r_1 < a \text{ .}$$

Daí surgem duas possibilidades:

(i) Se $r_1|a$, então usando o lema 1 temos que:

$$r_1 = mdc(a, r_1) = mdc(a, b - q_1 a) = mdc(a, b).$$

(ii) $r_1 \nmid a$, aplicando o Algoritmo de Euclides em a e r_1 , desta maneira existem inteiros q_2 e r_2, tais que:

$$a = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1 < a \text{ .}$$

O que também nos dá duas possibilidades:

$*r_2|r_1 \Rightarrow r_2 = mdc(r_1, r_2) = mdc(r_1, a - q_2 r_1) = mdc(r_1, a) = mdc(b - q_1 a, a) = mdc(a, b)$.

$**$Se $r_2 \nmid r_1$.

Aplicando novamente o Algortimo de Euclides, vimos que existem inteiros q_3 e r_3, tais que:

$$r_1 = r_2 q_3 + r_3, 0 < r_3 < r_2 < r_1 < a.$$

Como, este procedimento não é infinito, a sequência $a > r_1 > r_2 > r_3...$, possui um menor elemento.

Portanto, para algum n teremos que $r_n|r_n - 1$, pois em algum momento teremos que o resto é igual a zero, implicando em $mdc(a, b) = r_n$.

Para provar a unicidade suponhamos que $mdc(a, b) = d$ e $mdc(a, b) = d_0$.

Notemos que tanto d, quanto d_0 são divisores comuns de a e b, assim $d|d_0$ e $d_0|d$, e como d e d_0 são ambos positivos segue que $d = d_0 = mdc(a, b)$.

□

Proposição 2. Sejam os números inteiros a, b, c, d, d_0 com d *e* d_0 positivos. Se $d = mdc(a, b)$ e $d_0 = mdc(a, b, c)$, então $d_0 = mdc(mdc(a, b), c) = mdc(d, c)$.

Demonstração.

Seja $d_0 = mdc(a, b, c)$ e $d_1 = mdc(d, c)$, com $d = mdc(a, b)$.

Queremos mostrar que $d_0|d_1$ e $d_1|d_0$.

Daí, como d_0 e d_1 são positivos por definição, então $d_0 = d_1$

De $d_0 = mdc(a, b, c)$, segue por definição, que $d_0|a$ e $d_0|b$, e como $d = mdc(a, b)$ então $d_0|d$, e pelo fato de $d_0|c$, segue que $d_0|d_1$, pois $d_1 = mdc(d, c)$.

Por outro lado, $d_1 = mdc(d, c)$ por definição, $d_1|d$ e $d_1|c$.

Agora como $d = mdc(a, b)$, por definição $d|a$ e $d|b$, daí segue que $d_1|a$ e $d_1|b$, mas $d_1|c$, logo $d_1|d_0$, pois $d_0 = mdc(a, b, c)$.

Donde concluímos que $d_1 = d_0$.

□

Proposição 3. Dados $a, b \in \mathbb{Z}$ *e* $d = mdc(a, b)$. As seguintes afirmações são verdadeiras:

(i) Se $a = 0$ e $b = 0$, então $d = |b|$, já que $d \in \mathbb{Z}^*$;
(ii) Se $d = mdc(a, b)$, então $d = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$.

Demonstração.

(i) Se $a = 0$ e $b = 0$, teremos que existe $d \in \mathbb{Z}$; $d = mdc(0, 0) \Rightarrow d = 0$

(ii) Dados $a, b \in Z$, não ambos nulos. Temos que o maior divisor de a e $-a$ é $|a|$. Dessa forma, $mdc(a, b) = mdc(-a, b)$ e analogamente $mdc(a, -b) = mdc(-a, -b) = mdc(a, b)$.

□

Esses resultados apresentam uma maneira recursiva de se utilizar o Algoritmo Euclidiano, sendo que de acordo com Hefez(2013) houveram apenas aperfeiçoamentos do processo apresentado pelo próprio Euclides em "Os Elementos" que é o mais utilizado nos dias atuais. Ele consiste em se dividir o maior número pelo menor e no processo seguinte fazer o mesmo utilizando o quociente e o resto da divisão anterior, até que o resto final seja zero,assim o máximo divisor comum será o menor resto, diferente de zero. Veja o exemplo a seguir.

Exemplo 4. Determine o $mdc(680, 150)$:

Solução:

$$680 = 150 \cdot 4 + 80$$

$$150 = 80 \cdot 1 + 70$$

$$80 = 70 \cdot 1 + 10$$

$$70 = 10 \cdot 7$$

Verificamos que o resto zero aparece quando dividimos 70 por 10, assim o menor resto diferente de zero é o Máximo divisor comúm entre 680 e 150. Portanto o $mdc(680, 150)$ é 10.

Teorema 4. (Relação de Bézout) Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que $mdc(a, b) = a \cdot n + b \cdot m$.

Em outras palavras, a relação diz que o $mdc(a, b)$ pode ser escrito como combinação linear de a e b.

Demonstração.

Consideremos o conjunto de todos os números positivos da forma $a \cdot n + b \cdot m$, onde o m e o n podem variar ao longo dos inteiros.

É óbvio que esse conjunto contém alguns elementos, mesmo que a e b sejam negativos, porque se pusermos $m = a$ e $n = b$ temos que $a^2 + b^2$ é um número positivo e por isso pertence a esse conjunto.

Obviamente $mdc(a, b)$ divide todos os elementos desse conjunto. Seja d o menor desses números.

Usando o Algoritmo de Euclides, existem q e r, inteiros tais que:

$$a = qd + r.$$

Mas $d = am + bn$, logo:

$$r = qd - a = q(am + nb) - a = (qm - 1)a + nb.$$

Portanto r pertence ao conjunto. Uma vez que d é o menor elemento do conjunto, obtemos que $r = 0$.

Assim: $d|a$.

De forma análoga se prova que $d|b$.

Se houvesse algum número c maior que d tal que $c|a$e $c|b$, então $c|d$, o que entra em contradição com $c > d$. Assim d é o $mdc(a, b)$ e portanto $mdc(a, b)$ pode ser escrito da forma $am + bn$.

□

Exemplo 5. Aplicar o teorema de Bézout para os inteiros $a = 41$ e $b = 12$.

Solução:

Fazendo as divisões temos que:

$$41 = 12.3 + 5 \Rightarrow 5 = 41–12.3 \tag{5}$$

$$12 = 5.2 + 2 \Rightarrow 2 = 12–5.2 \tag{6}$$

$$5 = 2.2 + 1 \Rightarrow 1 = 5–2.2 \tag{7}$$

Substituindo as equações (7) em (6) temos que:

$$5–2.2 = 1 \Rightarrow 5–2.(12 - 5.2) = 1.$$

Logo,

$$5.5 + 12.(-2) = 1.$$

Novamente substituindo a equação (5) na equação acima, temos que:

$$5.(41–12.3) + 12.(-2) = 1.$$

Portanto,

$$41.(5) + 12.(-17) = 1.$$

Então $m = 5$ e $n = -17$.

O resultado anterior é muito utilizado em resolução de problemas, pois dele surge a demostração de Equações Diofantinas Lineares, cujo é uma aplicação muito importante de aritmética, e será ápresentada ao final deste capítulo.

3.2 Números Primos

Os números primos possuem um papel fundamental na matemática e facilitam o entendimento e resolução de inúmeros problemas que vem sendo resolvidos ao longo de várias gerações matemáticas. Esses números são os próprios átomos da aritmética. São os números indivisíveis que não podem ser representados pela multiplicação de dois números menores. A importância matemática dos primos se deve a sua capacidade de gerar todos os demais números (SAUTOY. 2007).

Apresentaremos na sequência, definições e teoremas relevantes para a compreensão deste conceito, pois no capítulo de aplicações utilizaremos estes conceitos para determinar alguns critérios de divisibilidade.

Definição 4. Um número natural maior que 1 que só possui como divisores positivos 1 e ele mesmo é chamado de número primo.

Sejam a, p e q números inteiros, p e q primos e q não nulo, da definição acima decorre que:

(i) Se $p|q$, então $p = q$;

(ii) Se $p\nmid a$, então $mdc(p, a) = 1$.

Exemplo 6. Seja $p = 3$ e q primo, se $p|q$ temos que $q = 3$. Por outro lado sendo $p = 3$ e $a = 5$ temos que $3\nmid 5$, logo $mdc(3, 5) = 1$.

Definição 5. Diz-se que dois números a e b são primos entre si se $mdc(a, b) = 1$. Um número maior que 1 e que não é primo será dito número composto.

Proposição 4. Sejan $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$

Demonstração.

Basta provar que, se $p|ab$ e $p \nmid a$,então $p|b$. Mas, se p$\nmid$a, temos que $mdc(p, a) = 1$, então o resultado segue de forma direta.

□

Corolário 1. Se $p, p_1, \cdots, p_n$ são números primos e $p|p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \cdots, n$. (A demonstração deste resultado é feita por indução sobre n)

Teorema 5. ***(Teorema Fundamental da Aritmética):*** Todo número natural n maior do que 1 ou é primo ou se escreve de modo único(a menos da ordem dos fatores) como um produto de números primos**.**

Demonstração.

Se $n = 2$, o resultado é claramente verificado, pois $2 = 1 \cdot 2$.

Suponhamos que o resultado seja válido para todo número menor do que n. Vamos provar que pra n também vale.

Se o número é primo, nada temos a demonstrar.

Suponhamos então que n seja composto, assim existem números naturais n_1 e n_2 tais que:

$$n = n_1 \,.\, n_2, \text{ com } 1 < n_1 < n \text{ e } 1 < n_2 < n.$$

Por hipótese de indução, temos que existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ tais que:

$$n_1 = p_1 \cdots p_r \text{ e } n_2 = q_1 \cdots q_s.$$

Portanto:

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

Para mostrar a unicidade suponha que $n = p_1 \cdots p_r = q_1 \cdots q_s$, com p_i e q_j primos,onde $i = 1, \cdots, r$ e $j = 1, \cdots, s$

Como $p_1 | q_1 \cdots q_s$, pelo corolário anterior, temos que $p_i = q_j$ para algum i e j.

Após reordenamento de $q_1, \cdots, q_s$ podemos supor que seja q_1.

Portanto $p_2 \cdots p_r = q_2 \cdots q_s$. Como $p_2 \cdots p_r < n$.

Pela hipotese de indução chegamos que $r = s$ e os p_i e os q_j são iguais aos pares.

□

Segundo Hefez (2013), outro fato importante , bem explorado e fixado por Euclides em "Os Elementos (Livro IX)" é a questão da infinidade dos números primos e sua distribuição, que seguem no teorema seguinte.

Teorema 6. Existem infinitos números primos.

Demonstração.

Supondo, por absurdo, que exista um número finito de números primos $p_{2,} \cdots, p_r$,considere o número natural :

$$n = p_2 \cdots p_r + 1$$

Pelo teorema fundamental da aritmética temos que o número n possui um fator primo p que , portanto deve ser um dos $p_1, \cdots, p_r$, e, consequentemente, divide o produto $p_1 p_2 \cdots p_r$. Mas isto implica que p divide 1, o que é absurdo.

□

Lema 2. Se um número natural $n > 1$, não é divisível por nenhum primo p tal que $p^2 \leqslant n$, então ele é primo.

Demonstração.

Suponhamos , por absurdo, que n não seja divísível por nenhum número primo p tal que $p^2 \leqslant n$ e que não seja primo.

Seja q o menor número que divide n; então, $n = qn_1$, com $q \leqslant n_1$.

Segue daí que: $q^2 \leqslant qn_1 = n$.

Logo n é divisível por um número primo q tal que $q^2 \leqslant n$, absudo.

□

Exemplo 7. Verifque se o número 353 é primo ou composto.

Solução:

De acordo com o resultado anterior se verificarmos que 353 não é divisível pelos primos: 2, 3, 5, 7, 11, 13 e 17 terminaremos o processo, visto que $19^2 \geqslant 353$. Caso contrário será composto. Pelo Algoritimo de Euclides temos que:

$$353 = 2 \cdot 176 + 1$$

$$353 = 3 \cdot 117 + 2$$

$$353 = 5 \cdot 70 + 3$$

$$353 = 7 \cdot 50 + 3$$

$$353 = 11 \cdot 32 + 1$$

$$353 = 13 \cdot 27 + 2$$

$$353 = 17 \cdot 20 + 13$$

Logo 353 é primo.

Proposição 5. Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.

Demonstração.

($\Longrightarrow$) Sejam a e b dois inteiros primos entre si, ou seja, $mdc(a, b) = 1$.

Pelo Teorema de Bézout, existem m, n, números inteiros, tais que $ma+nb = 1$.

($\Longleftarrow$) Seja $d = mdc(a, b)$, então $d|a$ e $d|b$, implica que $d|(ma + nb)$, ou seja, $d|1$.

Portanto, $d = 1$.

□

3.2.1 Crivo de Erátostenes

Eratóstenes foi um matemático grego que viveu entre os anos 276 a.C. até 194 a.C e estudou em Alexandria. Antes de se chegar a uma conclusão da finidade

ou não de números primos, Eratóstenes desenvolveu um método para descobrí-los , percebendo assim que são infinitos (BARBOSA. 2013). Isto não com uma fórmula, mas através de uma tabela de números naturais que consiste em eliminar números múltiplos de outros, em um conjunto limitado, restando assim, apenas os números primos. Na teoria o Crivo pode ser feito para qualquer quantidade de números. Porém, este é inviável para testes de primalidade de grandes números (centenas de dígitos). Isto ocorre devido ao fato de que a complexidade de tempo cresce exponencialmente com o número de dígitos, ou seja, quanto maior for o n, mais difícil de aplicar o Crivo de Eratóstenes.

O processo para uso do Crivo é feito da seguinte forma:

- Escreve-se numa tabela os números de 1 até n;
- Remove o número 1 pela definição de primos;
- Elimina-se os múltiplos dos primos como 2,3,5,...;
- Termina quando os múltiplos do maior primo e menor ou igual a $\sqrt{n}$, tenham sido descobertos.

Para melhor exemplificar o processo exposto, observe na figura abaixo os números de 1 a 100, dos quais são eliminados todos os não primos. Neste caso, marcam-se os multiplos de 2, $3, 5$ e 7, pois $11^2 \geqslant 100$.

Figura 2: Crivo de Erátostenes
Fonte:http://pt.static.z-dn.net/files/de5/36fe39f24154150cfd71be25375c4e3a.jpg

Desse modo, os números primos entre 1 e 100 são:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ e 97.

3.2.2 Pequeno Teorema de Fermat

Pierre de Fermat foi considerado o "Príncipe dos Amadores". Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Estudou direito em Toulouse, onde serviu no parlamento local, primeiro como advogado, mais tarde como conselheiro. Dedicava à Matemática apenas as suas horas de lazer e, mesmo assim, foi considerado um dos maiores matemáticos de seu tempo (BOYER. 2003). Por isso um de seus resultados que irá nos auxiliar em se tratando de congruências modulares é "O Pequeno Teorema de Fermat", que além de facilitar muito a resolução de algumas situações-problema, é considerado a base para a criação dos Testes de Primalidade modernos, sendo que a maioria destes testes foi uma modificação ou uma generalização do Teste de Fermat – que tem como base o Pequeno Teorema de Fermat, provado no próximo resultado.

Teorema 7. ***(Pequeno Teorema de Fermat):*** Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo a$\in \mathbb{Z}$.

Demonstração.

Se $p = 2$, o resultado é imediato, visto que o resultado $a^2 - a = a(a-1)$ que é par.

Suponhamos p ímpar. Neste caso basta mostrar o resultado para $a \geqslant 0$.Vamos provar por indução sobre a. O resultado vale para $a = 0$, pois $p|0$.

Supondo o resultado válido para a, mostraremos que também vale para $a+1$. Pelo Binômio de Newton, temos:

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a.$$

Por hipótese de indução, o segundo membro da igualdade acima é divisível por p, ou seja, temos que o resultado é verdadeiro para todo p primo e $a \in \mathbb{R}$.

□

Corolário 2. Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.

Demonstração.

Como pelo Pequeno Teorema de Fermat, $p|\ a(a^{p-1} - 1)$ e como $mdc(a, p) = 1$, segue imediatamente que p divide $a^{p-1} - 1$.

□

Esse resultado é considerado também como parte do teorema, visto ser um caso particular do mesmo.

Na história da humanidade o Pequeno Teorema de Fermat se destaca, pois há várias aplicações para o desenvolvimento dos critérios de divisibilidade, potenciação de congruências e principalmente na parte de criptografia avançada, a qual não será abordada nesta dissertação, tendo em vista o público alvo ser o ensino fundamental.

3.3 Equações Diofantinas Lineares

As Equações Diofantinas Lineares(EDL) são aplicações muito importantes do conceito de divisibilidade, porém não é explorada no ensino fundamental II. Vejamos o seguinte problema: "Uma corporação militar adquiriu automóveis e motocicletas. Considerando que a soma dos 2 pneus de cada moto e dos 4 pneus de cada automóvel é igual a 152 pneus, determine as quantidades possíveis de carros e motos?"

Esse tipo de problema é comúm de se aparecer em livros didáticos das séries finais do ensino fundamental como: "A conquista da Matemática- 8º Ano" de Benedicto Castrucci/José Ruy Giovanni/José Ruy Giovanni Jr; "Matemática e Diferença-8º ano " de Ayrton Olivares/ José Roberto Bonjorno/ Regina Azenha/ Tânia Gusmão, entre outros vários livros. Na maioria das vezes fica definida para o aluno apenas como uma equação de primeiro grau com duas incógnitas. Sua resolução geralmente é apresentada de tal forma que o aluno leve a dependência de uma dessas incógnitas a partir de um valor dado a outra. No entanto o verdadeiro teor do problema é deixado a mercê. Vejamos como é apresentado o processo de resolução por vários livros didáticos:

Como se tratam de veículos, então os valores de x e y devem necessáriamente ser positivos maiores ou iguais a 1 .

Tomando:

x= número de motos compradas;

y= número de carros.

Teremos uma equação do tipo: $2x + 4y = 152$.

Subtraindo $4y$ a ambos os membros da igualdade teremos:

$$2x = 152 - 4y.$$

Dividindo por 2 ambos reduziremos à equação semelhante:

$$x = 76 - 2y$$

Através de tabelas podemos atribuir valores para y , determinado assim valores de x. Note que:

y	$x = 76 - 2y$	x
1	$x = 76 - 2 \cdot 1$	74
2	$x = 76 - 2 \cdot 2$	72
3	$x = 76 - 2 \cdot 3$	70
4	$x = 76 - 2 \cdot 4$	68
$\vdots$	$\vdots$	$\vdots$
37	$x = 76 - 2 \cdot 37$	2

Tabela 1: EDL

Ao analisarmos o processo feito percebemos que podem haver vários valores pra ambas as incógnitas. Isto deve ser bem definido para o aluno, ou seja, o fato de a solução não ser única, visto que na medida que um foi aumentando o outro foi diminuindo, mas o valor final de rodas continuou o mesmo.

Na verdade esse tipo de problema pode ser resolvido por meio de EDL e sem problema algum pode ser trabalhado nas séries finais do ensino fundamental II, pois exige apenas conhecimentos de conceitos já estabelecidos logo nos 6^{o} e 7^{o} anos .

Uma Equação Diofantina Linear é uma equação polinomial que permite a duas ou mais variáveis assumirem apenas valores inteiros. A designação equação diofantina, é uma singela homenagem dos matemáticos a Diofante de Alexandria - grego do século III d.c. Muito pouco se sabe sobre a vida do matemático Diofante, que deve ter vivido apenas 84 anos, segundo interpretações dos livros de História da Matemática.

Resolver uma EDL significa achar todas as soluções inteiras dessa equação. O processo para essa resolução é uma ferramenta já bem conhecida pelos alunos, porém não tão detalhada como se deveria. Este processo é demonstrado nos próximos resultados:

Definição 6. Denomina-se Equação Diofantina Linear, toda equação da forma $ax+by = c$, onde a, b e $c \in \mathbb{Z}$ e x e y incógnitas a serem determinadas em $\mathbb{Z}$.

Existem algumas perguntas feitas em uma análise acerca de uma equação Diofantina :

- Existe alguma solução?
- Existe alguma solução além daquelas achadas facilmente por inspeção?
- Existe uma quantidade finita ou infinita de soluções?
- Todas as soluções podem ser achadas em teoria? É possível computar todas as soluções?

Estes problemas tradicionais comumente ficaram por séculos sem solução até alguns matemáticos começarem a entender sua profundidade (em alguns casos), ao invés de tratá-los como quebra-cabeças. A resposta destes questionamentos podem ser respondidas pelas proposiçoes abaixo.

Proposição 6. Uma equação diofantina $ax+by = c$ admite infinitas soluções nos inteiros se, e somente se, $mdc(a, b)$ divide c.

Demonstração.

($\Longrightarrow$)Seja $ax + by = c$, onde a, b e c são inteiros e que possua uma solução inteira, ou seja, existem x_0 e y_0 inteiros tais que:

$$ax_0 + by_0 = c. \tag{8}$$

Suponha que $d = mdc(a, b)$, assim existem m e n inteiros tais que:

$$a = dm \text{ e } b = dn, \text{ pois } d|a \text{ e } d|b.$$

Substituindo na equação (8) temos:

$$c = ax_0 + by_0 = dmx_0 + dny_0 c = d.(mx_0 + ny_0). \tag{9}$$

Como $mx_0 + ny_0$ é inteiro, da equação (9), obtemos:

$$dq = ax_0 q + by_0 q.$$

($\Longleftarrow$)Como $c = dq$, substituindo:

$$c = a(x_0 q) + b(y_0 q).$$

Se chamarmos de $x_0 q$ e $y_0 q$ de x e y respectivamente, temos $c = ax + by$.

Portanto se $d|c$ existem x e y que serão soluções da equação diofantina linear.

□

Exemplo 8. Resolver a equação diofantina linear $3x + 6y = 18$.

Solução:

Por se tratar de uma equação que apresenta números pequenos podemos obter o resultado por tentativa e erro. Desse modo, temos que:

$$3 \cdot (4) + 6 \cdot (1) = 18$$

$$3 \cdot (-6) + 6 \cdot (6) = 18$$

$$3 \cdot (10) + 6 \cdot (-2) = 18.$$

Logo, os pares de inteiros: 4 e 1, -6 e 6, 10 e -2, são soluções da equação dada.

Exemplo 9. É possível se criar galinhas e coelhos, tal que a soma de seus pés seja 95?

Modelando o problema dado podemos representa-lo pela EDL: $2x + 4y = 95$. No entanto temos que $mdc(2, 4) \nmid 95$.

Logo não há solução inteira para equação formada. Portanto a situação do problema é impossível.

Proposição 7. Seja x_0, y_0 uma solução da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são :

$$\begin{cases} x = x_0 + bt \\ \\ y = y_o - at \end{cases} ; t \in \mathbb{Z}.$$

Demonstração.

Seja x, y uma solução de $ax + by = c$. Assim:

$$ax_0 + by_0 = ax + by = c.$$

Consequentemente:

$$a(x - x_0) = b(y_0 - y). \tag{10}$$

Como $mdc(a, b) = 1$, segue que $b \mid (x - x_0)$.

Logo: $x - x_0 = bt$, $t \in \mathbb{Z}$.

Substituindo a expressão de $(x - x_0)$ acima na equação(10), segue-se que:

$$y_0 - y = at.$$

Por outro lado verifica-se que $x = x_0 + bt$ e $y = y_0 - at$, é solução, pois:

$$ax + by = a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c$$

□

Observação. Para $mdc(a, b) = d \neq 1$ temos que todas as soluções serão:

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_o - \frac{a}{d}t \end{cases} ; t \in \mathbb{Z}.$$

Exemplo 10. Determinar todas as soluções da equação diofantina linear :$172x + 20y = 1000$.

Solução:

Determinamos inicialmente o $mdc(172, 20)$ pelo algoritmo de Euclides, visto o processo de inspeção se torna exaustivo. Assim segue que:

$$172 = 20 \cdot 8 + 12 \Rightarrow 12 = 172 - 20 \cdot 8$$

$$20 = 12 \cdot 1 + 8 \Rightarrow 8 = 20 - 12 \cdot 1$$

$$12 = 8 \cdot 1 + 4 \Rightarrow 4 = 12 - 8 \cdot 1$$

$$8 = 4 \cdot 2 + 0$$

Portanto, o $mdc(172, 20) = 4$ e como $4|1000$, segue-se que a equação dada tem solução.

Agora devemos obter a expressão do inteiro 4 como combinação linear de 172 e 20. Substituindo os restos na equação de trás pra frente a partir do $mdc(172, 20)$ teremos:

$$4 = 12 - 8 \cdot 1$$

$$4 = 12 - (20 - 12 \cdot 1) \cdot 1$$

$$4 = 12 - 20 \cdot 1 + 12 \cdot 1$$

$$4 = 2 \cdot 12 - 20 \cdot 1$$

$$4 = 2 \cdot (172 - 20 \cdot 8) - 20 \cdot 1$$

$$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1$$

$$4 = 172 \cdot 2 - 20 \cdot 16 - 20 \cdot 1 \Rightarrow 4 = 172 \cdot 2 - 20 \cdot 17.$$

Logo temos a equação:

$$4 = 172 \cdot 2 + 20 \cdot (-17).$$

Como queremos uma solução para combinação que resulta 1000, multiplicamos ambos os membros desta igualdade por $1000/4 = 250$ e obtemos:

$$1000 = 172 \cdot 500 + 20(-4250).$$

Portanto, o par de inteiros $x_0 = 500$, $y_0 = -4250$ é uma solução particular da equação proposta, e todas as outras soluções são dadas pelas fórmulas:

$$\begin{cases} x = 500 + (\frac{20}{4})t \Rightarrow x = 500 + 5t \\ y = -4250 - (\frac{172}{4})t \Rightarrow y = -4250 - 43t \end{cases},$$

onde t é arbitrário.

Exemplo 11. Dispondo de R$ 100,00 quais são as combinações possíveis que podemos fazer ao se comprar selos de R$ 5,00 e selos de R$ 7,00.

Solução:

Inicialmente modelando o problema, chamemos de x os selos de R$ 5,00 e de y os selos de R$ 7,00.

A EDL formada será:

$$5x + 7y = 100.$$

Como $mdc(5, 7) = 1$ e $1 \mid 100$, temos que o problema tem solução.

Uma solução particular para o problema é $x_0 = 13$ e $y_0 = 5$.

A solução geral é dada por:

$$\begin{cases} x = 13 + 7t \\ y = 5 - 5t \end{cases}, \ t \in \mathbb{Z}.$$

A única restrição que temos é que x e y devem ser números naturais, pois se tratam de valores. Desse modo temos:

$$13 + 7t \geqslant 0 \text{ e } 5 - 5t \geqslant 0 \Rightarrow t \geqslant -1 \text{ e } t \leqslant 1.$$

Assim segue que t poderá assumir valores, tais que: $-1 \leqslant t \leqslant 1$.

Substituindo os valores possíveis de t na solução geral, determinaremos o resultado do problema. Logo as possíveis combinações de selos são:

- 6 selos de R$ 5,00 e 10 selos de R$ 7,00;
- 13 selos de R$ 5,00 e 5 selos de R$ 7,00;
- 20 selos de R$ 5,00 e nenhum selo de R$ 7,00.

Exemplo 12. (Questão 3-AVF 2014) A secretaria de educação de um certo município dispõe de 5000 reais para gastar na compra de livros: o livro Tipo A, que custa 26 reais a unidade, e o livro Tipo B, que custa 24 reais a unidade. Encontre todas as possibilidades para a compra desses dois tipos de livros, gastando todo o valor disponível.

Solução:

Indicando por x a quantidade de livros do tipo$A$ e por y a quantidade de livros do tipo B, temos que: $26x + 24y = 5000$.

Dividindo ambos os membros da equação por $2 = mdc(26, 24)$, obtemos a equação equivalente:

$$13x + 12y = 2500.$$

Vamos, em seguida, achar uma solução particular x_0, y_0 dessa equação. Note que:

$$13 \cdot (1) + 12 \cdot (-1) = 1,$$

e daí obtemos:

$$13 \cdot (2500) + 12 \cdot (-2500) = 2500.$$

Como procuramos soluções naturais, é conveniente escrevermos:

$$13 \cdot (12 \cdot 208 + 4) + 12 \cdot (-2500) = 2500.$$

Daí :

$$13 \cdot (4) + 12 \cdot (13 \cdot 208 - 2500) = 2500$$

obtendo:

$$13 \cdot (4) + 12 \cdot (204) = 2500 \ .$$

Logo $x_0 = 4$ e $y_0 = 204$ é solução natural particular da equação e, consequentemente, as soluções são:

$$x = 4 + 12t \text{ e } y = 204 - 13t;\ t \in \mathbb{Z}$$

Como procuramos por soluções naturais devemos ter $0 \leqslant t \leqslant 15$, portanto são16 possibilidades.

Exemplo 13. (Profmat-AV1 2014- Questão 5)Determine duas frações positivas que tenham 17 e 23 como denominadores e cuja soma seja igual a $\frac{234}{391}$.

Solução:

o Indicando as duas frações por $\frac{a}{17}$ e $\frac{b}{23}$, onde $a, b \in \mathbb{N}$, temos que:

$$\frac{a}{17} + \frac{b}{23} = \frac{234}{391} \ .$$

Reduzindo ao mesmo denominador obtemos a equação diofantina: $23a + 17b = 234$.

Para determinarmos os valores de a e b, resolveremos a equação diofantina.

Aplicando o algoritmo de Euclides e usando que o$mdc(23, 17) = 1$, temos que:

$$23 \cdot (3) + 17 \cdot (-4) = 1.$$

Multiplicando a equação por 234 teremos:

$$23 \cdot (702) + 17 \cdot (-936) = 234.$$

Para achar a solução minimal devemos encontrar respectivamente os restos das divisões de 702 por 17 e -936 por 23. Aplicando novamente o Algoritmo de Euclides a esses números teremos:

$$23 \cdot (17 \cdot 41 + 5) + 17 \cdot (-936 + 23 \cdot 41) = 234 \Rightarrow$$

$$23 \cdot (5) + 17 \cdot (7) = 234.$$

Logo, $a = 5$ e $b = 7$ é a solução minimal da equação.

Escrevendo a solução geral, onde $t \in \mathbb{Z}$, ($a = 5 + 17t$ e $b = 7 - 23t$), concluimos que $a = 5$ e $b = 7$ formam a única solução, em $\mathbb{N}$, da equação $23a + 17b = 234$.

Portanto, as duas frações positivas são: $\frac{5}{17}$ e $\frac{7}{23}$.

Capítulo 4

Congruência Modular

A Congruência Modular é uma ferramenta que pode auxiliar muito no desenvolvimento do pensamento aritmético e algébrico de nossos alunos. É um tema gerador de excelentes oportunidades de contextualização, pois apresenta a realização de operações aritméticas de uma forma diferente da utilizada normalmente pelos alunos (BARBOSA. 2013).

Desenvolvendo uma pesquisa sobre o tema percebe-se que é um assunto bastante abordado por mestrandos do PROFMAT. Para Esquinca (2013), ela colabora com a solução de algum problemas da atualidade, agilizando o processo de resolução destes no ensino básico. Por outro lado Souza (2015), salienta que é um forte aliado na preparação de alunos para as Olímpiadas Brasileira de Matemática das Escola Públicas (OBMEP).

Assim por ser um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental, formalizaremos os principais conceitos de congruência e suas propriedade para que possamos no capítulo seguinte, mostrar processos de aplicações em situações cotidianas, através de atividades didáticas desafiadoras.

4.1 Congruência módulo m

O conceito de congruência aparece da relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Por exemplo, o número 9 é congruente ao número 2, módulo7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2\, mod(7)$. Essa relação tem um comportamento semelhante à igualdade.

Definição 7. Dados $m, a, b \in Z$. Diremos que a e b são congruentes módulo m, quando o resto das divisões Euclidianas de a e b por m forem os mesmos. Denotaremos que a é congruente a b módulo m da seguinte forma: $a \equiv b\ mod(m)$.

Proposição 8. Considere a, $b \in Z$. Temos $a \equiv b\, mod(m)$ se, e somente se, $m|b-a$.

Demonstração.

($\Longrightarrow$) Suponhamos que $a \equiv b\, mod(m)$.

Pela definição 7 temos que: $a = qm + r$ e $b = q_1 + r$, com $0 < r < m$ e $q, q_1 \in Z$.

Segue então que::

$$b-a = (q_1-q)m \Rightarrow m|(b-a).$$

($\Longleftarrow$) Suponhamos que $m|(b-a)$.

Logo existe $q \in Z$ tal que $b-a = mq$.

Daí:

.

$$b = a + mq.(*) \tag{11}$$

Sejam r e q_1 o resto e o quociente da divisão euclidiana de b por m, isto é:

$$b = mq_1 + r,\ com\, 0 < r < m \tag{12}$$

Das equações (11) e (12) temos que: $a+mq = mq_1+r$, logo, $a = m(q_1-q)+r$, com $0 < r < m$.

Portanto r também é o resto da divisão euclidiana de a por m.

□

Para exemplificar podemos afirmar que $5 \equiv -6\, mod(11)$, pois deixam o mesmo resto na divisão por 11, ou seja $11 \mid 5-(-6)$,o que implica que: $11 \mid 11$.

Observação. $x = 1 \cdot x + 0$ para todo $x \in Z$, ou seja, todo número inteiro quando dividido por 1 deixa resto zero. Portanto para nosso trabalho admitirenos apenas a congruência módulo m , para valores de m maiores que 1, pois o caso $m = 1$ é trivial.

4.2 Propriedades da Congruência Modular

As proposições apresentadas abaixo mostram que a relação de congruência módulo m possui algumas propriedades relevantes tornando-a uma relação de equivalência em $\mathbb{Z}$ e ainda mostrando que a a congruência é compatível a adição e a multiplicação.

Nas propriedades, não se utiliza o caso $m = 1$, pois se usássemos congruência módulo 1, obteríamos $a \equiv b\, mod(1)$que é o mesmo que $1|a–b$, o que é sempre verdade para quaisquer a e b. Por isso excluímos essa possibilidade.

Proposição 9. Dados $m, a, b \in \mathbb{N}$ tais que $m > 1$. São verdadeiras as sentenças*:*

i) $a \equiv a\, mod(m)$;

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

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

Demonstração.

i) Como $m|0$, então $m|a–a$, o que nos diz que $a \equiv a\, mod(m)$;

ii) Se $a \equiv b\, mod(m)$, temos que $m|a–b$, logo $a–b = mk$

Multiplicando essa última igualdade toda por (-1), temos que $–(a–b) = –mk$

.

Assim $b–a = m(-k)$, logo $b \equiv a\, mod(m)$;

iii) Se $a \equiv b\, mod(m)$ e $b \equiv c\, mod(m)$, então existem inteiros k e k' tais que:

$$a–b = mk \text{ e } b–c = mk'.$$

Somando membro a membro as duas igualdades anteriores, temos:

$$(a–b) + (b–c) = mk + mk' \Rightarrow a–c = m(k + k').$$

Logo:

$$m|(a–c) \Rightarrow a \equiv b\, mod(m).$$

□

Para melhor exemplificar as propriedades de reflexão, simetria e transitividade observe os exemplos seguintes:

- $3 \equiv 3\, mod(2) \Leftrightarrow 2 \mid (3-3) \Leftrightarrow 2 \mid 0$;
- $5 \equiv 7\, mod(2)$ e $7 \equiv 5\, mod(2) \Leftrightarrow 2 \mid (5-7)$ e $2 \mid (7-2) \Leftrightarrow 2 \mid -2$ e $2 \mid 2$;.
- $15 \equiv 3\, mod(4)$ e $3 \equiv 7\, mod(4) \Rightarrow 15 \equiv 7\, mod(4) \Leftrightarrow 4 \mid (15-3)$ e $4 \mid (3-7)$ $\Rightarrow 4 \mid 12$ e $4 \mid -4$.

4.2.1 Propriedades Operatórias

(i) Se $a \equiv b\, mod(m)$ e $c \equiv d\, mod(m)$, então $a + c \equiv b + d\, mod(m)$;

(ii) Se $a \equiv b\, mod(m)$ e $c \equiv d\, mod(m)$, então $ac \equiv bd\, mod(m)$;

(iii) Se $a \equiv b\, mod(m)$, então $a + c \equiv b + c\, mod(m)$;

(iv) Se $a \equiv b\, mod(m)$, então $an \equiv bn\, mod(m)$, para todo n.

(iv) Se $a \equiv b\, mod(m)$ e $n|m$, então $a \equiv b\, mod(n)$.

Demonstração.

(i) Se $a \equiv b\, mod(m)$ e $c \equiv d\, mod(m)$, então existem inteiros k e k' tais que:

$$a\text{–}b = mk \text{ e } c\text{–}d = mk\text{'}.$$

Somando membro a membro as duas igualdades anteriores, temos:

$$(a\text{–}b) + (c\text{–}d) = mk + mk\text{'} \Rightarrow (a+c)\text{–}(b+d) = m(k+k\text{'}).$$

Logo resulta que:

$$m|[(a+c)\text{–}(b+d)] \Rightarrow a + c \equiv b + d(modm).$$

(ii) A demonstração é análoga ao item (i).

(iii) Se $a \equiv b\, mod(m)$, temos que $a\text{–}b = mk$. Somando e subtraindo c no primeiro membro da igualdade, temos:

$$a\text{–}b + c\text{–}c = mk \Rightarrow (a+c)\text{–}(b+c) = mk.$$

Assim temos que: $a + c \equiv b + c\, mod(m)$.

(iv) Se $a \equiv b\, mod(m)$, então, $m|a–b$.

Sabemos que:

$$an–bn = (a–b)(an - 1 + an - 2b + \cdots + abn - 2 + bn - 1).$$

Como $m|a–b$, então $m|an–bn$. Assim $an \equiv bn\, mod(m)$.

(v)Se $a \equiv b\, mod(m)$, então $m|a–b$.

Como $n|m \Rightarrow n|a–b$.

Logo $a \equiv b\, mod(n)$

□

Das propriedades operatórias demosntradas seguem respectivamente alguns exemplos numéricos de aplicação das mesmas:

- Temos que: $7 \equiv 2\, mod(5)$ e $6 \equiv 1\, mod(5)$, pois $5 \mid (7 - 2)$ e $5 \mid (6 - 1)$.

Multiplicando ambas congruências membro a membro, segue que:

$$42 \equiv 2\, mod(10) \Leftrightarrow 5 \mid 40.$$

- Se $8 \equiv -1\, mod(3)$,pois $3 \mid (8 + 1)$, somando 5 a ambos os lados da congruência teremos que:

$$13 \equiv 4\, mod(3), \text{ pois } 3 \mid (13 - 4) \Rightarrow 3 \mid 9.$$

- Note que: $7 \equiv -3\, mod(10) \Leftrightarrow 10 \mid 10$.Multiplicando por 3 os dois lados da congruência teremos:

$$21 \equiv -9\, mod(10), \text{ pois } 10 \mid (21 + 9).$$

Entretanto a recíproca não é verdadeira , pois $54 \equiv 30\, mod(8)$, mas $9 \not\equiv 5\, mod(8)$.

- Sabemos que: $21 \equiv -9\, mod(10)$, pois $10 \mid 30$, e ainda, $5 \mid 10$.

Logo,

$$21 \equiv -9\, mod(5) \Leftrightarrow 5 \mid 30.$$

Ainda levando em consideração as propriedades apresentadas nos itens (i) e (ii) das propriedades operatórias deriva o resultado abaixo.

Corolário 3. Para todo $n \in \mathbb{N}$, a e $b \in \mathbb{Z}$, se $a \equiv b\, mod(m)$, então tem-se que $a^n \equiv b^n\, mod(m)$.

Outro fato que também é importante e já foi demostrado anteriormente é o caso do Pequeno Teorema de Fermat que pode ser expressado claramente em termos de congruência e fica ainda dividido em dois casos específicos:

(1)Se p é um número primo e $a \in \mathbb{Z}$ e p$|$ a então:

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

(2)Se $p \nmid a$, então:

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

Decorrente do Pequeno Teorema de Fermat com p primo e a, $b \in \mathbb{Z}$ temos ainda três importantes resultados que irão nos auxiliar nas aplicações de congruências tratadas no próximo capítulo:

$(i)\ (a+b)^p \equiv a^p + b^p\, mod(p)$

$(ii)\ (a-b)^p \equiv a^p - b^p\, mod(p)$

$(iii)\ a^p \equiv b^p\, mod(p^2)$

Demonstração.

$(i)\ (a+b)^p \equiv a+b \equiv a^p + b^p\, mod(p)$

$(ii)\, a^p \equiv (a-b+b)^p \equiv (a-b)^p + b^p \, mod(p)$.

Subtraindo b^p em ambos os lados da congruência segue que:

$a^p - b^p \equiv (a-b)^p \, mod(p) \Leftrightarrow (a-b)^p \equiv a^p - b^p \, mod(p)$

(iii) Do item (ii) sabemos que:

$(a-b)^p \equiv a^p - b^p \, mod(p)$

Por hipótese, temos que p divide $ap - bp$ e da congruência acima segue que: $p \mid (a-b)p$.

Logo $p \mid a-b \Rightarrow a \equiv b \, mod(p) \Rightarrow a^i \equiv b^i mod(p)$ para todo $i \in \mathbb{N}$.

Daí tem-se que:

$$a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + b^{p-1} \equiv pb^{p-1} \equiv 0 \, mod(p).$$

Logo o resultado decorre, pois :

$$a^p - b^p = (a-b)(a^{p-1} + ba^{p-2} + \cdots + b^{p-2}a + b^{p-1}$$

e ambos os fatores do lado direito são divisíveis por p.

□

4.3 Aritmética dos Restos

As propriedades das congruências podem facilitar muito o cálculo do resto de uma divisão de dois números inteiros. Deteminar o resto da divisão de 25 por 11 é muito simples. Imagine descobrir o resto da divisão de 25^{45} por 11 por exemplo?

Se não tivermos o conhecimento das propriedades acima citadas se torna uma tarefa exaustiva. Porém não o é, tendo estas ferramentas à mão.

Exemplo 14. Deteminar o resto da divisão de 25^{45} por 11.

Solução:

Como 11 é primo e $11 \nmid 25$, temos pelo Teorema de Fermat que:

$$25^{11} \equiv 25\, mod(11) \Rightarrow 25^{11} \equiv 3\, mod(11).$$

Pelo Colorário 3 temos:

$$25^{44} \equiv 4\, mod(11).$$

Da propriedade (iv) segue que:

$$25^{45} \equiv 100\, mod(11) \Rightarrow 25^{45} \equiv 1\, mod(11).$$

Portanto o resto da divisão é 1.

Exemplo 15. Prove que $2^{70} + 3^{70}$ é divisível por 13.

Solução:

Notemos que, $mdc(2, 13) = 1$, então pelo teorema de Fermat:

$$2^{12} \equiv 1\, mod(13).$$

Pelo Colorário 3 segue que:

$$2^{60} \equiv 1\, mod(13).$$

Temos também que:

$$2^4 \equiv 3\, mod(13).$$

Assim,

$$2^{60}.2^4.2^4.2^2 \equiv 1.3.3.4\, mod(13),$$

logo,

$$2^{70} \equiv 10\, mod(13) \tag{13}$$

Por outro lado ainda pelo teorema de Fermat:

$$3^{12} \equiv 1\, mod(13) \text{ e } 3^4 \equiv 243 \equiv 1\, mod(13).$$

Assim:$3^{60} \equiv 1\, mod(13)$.

Temos também que:

$$3^3 \equiv 1\, mod(13) \Rightarrow 3^9 \equiv 1\, mod(13).$$

Logo,

$$3^{60}.3^9.3 \equiv 1.1.3\, mod(13),$$

logo,

$$3^{70} \equiv 3\, mod(13). \tag{14}$$

Agora somando as equações (13) e (14) e usando as propriedade operatórias, concluímos que:

$$2^{70}+3^{70} \equiv 0\, mod(13).$$

Portanto $2^{70}+3^{70}$ é divisível por 13.

Determine o resto da divisão de $5^{85} + 7^{85} + 11^{85} + 25^{85}$ por 8.

Solução:

Observe que:

- $5 \equiv -3\, mod(8) \Rightarrow 5^{85} \equiv (-3)^{85}\, mod(8)$
- $7^{85} \equiv -1\, mod(8) \Rightarrow 7^{85} \equiv (-1)^{85}\, mod(8)$
- $11 \equiv 3\, mod(8) \Rightarrow 11^{85} \equiv 3^{85}\, mod(8)$
- $25 \equiv 1\, mod(8) \Rightarrow 25^{85} \equiv 1^{85}\, mod(8)$

Somando menbro a menbro as quatro congruências:

$$5^{85} + 7^{85} + 11^{85} + 25^{85} \equiv (-3)^{85} + (-1)^{85} + 3^{85} + 1^{85}\, mod(8).$$

Assim,

$$5^{85} + 7^{85} + 11^{85} + 25^{85} \equiv 0\, mod(8).$$

Portanto o resto da divisão é zero.

Exemplo 16. (Profmat-AV2 2014-Questão 1) Determine o resto da divisão do número $2222^{5555} + 5555^{2222}$ por 7.

Solução:

(1)Sendo: $2222 = 7 \cdot 317 + 3 \equiv 3\, mod(7)$, temos:

$$2222^{5555} \equiv 3^{5555}\, mod(7).$$

Análogamente: $5555 = 7 \cdot 793 + 4 \equiv 4\, mod(7)$, donde:

$$5555^{2222} \equiv 4^{2222}\, mod(7).$$

Obtemos assim:

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222}\, mod(7).$$

(2)Como $mdc(3, 7) = mdc(4, 7) = 1$, usando o Pequeno Teorema de Fermat segue que:

$$3^6 \equiv 1\, mod 7 \text{ e } 4^6 \equiv 1\, mod(7).$$

Escrevendo:

$$5555 = 6 \cdot 925 + 5 \text{ e } 2222 = 6 \cdot 370 + 2, \text{ teremos:}$$

$$3^{5555} + 4^{2222} = 3^{6 \cdot 925} \cdot 3^5 + 4^{6 \cdot 370} \cdot 4^2 \equiv 3^5 + 4^2\, mod 7.$$

Assim:

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \equiv 5 + 2 \equiv 0\, mod(7).$$

Portanto, o resto da divisão de $2222^{5555} + 5555^{2222}$ por 7 é zero.

Exemplo 17. (Profmat- AV2 2011-Questão 2) Ache o resto da divisão por 17 do número $S = 1^{16} + 2^{16} + 3^{16} + \cdots + 85^{16}$.

Solução:

Pelo Pequeno Teorema de Fermat temos que:

$$a^{16} \equiv \begin{cases} 1,\ se\, 17\, não\, divide\, a \\ 0,\ se\, 17\, divide\, a \end{cases} \quad mod(17)$$

Como $85 = 17 \cdot 5$, temos que de 1 a 85 há 5 múltiplos de 17 e $85-5 = 80$ não múltiplos de 17 (i.e., primos com 17).

Logo:

$$S \equiv 80 \cdot 1 \equiv 12\, mod(17).$$

Portanto, o resto da divisão de S por 17 é 12.

Exemplo 18. (Profmat-AV2 2012- Questão 2 (b)) Determine o resto da divisão por 7 do número $1^7 + 2^7 + 3^7 + \cdots + 100^7$.

Solução:

Usando o Pequeno Teorema de Fermat, vemos que:

$$a^7 \equiv a\, mod(7);\ a = 1, 2, 3, 4, 5, 6.$$

Além disso, se $n = 7k + a$, então:

$$n^7 = (7k + a)^7 \equiv a^7 \equiv a\, mod(7);\ a = 1, 2, 3, 4, 5, 6.$$

Desta forma:

$1^7 + 2^7 + 3^7 + \cdots + 100^7 \equiv (1+2+3+4+5+6+0) + \cdots + (1+2+3+4+5+6+0) + 1 + 2 = \frac{7 \cdot 6}{2} \cdot 14 + 3 = 21 \cdot 14 + 3 \equiv 3\, mod(7)$.

Portanto, o resto da divisão de $1^7 + 2^7 + 3^7 + \cdots + 100^7$ por 7 é 3.

Capítulo 5

Divisibilidade/Congruência-Outras Aplicações

Conceitos como divisibilidade e congruência são assuntos muito presentes no nosso dia-a-dia, porém divisibilidade se trabalha de maneira a memorizar conceitos e congruência não está presente nos currículos do fundamental II. No entanto, a proposta aqui apresentada visa mostrar algumas aplicações de forma interessante, estabelecendo relações entre divisibilidade/congruências e cotidiano, visto que por definição uma congruência é simplesmente a relação entre dois números que, divididos por um terceiro, chamado módulo, deixam o mesmo resto.

Apresentaremos neste capítulo algumas aplicações de divisibilidade e congruência modular além das já apresentadas em alguns dos capítulos anteriores. Dentre elas os Critérios clássicos de divisibilidade por 2, 3 e 11; Dígitos de verificação em códigos como: o de barras, *International Standard Book Number* **(ISBN)**, o Cadastro de Pessoas Físicas(CPF) e alguns problemas com Calendários.

Procuramos apresentar ao professor uma metodologia contextualizada e simples ao se abordar problemas que podem ser trabalhados com alunos do ensino fun-

damental II.

5.1 Critérios Clássicos de divisibilidade

Os "critérios de divisibilidade" é um conteúdo que faz parte do currículo escolar do ensino fundamentaldo. Entretanto são apresentados como um conjunto de regras a serem memorizadas e aplicadas de maneira direta. Estas regras são muito úteis na resolução de problemas. Mas de que maneira esses conceitos são transmitidos para os alunos? Será que os alunos foram instigados a elaborar esses conceitos? A atual metodologia prioriza o resultado imediato e deixa a desejar o desenvolvimento do pensamento analítico no aluno (SANT'ANNA. 2013).

Na realidade, grande parte dos professores antecipam conceitos, perdendo a ordem dos fatos e consequentemente argumentações para justificá-los perante as aluno. Isto muitas vezes gera, desconfiança e falta de estímulo.

Nosso objetivo nesta parte é apresentar alguns critérios de divisibilidade, formulados através de procedimentos de congruência modular, de tal forma a levar os alunos das séries finais do ensino fundamental a uma compreensão lógico dedutiva dos resultados e gerar especulações sobre outros critérios não apresentados.

Para estabelecer um critério de divisibilidade por m, a idéia é descobrir uma expressão mais simples em termos dos dígitos $a_n, a_{n-1}, a_{n-2}, \cdots, a_1, a_0$ à qual o polinômio é côngruo módulo m, e depois usar o fato de que se a e b são congruentes módulo m, o resto das divisões de a e b por m são os mesmos. Iniciaremos o critério com um exemplo númérico para depois escrevê-lo de forma generalizada.

5.2.1 Divisibilidade por 2

Utilizaremos neste e nos demais exemplos sobre critérios de divisibilidade a forma estendida da base 10 de um número e através de congruências módulo m, desenvolveremos todo o processo.

Exemplo 19. Verifique se 1987 e 25384 são divisíveis por 2.

Solução:

Notemos que 1987 se escreve na base 10 da seguinte forma:

$$1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 7.$$

Aplicando congruência modular teremos:

$$1987 \equiv 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10 + 7 \, mod(2)$$

Por outro lado sabemos que: $10 \equiv 0 \, mod(2)$.

Desse modo:

$$1987 \equiv 1 \cdot 0 + 9 \cdot 0 + 8 \cdot 0 + 7 \equiv 7 \, mod(2).$$

Como, $7 \equiv 1 \, mod(2)$, por transitividade, temos que o número $1987 \equiv 1 \, mod(2)$.

Logo 1987 não é divisível por 2.

Fazendo o mesmo processo para o número 25384 :

$$25384 \equiv 2.10^4 + 5.10^3 + 3.10^2 + 8.10 + 4 \, mod(2).$$

Logo,

$$25384 \equiv 4 \, mod(2) \text{ e } 4 \equiv 0 \, mod(2).$$

Assim:

$$25384 \equiv 0 mod(2).$$

Portanto 25384 é divisível por 2.

Para fazer a generalização do resultado acima consideremos como N um número natural dado. Sua forma estendida na base 10 é:

$$N = a_n a_{n-1} a_{n-2} a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0;\ n \in \mathbb{N}$$

Note que:

$$\begin{cases} 10 \equiv 0\, mod(2) \\ 10^2 \equiv 0\, mod(2) \\ 10^3 \equiv 0\, mod(2) \\ \vdots \\ 10^t \equiv 0\, mod(2) \end{cases}$$

Nosso objetivo é chegar no valor de N.

Multiplicando uma a uma as congruências acima, por $a_1, a_2, \cdots, a_n$, respectivamente, teremos:

$$\begin{cases} a_1 \cdot 10 \equiv 0\, mod(2) \\ a_2 \cdot 10^2 \equiv 0\, mod(2) \\ a_3 \cdot 10^3 \equiv 0\, mod(2) \\ \vdots \\ a_n \cdot 10^n \equiv 0\, mod(2) \end{cases}$$

Agora somando menbro a membro segue que:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 \equiv 0\, mod(2)$$

Das propriedades operatórias vem:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_0 \ mod(2).$$

Portato um dado número só é divisível por 2 se seu termo a_0 o é. Isso ocorre se a_0 for par.

Observação. A divisibilidade por 5 e por 10 decorrem no mesmo sentido.

5.2.2 Divisibilidade por 3

Exemplo 20. Verifique se os números 12564890 e 1235 são divisíveis por 3.

Solução:

Para o número 12564890 temos que:

$$12564890 \equiv (1.10^7 + 2 \cdot 10^6 + 5 \cdot 10^5 + 6 \cdot 10^4 + 4 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10 + 0) \, mod(3).$$

Como $10 \equiv 1 \, mod(3)$ e por consequência $10^n \equiv 1 \, mod(3)$, temos que:

$$12564890 \equiv (1 + 2 + 5 + 6 + 4 + 8 + 9 + 0) \, mod(3).$$

Logo,

$$12564890 \ \equiv \ 45 \, mod(3) \text{ e } 45 \ \equiv \ 0 \, mod(3).$$

Por transitividade tem-se que:

$$12564890 \equiv 0 \, mod(3).$$

Portanto 12564890 é divisível por 3.

Da mesma forma:

$$1235 \equiv (1.10^3 + 2.10^2 + 3.10 + 5)\, mod(3).$$

Logo,

$$1235 \equiv (1 + 2 + 3 + 5)\, mod(3).$$

Assim,

$$1235 \equiv\ 11\, mod(3) \text{ e } 11 \equiv 2\, mod(3),$$

que implica,

$$1235 \equiv 2\, mod(3).$$

Portanto 1235 não é divisível por 3.

O critério de divisibilidade por 3 é exatamente igual ao critério por 9, visto que o número 10 deixa o mesmo na divisão por ambos.

Assim como na generalização da divisibilidade por 2, consideremos:

$N = a_n a_{n-1} a_{n-2} a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0;\ n \in \mathbb{N}$

Sabemos que:

$$\begin{cases} 10 \equiv 1\, mod(3) \\ 10^2 \equiv 1\, mod(3) \\ 10^3 \equiv 1\, mod(3) \\ \vdots \\ 10^n \equiv 1\, mod(3) \end{cases}$$

Multiplicando $a_1, a_2, \cdots, a_n$ termo a termo por cada congruência e somando as mesmas, verificamos que:

$$\begin{cases} a_1 \cdot 10 \equiv a_1 \, mod(3) \\ a_2 \cdot 10^2 \equiv a_2 \, mod(3) \\ a_3 \cdot 10^3 \equiv a_3 \, mod(3) \\ \vdots \\ a_n \cdot 10^n \equiv a_n \, mod(3). \end{cases}$$

Logo,

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 \equiv a_n + a_{n-1} + \cdots + a_1 \ \ mod(3).$$

Adicionando o termo a_0 em ambos os lados da congruência teremos:

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \, mod(3).$$

Percebemos assim, que um número é divisivel por 3, se a soma de seus algarismos for um número divisível por 3.

5.2.3 Divisibilidade por 11

Exemplo 21. Verifique se o número 1327 é divisível por 11.

Solução:

Sabemos que:

$$1327 = 3 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 7.$$

Por congruência modular temos:

$$31327 \equiv 3 \cdot 10^4 + 1 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 7 \, mod(11).$$

Notemos ainda que:

$$\begin{cases} 10 \equiv -1\, mod(11) \\ 10^2 \equiv (-1)^2\, mod(11) \\ 10^3 \equiv (-1)^3\, mod(11) \\ 10^4 \equiv (-1)^4\, mod(11). \end{cases}$$

Assim,

$$\begin{cases} 10 \equiv -1\, mod(11) \\ 10^2 \equiv 1^2\, mod(11) \\ 10^3 \equiv -1\, mod(11) \\ 10^4 \equiv 1\, mod(11). \end{cases}$$

No entanto:

$$31327 \equiv 3 \cdot 1 + 1 \cdot (-1) + 3 \cdot 1 + 2 \cdot (-1) + 7\, mod(11).$$

Logo,

$$31327 \equiv 10\, mod(11).$$

Portanto, 31327 não é divisível por 11.

Para determinar a forma genérica de divisibilidade por 11, considere um natural dado tal que:

$$N = a_n a_{n-1} a_{n-2} a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0;\ n \in \mathbb{N}$$

e observando o fato de que:

$$\begin{cases} 10 \equiv -1\, mod(11) \\ 10^2 \equiv 1\, mod(11) \\ 10^3 \equiv -1\, mod(11) \\ \vdots \\ 10^n \equiv \begin{cases} 1\, mod(11); & n\, é\, par \\ -1\, mod(11); & n\, é\, ímpar \end{cases} \end{cases}$$

Novamente multiplicando por $a_1, a_2, \cdots, a_n$ simultaneamente em cada congruência e somando o termo a_0 teremos:

$$\begin{cases} a_1 \cdot 10 \equiv -1 \cdot a_1 mod(11) \\ a_2 \cdot 10^2 \equiv 1 \cdot a_2 mod(11) \\ a_3 \cdot 10^3 \equiv -1 \cdot a_3 mod(11) \\ \vdots \\ a_n \cdot 10^n \equiv \begin{cases} 1 \cdot a_n mod(11); & n\, é\, par \\ -1 \cdot a_n mod(11); & n\, é\, ímpar. \end{cases} \end{cases}$$

Logo,

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdots - a_1 + a_0 mod(11).$$

Portanto,

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + 10 \cdot a_1 + a_0 \equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdots - a_1 + a_0 mod(11).$$

Percebemos que sempre que há um algarismo de ordem par, este será positivo e o algarismo de ordem ímpar será negativo.

Portanto um número será divisível por 11 se a soma dos algarismos de ordem par, subtraída da soma dos algarismos de ordem ímpar, for um número divísivel por 11.

5.3 Dígitos de Verificação

Digitos de verificação (DV) são números que estão sempre presentes no nosso dia-a-dia em Códigos de barras, CPF, RG, Números de Contas Bancárias, entre outras sequências numéricas. Geralmente em uma sequência de números ele é o ultimo algarismo, exceto no caso do CPF que são dois dígitos de verificação. Eles servem para validar o código e evitar fraudes. Esse dígito pode variar de zero à nove ou ainda pode ser uma letra (no caso usam-se X) o que será explicado na sequência. A determinação do DV é uma aplicação de congruência modular, que pode facilmente ser compreendida e levada como apoio pedagógico para as aulas de matemática, logo nas séries iniciais do ensino fundamental II.

5.3.1 Código de Barras

Normalmente ao comprar algum produto percebemos uma marca presente denominada código de barras. A vantagem das barras é que elas podem ser identificadas rapidamente, e sem risco de erros, por aparelhos decodificadores portáteis de leitura óptica, como os usados pelos caixas de supermercados. Mas o que realmente importa para identificar o produto é sua sequência numérica, que também pode ser digitada manualmente pelos operadores de caixa. O código de barras funciona como uma espécie de RG do produto. Como não existem duas pessoas com o mesmo RG, não existem dois produtos diferentes com o mesmo código. O interessante disso tudo é que o Código de Barras é gerado por uma matemática pura e pode ser utilizado como ferramenta no ensino de alguns tópicos de matemática na sala de aula (ESQUINCA. 2013).

O código de barras *Universal Product Code* (UPC) ou *European Article Number* (EAN) nada mais é do que a representação gráfica da sequência de algarismos

que vem impressa logo abaixo das barras. Este é um conjunto de normas comercial. Originalmente criado nos Estados Unidos em 1973 pela empresa *Uniform Code Council*(UCC) para auxiliar os mercados a aumentar a velocidade do processo de verificação na saída de produtos e melhorar o controle de inventário. Mais tarde, constatou-se a eficiência desse tipo de código e sua utilização foi estendida rapidamente para o Brasil em 1983.

O Brasil deu um grande passo à frente de outros países da América Latina, aderindo ao sistema de código de barras na maioria das cidades e estados. Muitas empresas sentem a necessidade e a obrigação de adquiri-los quando a produção aumenta e quando os códigos de barras são exigidos pelos varejistas. Com isso, a demanda e a adesão aos códigos de barras no Brasil vem aumentando cada vez mais (PEREIRA DE SÁ. 2015). A EAN é a organização internacional que gerencia a distribuição dos códigos no mundo e tem uma representação no Brasil, porém existem várias formas de representar os códigos de barras nos diversos países. Enquanto os americanos usam uma sequência numérica de 12 dígitos (EAN–12), os europeus optaram por um padrão com 13 (EAN–13), que foi adotado no resto do mundo, inclusive no Brasil. Existem ainda outros tipos de códigos especiais, como o formado por 14 dígitos (EAN–14), usado em caixas de papelão para informar a quantidade de produtos guardados e o de 8 dígitos (EAN–8) utilizado quando a embalagem do produto é muito pequena.

Vejamos como exemplo a imagem de um código de barras do sistema mais comum e utilizado no Brasil, o EAN-13, que usa 13 algarismos para cada produto:

Figure 3: Código de barras
Fonte:http://www.proteste.org.br/familia/nc/noticia/entenda-o-codigo-de-barras

As duplas de barras mais compridas são uma sinalização, fazem separação indicando que a seguir vem o código do produto. As barras e seus respectivos algarismos não ficam alinhados, porisso o número 7 vem antes das barras de sinalização.

Os três primeiros números (789) é o registro nacional, que indicam que o produto foi cadastrado no Brasil, apesar de não, necessariamente, ter sido fabricado aqui. Cada país tem uma combinação própria. A da Argentina, por exemplo, é 779.

A segunda sequência de números (8357) que pode variar de quatro a sete algarismos é a identificação da empresa fabricante (RG do fabricante). Esse número é fornecido pela EAN, que faz o controle para que não sejam distribuídos números iguais.

A terceira sequência (41001) identifica o produto em si. A numeração varia conforme o tipo, o tamanho, a quantidade, o peso e a embalagem do produto – um refrigerante em lata, por exemplo, tem uma sequência diferente de um em garrafa.

O último número (5) é um dígito verificador. Ao ler todo o código do produto, o computador faz um cálculo simples:

- Efetua ordenadamente da esquerda para a direita o produto de cada algarismo por 1 e 3 de forma alternada;
- A partir da soma desses produtos, calcula-se o resto da divisão pelo número 10;
- O resto encontrado será o DV do produto.

Se a leitura estiver correta, o resultado desse cálculo é igual ao do dígito verificador. O interessante para nós é que esse dígito verificador nada mais é do que uma simples aplicação de congruência modular.

Observe o cálculo detalhado do procedimento descrito anteriormente para a figura 3.

A sequência dos 12 primeiros dígitos do código é 789835741001 que matemáticamente pode ser escrita na forma: $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}$. Devemos multiplicá-los, nessa ordem, pela base $\{1,3,1,3,1,3,1,3,1,3,1,3\}$ e somar os produtos obtidos. Essa soma acrescida do algarismo a_{13} deve ser um múltiplo de 10, ou seja, o algarismo procurado é obtido da seguinte relação de congruência:

$$1\cdot a_1+3a_2+1a_3+3a_4+1a_5+3a_6+1a_7+3a8+1a_9+3a_{10}+1a_{11}+3a_{12}+a_{13} \equiv 0\, mod(10).$$

Efetuando os produtos do códigos de barras pela base de multiplicação teremos:

$$1\cdot 7+3\cdot 8+1\cdot 9+3\cdot 8+1\cdot 3+3\cdot 5+1\cdot 7+3\cdot 4+1\cdot 1+3\cdot 0+1\cdot 0+3\cdot 1+a_{13} \equiv 0\, mod(10).$$

Assim,

$$7+24+9+24+3+15+7+12+1+0+0+3+a_{13} \equiv 0\, mod(10).$$

Então,

$$105 + a_{13} \equiv 0\, mod 10\ .$$

Somando (-105) a ambos os lados da congruência segue que:

$$a_{13} \equiv -105\, mod(10).$$

Logo,

$$a_{13} \equiv 5\, mod(10).$$

Portanto o DV correspondente ao código de barras apresentado é 5, o qual se completa conforme a fig. 3.

5.3.2 International Standard Book Number (ISBN)

O Sistema ISBN (*International Standard Book Number*) foi criado em 1969 e assim como o código de barras, é um sistema de identificação numérica, mas, de livros,

CD-Roms e publicações em braile. Antigamente as editoras identificavam seus livros com um número da forma $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ de 10 dígitos, onde os primeiros 9 algarismos eram divididos em 3 seções de comprimento variável para identificar o livro e o algarismo a_{10} seria o dígito verificador (PEREIRA DE SÁ. 2015). A partir de 1 de Janeiro de 2007, devido ao crescente número de publicações, com suas respectivas edições e formatos, este sistema sofreu uma mudança , passando a ter 13 dígitos, no intuito de aumentar sua capacidade, . A nova númeração foi precedida pelo número 978, que identifica o produto e ainda foi recalculado o número de controle. O novo formato de numeração foi adotado para padronizar a quantidade de dígitos de acordo com o seu equivalente de 13 dígitos no código de barras. Quando o "prefixo 978" se esgotar, será adotado o "prefixo 979", que resultará em nova mudança de prefixo editorial para os Editores.

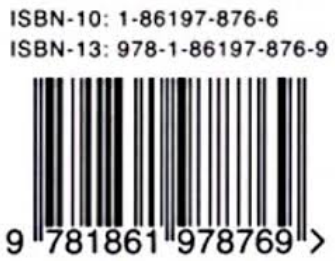

Figure 4: ISBN I
Fonte:http://quezi.com/wp-content/uploads/2009/01/2175016522_ecbf98c8b4_o.jpg

No novo sistema ISBN-13, tem-se que a distribuiçao dos códigos se apresentam da seguinte forma: a primeira seção de algarismos identifica o livro, a segunda o país ou um agrupamento geográfico de editoras, a terceira seção uma empresa editora particular desse grupo, a quarta o título do livro dentro do catálogo da empresa editora e o último dígito é o de verificação, que serve para validar a existência do produto.

Figure 5: ISBN II

Novamente usaremos a congruência módulo m para resolver esta situação.

Voltando ao exemplo da figura 4 para o sistema ISBN-10 podemos verificar o dígito teste da seguinte maneira:

- Determinamos o resto da divisão por 11 tomando a base 10, tal que os números $\{10, 9, 8, 7, 6, 5, 4, 3, 2, 1\}$, nesta ordem sejam multiplicados termo a termo com com os algarismos apresentados pelo sistema da esquerda para a direita;
- Efetuamos a soma dos 9 primeiros produtos;
- A diferença entre o que falta para o próximo múltiplo de 11 é o número procurado(termo a_{10}), ou seja, efetuando a seguinte congruência:

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + 1a_{10} \equiv 0\, mod(11)$$

Observação. a_{10} é substituído por X caso a congruência deixe resto 10.

Assim, no caso em questão o dígito de controle (6) é determinando efetuando o seguinte cálculo:

$$10 \cdot 1 + 9 \cdot 8 + 8 \cdot 6 + 7 \cdot 1 + 6 \cdot 9 + 5 \cdot 7 + 4 \cdot 8 + 3 \cdot 7 + 2 \cdot 6 + a_{10} \equiv 0 mod(11),$$

que é equivalente a:

$$291 + a_{10} \equiv 0 \; mod(11),$$

logo,

$$a_{10} \equiv -291 \, mod(11).$$

Portanto,

$$a_{10} \equiv -5 \, mod(11) \;\; \Rightarrow a_{10} = 6$$

Um problema que acontece frequentemente gerando erro nas edições é o fato de aparecer um dígito errado ou a troca de dígitos adjacentes. A única garantia é que esses dois erros sempre serão detectados, de acordo com o método de cálculo de verificação de dígito do ISBN. Não sendo detectado o livro será editado com ISBN inválido.

Para o cálculo do dígito de verificação do ISBN-13 o procedimento ocorre de maneira análoga ao código de barras usual. Um zero(0) substitui dez (10), garantindo assim, que o resultado da verificação não é maior que um dígito. Por exemplo, o dígito de verificação para o ISBN-13 da figura 4 será calculado da seguinte maneira:

$$1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 + 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12+}a_{13} \equiv 0 \, mod(10),$$

Logo,

$$1 \cdot 9 + 3 \cdot 7 + 1 \cdot 8 + 3 \cdot 1 + 1 \cdot 8 + 3 \cdot 6 + 1 \cdot 1 + 3 \cdot 9 + 1 \cdot 7 + 3 \cdot 8 + 1 \cdot 7 + 3 \cdot 6 + a_{13} \equiv 0 \, mod(10),$$

que é equivalente a,

$$a_{13} + (9 + 21 + 8 + 3 + 8 + 18 + 1 + 27 + 7 + 24 + 7 + 18) \equiv 0 \, mod(10).$$

Assim

$$a_{13} + 151 \equiv 0 \, mod(10),$$

o que implica em:

$$a_{13} \equiv -151 \, mod(10).$$

Daí obtemos que:

$$a_{13} \equiv -1 \, mod(10).$$

Somando 1 a ambos os lados da congruência teremos:

$$a_{13} + 1 \equiv 0 \, mod(10) \Rightarrow a_{13} = 9$$

Portanto, $a_{13} = 9$.

Contudo este sistema de verificação, similar ao utilizado para a verificação do Código Universal de Produtos (UPC), não detecta todos os erros de transposição(mudança de posição) adjacente, especificamente, se a diferença entre ambos for igual a 5. Um exemplo é se ocorrer que sejam estes dígitos 6 e 1 . A ordem correta contribui $3 \cdot 6 + 1 \cdot 1 = 19$ para a soma, enquanto que, se os dígitos são transpostos (1 seguido por 1) , a contribuição dos dois dígitos para a soma será $3 \cdot 1 + 1 \cdot 6 = 9$. Como, 19 e 9 são congruentes módulo 10, produzirão o mesmo resultado final para os ISBN's. A fórmula do ISBN-10 usa o módulo 11, que é primo, o que evita esse problema, mas requer mais do que um dígito para expressar o dígito de verificação o que no caso ocorrendo substitui-se por X. Além disso, se triplicar a soma das $2^{\underline{a}}, 4^{\underline{a}}, 6^{\underline{a}}, 8^{\underline{a}}, 10^{\underline{a}}$ e $12^{\underline{a}}$ posições e em seguida as adicionar aos restantes dígitos ($1^{\underline{o}}, 3^{\underline{o}}, 5^{\underline{o}}, 7^{\underline{o}}, 9^{\underline{o}}, 11^{\underline{o}} e 13^{\underline{o}}$), o total será sempre ser divisível por 10 (ou seja termina em 0).

Esse Digito Verificador também é utilizado em documentos pessoais como: CPF, RG, CNPJ, Título de Eleitor, etc. Os processos utilizados para o cálculo desses dígitos podem, nesses casos, variar de um documento para outro de forma distinta, dependendo muitas vezes da região ou órgão expedidor, exceto no caso do Cadastro de Pessoas Físicas (CPF) que segue um padrão em todo território nacional e será destacado na sequência.

5.3.3 Cadastro de Pessoas Físicas(CPF)

O CPF é outro exemplo importante, do nosso cotidiano. Este número é

constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois. Estes, assim como no ISBN e nos códigos de barra, são os dígitos de controle, que servem para garantir a autenticidade do documento. A determinação desses dois dígitos de controle pode ser feita utilizando congruência modular.

A diferênça entre o CPF e os códigos de barras são que estes aqui tratados possuem o DV munido de dois algarismos, tal que o primeiro deles é o resultado de uma congruência módulo 11, obtido por uma operação dos nove primeiros, e o segundo é determinado incluindo-se o dígito encontrado e resolvendo novamente outra congruência módulo 11.

Suponhamos um CPF com os nove primeiros dígitos sendo 002007571. Primeiramente lembremos que todo CPF possui um número da forma:

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9 - a_{10}a_{11}.$$

Para obter o primeiro dígito verificador devemos:

- Multiplicar da esquerda para direita os nove primeiros algarismos do CPF, pelos 9 números$\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$,nesta ordem;
- Somar os produtos obtidos;
- O dígito a_{10}, ser subtraído da soma obtida gerando um múltiplo de 11.

Observe o cálculo:

Como,

$$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 - a_{10} \equiv 0\, mod(11),$$

então:

$$1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 \equiv a_{10}\, mod(11).$$

Aplicando a propriedade simétrica teremos:

$$a_{10\equiv}(1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9)\, mod(11).$$

Desse modo:

$$a_{10} \equiv (1 \cdot 0 + 2 \cdot 0 + 3 \cdot 2 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 7 + 7 \cdot 5 + 8 \cdot 7 + 9.1)\, mod(11),$$

logo,

$$a_{10} \equiv 148\, mod\,(11).$$

Assim,

$$a_{10} \equiv 5\, mod\,(11).$$

Portanto, $a_{10} \equiv 5\, mod(11)$

A determinação do segundo dígito verificador é feita de maneira similar módulo 11. No entanto, acrescentamos o dígito encontrado anteriormente estendendo agora a base de multiplicação para 10 algarismos, a começar do zero.

Assim teremos:

$$0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10} - a_{11} \equiv 0\, mod(11).$$

Logo,

$$(0 \cdot 0 + 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 7 + 6 \cdot 5 + 7 \cdot 7 + 8 \cdot 1 + 9 \cdot 1) - a_{11} \equiv 0\, mod(11).$$

Assim:

$$0 \cdot 0 + 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 7 + 6 \cdot 5 + 7 \cdot 7 + 8 \cdot 1 + 9 \cdot 1 \equiv a_{11}\, mod(11).$$

Portanto, $171 \equiv a_{11}\, mod(11)$.

Aplicando a propriedade simétrica:

$$a_{11} \equiv 171\, mod(11) \Rightarrow a_{11} \equiv 6\, mod(11)$$

Logo, o segundo dígito de controle é 6 e portanto concluímos que o CPF completo será:

00200757156

5.4 O Calendário

Há centenas de anos o homem se preocupa em registrar de forma empírica o passar do tempo. O dia e o ano, por exemplo, podem ser observados por qualquer pessoa, já que suas definições se baseiam em considerações astronômicas. No entanto, as definições de semana e mês são muito dependentes da cultura de cada povo ao longo da história.

Para a contagem do tempo desenvolveu-se o calendário, que é um sistema de contagem e agrupamento de dias, que visa atender principalmente às necessidades civis e religiosas de uma cultura, organizadas com o propósito de medir e registrar eventos ao longo de "grandes períodos" (PEREIRA DE SÁ. 2015).

Na atualidade existem aproximadamente 40 Calendários em uso no mundo, que podem ser classificados em três tipos:

- **Solares**: Baseados no movimento da Terra em torno do Sol; os meses não têm conexão com o movimento da Lua. (exemplo: Calendário Cristão e Gregoriano);
- **Lunares**: Baseados no movimento da Lua; o ano não tem conexão com o movimento da Terra em torno do Sol. (exemplo: Calendário Islâmico). Os meses de um Calendário Lunar, como o Islâmico, sistematicamente vão se afastando dos meses de um Calendário Solar, como o nosso;
- **Lunisolares***:* Os anos estão relacionados com o movimento da Terra em torno do Sol e os meses com o movimento da Lua em torno da Terra. O Calendário Hebreu possui uma seqüência de meses baseada nas fases da Lua, mas de tempos em tempos um mês inteiro é intercalado para o Calendário se manter em fase com o ano tropical.

Nos calendários solares, que são os mais utilizados, a unidade básica para a contagem do tempo é o dia, este que possui por sua vez 24 horas, divididas em duas etapas, que são intercaladas entre o nascer e o pôr do sol. O ano solar, também conhecido como ano trópico, é o período de tempo decorrido para completar um ciclo de estações (primavera, verão, outono e inverno), tendo a duração de aproximadamente 365 dias, 5 horas, 48 minutos e 47 segundos (365,2422 dias). Assim por excesso a cada quatro anos, as horas extra acumuladas são reunidas no dia 29 de Fevereiro, formando o ano bissexto, ou seja, o ano com 366 dias (BRASIL. 2009).

No Brasil utilizamos o Calendário Gregoriano, que deriva do calendário solar. Os anos são formados por meses constituídos por 30 ou 31 dias; com exceção de fevereiro constituído por 29 dias nos anos bissextos e 28 nos demais anos. No Calendário Gregoriano, existem 97 anos de 366 dias (que chamamos de bissextos) em cada período de 400 anos. Os anos bissextos são determinados pela seguinte regra (BRASIL. 2009):

- Todo ano bissexto é divisível por 4;
- II- Todo ano divisível por 4, exceto os centenários não divisíveis por 400, é bissexto;

Um exemplo pra melhor entender os critérios acima é comparar os anos 1900 e 2000. O primeiro não foi bissexto pois 1900 não é um número divisível por 400, o que já acontece com o ano de 2000.

Percebendo que há um grande envolto matemático ao se tratar de calendários, uma vez que é dividido de forma periódica e sequêncial, por dias, semanas, meses e anos, apareceram em vários programas de televisão pessoas que dizem apresentar "habilidades especiais" para memorizar dias da semana de anos anteriores. Será que realmente são habilidades especias ou facilidade em utilizar algoritmos?

Provavelmente a segunda resposta seria mais conveniente ao chamarmos de verdade. O calendário possui alguns elementos arbitrários onde podemos usar algoritmos com operações básicas de matemática para relacionar uma data estabelecida ao dia da semana em que ela se deu (OLIVEIRA. 2015). O procedimento envolvido nesses algoritmos é acessível para qualquer pessoa que saiba usar as quatro operações básicas. O desafio, na verdade, é criar uma sequência de passos que direcionem o exercício mental. Saber criar e lidar com algoritmos é interessante e pode ser útil no mundo informatizado de hoje.

Observemos também a relação de uma simples congruência modular com o calendário, referente ao mês de setembro de 2014.

Figura 6: Calendário 2014
Fonte: http://arterocha.blogspot.com.br/2013/11/calendario-mes-de-setembro-2014.html

Notemos que ao analisar a disposição dos dias no mês de setembro em relação a congruência modulo m teremos:

- Domingo- $n \equiv 0 \, mod(7)$;
- Segunda - $n \equiv 1 \, mod(7)$;
- Terça- $n \equiv 2 \, mod(7)$;

- Quarta-$n \equiv 3\, mod(7)$;
- Quinta-$n \equiv 4\, mod(7)$;
- Sexta - $n \equiv 5\, mod(7)$;
- Sábado-$n \equiv 6\, mod(7)$.

Se quisermos, por exemplo, determinar em qual dia da semana será 27 de setembro de 2014, sem olhar no calendário , bastaria apenas sabermos a que classe de congruencia, este pertenceria, módulo 7. Assim dividindo 27 por 7, resultaria quociente 3 e resto 6. Desse modo teriamos que $27 \equiv 6\, mod(7)$, ou seja, tomando segunda-feira como dia 1(data inicial do mês) , a classe de restos 6 pertenceria nesta sequência aos sábados. Logo dia 27 é sabado(verifique figura 5.5.1).

O fato mais interessante nesta parte da aritmética é que ela nos permite ainda verificar dias da semana de datas muito anteriores aos dias atuais. A história registra seus fatos, basicamente, pelas datas. Para entender como funciona tal procedimeto faremos alguns exemplos retirados da video aula 37 do professor Fabio Henrique Teixeira de Souza[3], direcionada aos alunos da OBMEP e que trata de problemas com calendários.

Exemplo 22. O ano de 2013, começou em uma terça-feira. Qual o dia da semana termina o ano?

Solução:

Primeiramente devemos observar que aqui é um caso geral onde o respectivo ano possui 365 dias, agrupados de 7 em 7 dias, que são as semanas. Neste caso ao dividir 365

[3] (Disponivel em: https://www.youtube.com/watch?v=Gj5uopyMoKc)

por 7, obteremos 52 ciclos semanais completos e sobrará um dia. Sendo que cada ciclo inicia-se na terça-feira e termina na segunda, devemos acrescentar 1 dia ao próximo ciclo. Assim sendo o último dia do ano será também uma terça-feira. Observe o cálculo:

$$365 \equiv a\, mod(7), \text{ onde } a \text{ é o resto.}$$

Portanto,

$$365 \equiv 1\, mod(7).$$

Observação. Em geral, exceto os anos bissextos, todos os anos começam e terminam no mesmo dia da semana.

A figura a seguir se trata da imagem de um calendário do ano de 2013. Faremos alguns exemplos para que possamos mostrar ao aluno que tendo apenas um ponto de partida, ou seja, uma data inicial, conseguimos determinar qualquer outra.

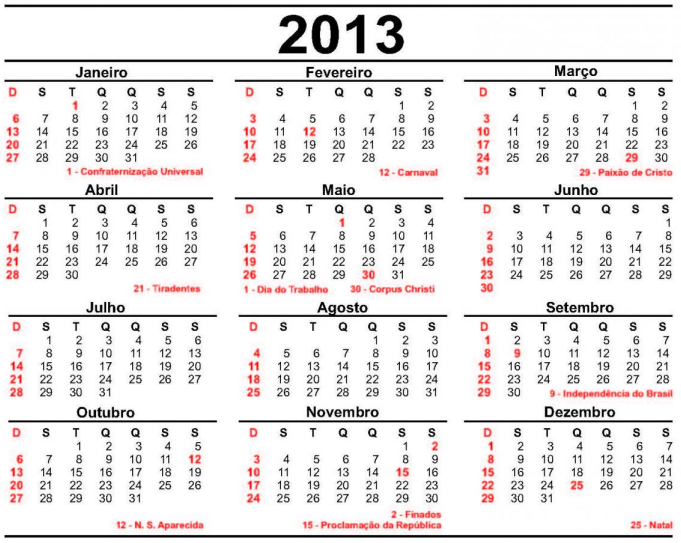

Figura 7: Calendário 2013
Fonte:http://www.tatendoaqui.com/wp-content/uploads/2013/01/calendario-2013.jpg

Exemplo 23. Sabendo que o 2013 começou em terça-feira, qual dia da semana será 1^{o} de janeiro de 2016?

Solução:

Como entre 2013 e 1^{o} de janeiro de 2016 não há nenhum ano bissexto, então, podemos raciocinar da seguinte maneira:

- 2013 começa e termina em uma terça-feira;
- 2014 começa e termina em uma quarta-feira;
- 2015 começa e termina em uma quinta-feira.

Então 1^{o} de janeiro de 2016 será uma sexta-feira.

Exemplo 24. Sabendo que o 2013 começou em terça-feira, qual dia da semana será 31^{o} de dezembro de 2016?

Solução:

Neste caso devemos levar em consideração que 2016 é um ano bissexto, visto ser um número divisível por 4 e não terminado em 00. Assim não podemos dizer que terminou no mesmo dia da semana, pois agora o mês de fevereiro possui 29 dias. Poderiamos pela informação do exemplo 23 acrescentar 1 dia o que nos forneceria domingo. Caso não tivessemos esses dados, procederíamos da seguinte maneira:

- 2013, 2015 e 2015(365 dias)
- 2016(366 dias)

Então,

$$365 + 365 + 365 + 366 \equiv a\, mod(7).$$

Logo,

$$1461 \equiv a\, mod(7).$$

Portanto, se o ciclo se inicia na terça-feira acrescetando 5 unidades a este ciclo teremos que o ultimo dia de 2016 será um sábado.

Contudo podemos dado uma data qualquer como ponto de partida, determinar qualquer outra anterior ou posterior a ela.

CURIOSIDADES:

- Os anos terminados em 00 que não são divisíveis por 400, não são bissextos devido as chamadas de excessões seculares , fato que ocorre em função do tempo que Terra leva para dar a volta em torno do Sol que é estimado (em aproximadamente 365 dias, 5 horas, 48 minutos e 46 segundos) e não exato, tal que essa pequena diferença de menos de 12 minutos poderia provocar erros a cada cerca de 100 a 120 anos. Contudo a diferença de 46 segundos pode provocar novas revisões no calendáriono no ano 3000. Porém os astrônomos têm corrigido os relógios mundiais em 1 segundo em algumas passagens de ano, o que poderá dispensar tal revisão.
- Existem 14 formatos diferentes para o calendário que usamos. Sete deles formados com inicio e fim no mesmo dia da semana(seg-seg), ou seja para anos não bissextos, e os outros 7 com início em um determinado dia e fim em um dia posterior da semana(ex: seg-ter)

Capítulo 6

Considerações Finais

Através da proposta apresentada, percebemos que nós professores, devemos ter muito cuidado ao transmitir conhecimentos para nossos alunos, levando em consideração o fato de que um aluno desistimulado gera muito desconforto e insegurança na sala de aula. Trabalhar o conceito de divisibilidade e suas propriedades é fundamental para que o professor tenha firmeza ao apresentar temas onde se faz uso destes. Não há relevância alguma em trabalhar regras por memorização. Devemos construir todo um processo, onde o aluno tenha um espaço para desenvolver seu raciocínio lógico matemático de forma justificada, contextualizada e agradável.

Ao introduzir o conceitos de Equações Diofantinas Lineares estamos proporcionando a nossos alunos, uma ferramenta para que eles possam modelar uma situação cotidiana transformando-a numa linguagem matemática. Além disso, o professor estará saindo do básico, que é abordado por livros didáticos e partindo para o uma metodologia onde o aluno, através do uso destes conceitos possa solucionar problemas e compreender conceitos pré-estabelecidos.

Podemos concluir também, que existem muitas aplicações em que a aritmética modular age de forma essencial e simples. Vários desses usos podem ser encontrados durante o percorrer do dia e suas aplicações podem variar de forma muito interessante, seja para critérios de divisibilidades, códigos de identificação, calendários, entre outros. Essas aplicações podem servir de metodologia estimulante no trabalho com alunos de várias faixas etárias.

É importante que os critérios de divisibilidade sejam apresentados de forma generalizada, para que o professor tenha ferramentas que possam justificar regras pré -estabelecidadas e assim deixar o fato de o aluno não ficar se perguntando de onde apareceu este conceito e assim desacreditar da matemática.

Ao se trabalhar com aplicações no calendário através de problemas básicos o aluno sentirá curiosidade em descobrir datas passadas e futuras e isso levará a uma concentração maior. Essa concentração de maneira muito suave instigará o aluno, e o professor, poderá posteriormente criar generalizações e aprofundar o conhecimento dentro do tema.

Mesmo não sendo parte do currículo escolar em nenhum momento, a Congruência Modular e suas relações podem ser trabalhadas de forma eficaz, pois permitem ao aluno a capacidade de visualizar propriedades ligadas a divisibilidade e potenciação, fazendo correlações entre elas para determinar restos de números grandes, sem o trauma de efetuar um cálculo exaustivo. Contudo, por estar tratando de assuntos cotidianos, gera maior interesse e concentração ao momento das atividades propostas.

Acredita-se que este trabalho seja referência pelo qual o professor possa fazer uso, tendo em vista que sua linguagem é simples e atualizada e pode ser aplicada logo no início do ensino fundamental II, e posteriormente melhorada nas séries finais desta fase para que num momento futuro, o aluno já familiarizado com estes conceitos, possa sentir-se seguro em trabalhar com congruências um pouco mais complexas, caso

professores de outros níveis de ensino o queiram fazer.

São inúmeras as aplicações de divisibilidade e congruência, além de serem muito amplas. É impossível exibir todas em um trabalho como este. Desse modo, deixo como sugestão para professores comprometidos com a educação, uma possível pesquisa na área de Criptografia. Este tema também é muito relevante e pode ser trabalhado a partir do $6^{\underline{o}}$ ano e até em um nível superior, sem perda de mérito, pois além de se trabalhar a matemática pura que há na formação dos conceitos, levará o aluno a ter conhecimento de sua definição e importância em vários campos que utilizam métodos extensos e complexos.

Referências Bibliográficas

[1] BARBOSA, José Hélio Júnior. Congruências Modulares: Construindo um conceito e as susa aplicações no ensino médio. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT)- São Cristovão- SE.2013

[2] BOYER, Carl B. História da Matemática. Tradução: Elza F. Gomide.2ª Edição. São Paulo. Edgard Blücher, 2003.

[3] BRASIL. Ministério da Educação. Secretária de Educação Fundamental. Parâmetros curriculares nacionais: terceiro e quarto ciclos do ensino fundamental: introdução aos parâmetros curriculares nacionais. Secretaria de Educação Fundamental Brasília: MEC/ SEF, 1998.

[4] BRASIL. Ministério da Educação. Secretaria de Educação a Distância.A matemática dos Calendários. Guia do professor. FNDE. Unicamp.2009.

[5] ESQUINCA, Josiane Colombo Pedrini. Aritmética: código de barras e outra aplicações de congruência. Dissertação (Mestrado Profissional em Matemática em Rede Nacional PROFMAT)- Instituto de Ciência exatas e tecnologia.Campo Grande- MS. 2013.

[6] GROENWALD, Claudia Lisete Oliveira; FRANKE, Rosvita Fuelber; OLGIN,Clarissa de Assis. Códigos e Senhas no Ensino Básico. Educação Matemática em Revista(Passwords in Basic Education)- RS. Ano 10.Volume 2. 2009.

[7] HEFEZ, Abramo.Aritmética. 1ª Edição. Rio de Janeiro: SBM,2013.

[8] LORENSATTI, Edi Jussara Candido. Aritmética: um pouco de história. Disponível em:<http://www.portalanpedsul.com.br/admin/uploads/2012/Ensino de Matematica e ciências>. Acesso em: 05 de dez.2015.

[9] MERTINES, Fabio E. B; MOREIRA, Carlos G. T.A; SALDANHA, Nicolau C, "et. al". Teoria dos Números: um passeio com primos e outros números familiares

pelo mundo inteiro.2013.Disponível em: <http://www.livrariavirtual.impa.br.> Acesso em : 30/01/2016.

[10] MIYASCHITA, Wagner Yuwamamoto. Sistemas de Númeração: Como funcionam e como são estruturados os números.Universidade Estadual Paulista– UNESP.Bauru-SP. 2002.

[11] MOURA, Rafael nogueira de.Congruências Modulares e Algumas aplicações para a Educação Básica. Dissertação (Mestrado Profissional em Matemática em Rede Nacional PROFMAT)- Centro de Ciências e Tecnologia. Fortaleza- CE. 2015.

[12] PEREIRA DE SÁ, I. A aritmética modular e suas aplicações no cotidiano. Disponível em : <www.magiadamatematica.com> Acesso em: 05 dEZ. 2015

[13] RODRIGUES, Jaqueline de Moraes. Criptografia e conteúdos de matemática no ensino fundamental.2013. Dissertação(Mestrado Profissional em Matemática em Rede Nacional PROFMAT)- Centro de Ciências exatas e de tecnologia- Departamento de Matemática, São Carlos. 2013.

[14] SANT'ANNA, I. K. A aritmética modular como ferramenta para as séries finais do ensino fundamental. Dissertação (Mestrado Profissional em Matemática em Rede Nacional PROFMAT) - Instituto de Matemática Pura e Aplicada, Rio de Janeiro. 2013.

[15] SAUTOY, Marcus du. A Música dos Números Primos: a história de um problema não resolvido na matemática. Tradução: Diego Alfaro. Rio de Janeiro. Ed.Jorge Zahar. 2007.

[16] SILVA, , Viviane Azevedo da. FRIEDMANN, Clicia Valladares Peixoto. Congruência Módulo M e a Aritmética Modular: conceitos, resultados e aplicações. Escola de Educação, Ciências, Letras, Artes e Humanidades, UNIGRANRIO - Rio de Janeiro. 2011.

[17] SOUZA, Leticia Vasconcellos de. Congruência modular nas séries finais do ensino fundamental-Dissertação (Mestrado Profissional em Matemática em Rede Nacional PROFMAT). Instituto de Ciência exatas.Juiz de Fora.2015.