UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

OS NÚMEROS NO NOSSO DIA A DIA E ALGUMAS DE SUAS APLICAÇÕES NO ENSINO BÁSICO

LUIZ CARLOS CONRADO MENDES

MANAUS
2015

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

LUIZ CARLOS CONRADO MENDES

OS NÚMEROS NO NOSSO DIA A DIA E ALGUMAS DE SUAS APLICAÇÕES NO ENSINO BÁSICO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Roberto Antonio Cordeiro Prata

MANAUS
2015

LUIZ CARLOS CONRADO MENDES

OS NÚMEROS NO NOSSO DIA A DIA E ALGUMAS DE SUAS APLICAÇÕES NO ENSINO BÁSICO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito para obtenção do título de Mestre em Matemática

Aprovado em 04 de fevereiro de 2015.

BANCA EXAMINADORA

Prof. Dr. Roberto Antonio Cordeiro Prata
Presidente

Prof. Dr. Nilomar Vieira de Oliveira
Membro

Profa. Dra. Jeanne Moreira de Sousa
Membro

AGRADECIMENTOS

Primeiro a Deus por tudo que fez em minha vida.

A minha mãe, Senhora Osmarina Sampaio Mendes, por criar sozinha seus seis filhos, a minha eterna gratidão por tudo que tem feito por mim. A toda a minha família, pela dedicação, amor, apoio e incentivo que sempre estiveram presentes.

Em especial aos professores Dr. Roberto Antonio Cordeiro Prata e Dr. Nilomar Vieira de Oliveira, por suas competências, dedicações e confianças no desenvolvimento dessa dissertação.

A todos meus professores da Universidade Federal do Amazonas e do Mestrado Profissional em Matemática, por me ensinarem e acreditarem na minha capacidade de aprender.

Enfim, a todos os meus amigos do PROFMAT pelo companheirismo nas árduas vitórias conquistadas e todas as pessoas que, direta ou indiretamente, contribuíram para a execução dessa Dissertação de Mestrado.

RESUMO

A presente dissertação tem como objetivo principal apresentar a alunos e professores de matemática do ensino básico algumas resoluções de problemas no campo da aritmética que pode beneficiar o processo ensino-aprendizagem. Serão abordados inicialmente a divisibilidade, com suas propriedades e seus critérios, após apresentação da divisão euclidiana e suas aplicações no ensino básico. Além disso, será apresentado um breve embasamento teórico, pautado no conceito e nas propriedades operacionais da congruência modular com suas classes residuais, seguido de suas aplicações. No final, será feito um breve histórico dos números nos calendários.

Palavras-chave: Matemática, Ensino Básico, Aritmética, Congruência Modular, Ensino-Aprendizagem, Divisibilidade, Aplicações, Calendários.

ABSTRACT

This paper aims to introduce students and teachers of basic mathematical education some resolutions of problems in the field of arithmetic which can benefit the teaching-learning process. Initially, it will be addressed the divisibility with their properties and criteria. This is done after a presentation of Euclidean division and its applications in basic education. Moreover, it will be presented a brief theoretical background based on the concept and the operational properties of modular congruence with their residue classes, followed by their applications. Finally, it will be presented a brief history of the numbers in the calendars.

Keywords: Mathematics, Teaching Basic Arithmetic, Congruence Modular, Teaching and Learning, Divisibility, Euclidean Division, Applications, Calendars.

Sumário

Introdução

A vida do ser humano é cercada por números. Do momento em que acordamos e durante todo o dia os números estão presentes, nas horas, nos minutos e segundos. Até mesmo quando fazemos uma compra, os produtos, no comércio, assim como os alimentos e vários outros objetos, estão representados por números que são chamados de códigos de barras. No dinheiro e nos cartões de créditos ou débitos, na carteira de identidade, na certidão de nascimento, no CPF e muitos outros, tudo são formados por números.

Como já dizia Pitágoras, segundo Singh [11]:

"Todas as coisas são números".

Dessa forma, justifica-se a realização desta dissertação, pois os números estão presentes no nosso dia a dia e queremos saber como eles aparecem, como são formados e algumas de suas diversas aplicações. O conhecimento de como os números influenciam o nosso dia-a-dia, pode ajudar em uma melhor compreensão da sua importância e utilização, principalmente por parte dos alunos do Ensino Básico.

No primeiro capítulo é feito um breve histórico da Aritmética na Magna Grécia. Primeiramente com Tales de Mileto que introduziu o estudo da Aritmética na Grécia, em seguida, Pitágoras de Samos, que fundou a escola pitagórica, adotou a Aritmética como um fundamento filosófico. Depois, Platão exerceu uma forte influência na ciência dos números. Em seguida, Euclides surgiu com o tratado de treze livros, chamado de *Os Elementos de Euclides*, que versam sobre a teoria dos números e geometria, com conceitos, definições e teoremas, em particular, também temos nessa obra a divulgação da divisão euclidiana, a qual chamamos de divisão com resto. E no final deste capítulo, relatamos o trabalho de Diofanto de Alexandria, considerado como o pai da Álgebra, com uma coleção de livros de 6 volumes, sendo conhecido como *"Arithmetica"*, uma obra com 130 problemas algébricos.

No capítulo 2 abordamos a divisibilidade, sua definição, suas propriedades e os principais critérios de divisibilidade e, no final, é feito a demonstração do Teorema da Divisão Euclidiana e suas aplicações para o ensino básico.

No capítulo 3, é feito um breve histórico sobre congruência modular. Leonard Euler que é um dos maiores matemáticos de todos os tempos introduziu a ideia de *Congruência Módulo um número natural* e Gauss, sendo considerado como o *Príncipe da Matemática*,

desenvolveu a Aritmética Modular em seu livro *Disquisitiones Arithmeticae.* Depois, a congruência modular é apresentada com sua definição, proposições, teorema e a retomada dos principais critérios de divisibilidade através da congruência modular. E por fim, as classes residuais com sua definição e as suas principais propriedades

No capítulo 4 mostraremos diversas aplicações para o ensino básico no nosso dia-a-dia, que formam fenômenos periódicos, nos relógio analógico, nos códigos do sistema de identificação: ISBN, CPF, CNPJ, no código de barras que aparecem nas mercadorias de diversos produtos e na criptografia com seus códigos secretos.

E por fim mostraremos o capítulo 5 com o título de "Os Números nos Calendários". Pretendemos neste capítulo, fazer um breve histórico nos calendários, depois mostraremos o calendário gregoriano, adotado por vários países, como foi feito e como surgiu, mostrando os anos normais de 365 dias e o anos bissexto de 366 dias.

Capítulo 1

A Aritmética na Magna Grécia

1.1 Tales, Pitágoras e Platão

Tales de Mileto[1], começou sua vida como mercador e com essa atividade tornou-se rico o bastante para dedicar-se até o final de sua vida ao estudo e viagens de conhecimento. Há informações não comprovadas que ele viveu por algum tempo no Egito e ficou admirado com a beleza e o tamanho das pirâmides, a partir daí calculou a altura de uma pirâmide por meio de sua sombra.

De volta a Mileto, ganhou uma boa reputação, graças ao seu gênio versátil de estadista, conselheiro, engenheiro, homem de negócios, filósofo, matemático e astrônomo. Com o passar do tempo abandonou os negócios e a vida pública para dedicar-se inteiramente a Filosofia, a Astronomia e a Matemática. Foi considerado o primeiro Matemático Grego a introduzir o estudo da Matemática na Grécia, trazendo dos sacerdotes Egípcios, os rudimentos da *Aritmética* e da *Geometria*, dando uma característica que se conserva até hoje, com o conceito de "demonstração ou prova". Foi considerado um dos sete sábios mais importante da antiguidade (EVES, 2004, p.94-96) [14].

Outro matemático, Pitágoras [2] aos 18 anos, dominava muitos conceitos matemáticos e filosóficos de seu tempo, recebeu muita influência científica e filosófica de Tales e de outros filósofos, segundo Eves [5]. Em uma visita ao Egito, impressionando-se com as Pirâmides, desenvolveu o Teorema de Pitágoras que já era conhecido na Grécia a 2000 a.C. Durante os vinte anos de suas viagens, chegou a assimilar os conhecimentos matemáticos conhecidos até então. De volta para sua terra natal, a ilha de Samos, fundou a famosa Escola Pitagórica que permaneceu em atividade durante vários séculos, os pitagóricos atribuíam

[1]Tales de Mileto, Cidade da Ásia Menor, Grécia - Nasceu por volta de 645 ou 624 a.C em Mileto e provavelmente morreu em 558 a.C ou 556 a.C, não comprovado historicamente, em Mileto, - Matemático, Astrônomo e Filósofo, fundou a mais antiga escola filosófica - Jônica. Disponível em: http://www.educ.fc.ul.pt/icm/icm99/icm28/tales.htm

[2]Pitágoras de Samos, Grécia - Nasceu por volta de 571 a.C ou 570 a.C em Samos, no mar Egeu, na região da Ásia Menor e morreu em Metaponto, sul da Itália, entre 497 a.C ou 496 a.C - Matemático e Filósofo Grego.

aos números um poder místico e adotavam como fundamento de seu sistema filosófico.

Singh, Simon[3], assim descreve[11]:

> [...] Como não existem relatos originais de sua vida e de seus trabalhos, Pitágoras está envolto no mito e na lenda, tornando difícil separar o fato da ficção. O que parece certo é que Pitágoras desenvolveu a ideia da lógica numérica e foi responsável pela primeira idade de ouro da matemática. Graças ao seu gênio, os números deixaram de ser apenas coisas usadas meramente para calcular e passaram a ser apreciados por suas próprias características.[...] (p.28).
> [...] Depois da morte de Pitágoras de Samos, a ideia da demonstração matemática se espalhou rapidamente pelo mundo civilizado. Dois séculos depois do incêndio de sua escola, o centro do estudo da matemática tinha se mudado de Crotona para a cidade de Alexandria. No ano 332 a.C, depois de conquistar a Grécia , a Ásia Menor e o Egito, Alexandre, o Grande, decidiu construir uma capital que seria uma cidade mais imponente do mundo.[...] (p.64).

Quase nada sobrou dos escritos originais dessa fase da matemática grega, chegando apenas referências e comentários feitos por outros matemáticos posteriores.

O filósofo Platão[4] exerceu uma forte influência na matemática, sua preferência pelos aspectos teóricos e conceituais o fazia estabelecer uma clara diferenciação entre a Ciências dos Números, que é a Aritmética, e a arte de calcular (cálculo é uma palavra oriunda do latim "calculus", que significa "pedra que serve para contar"), que é a logística, de acordo com Hefez [7].

Platão elaborou um livro de 10 volumes, chamado de *A República*, segundo Maria Helena da Rocha Pereira [10]. No livro VII, discutiu a importância da aritmética, da geometria, da astrologia e da harmonia; admitindo que sem o conhecimento do cálculo e da aritmética, a verdade não poderá ser alcançada. Segundo Platão:

"O aprendizado do cálculo, deve acontecer pela contemplação da natureza dos números exclusivamente pelo pensamento. A experiência, assim, gera conhecimento" .

[3]SINGH,Simon tradução por Calife, Jorge Luiz - O Último Teorema de Fermat - 13ª ed. - Rio de Janeiro: Record, 2008.

[4]Platão(palavra que se utilizava para homens de ombros largos) - Nasceu em 427 a.C em Atenas e provavelmente morreu em 348 a.C - Filósofo Grego.

1.2 Euclides e Diofanto

Euclides [5] foi um dos primeiros geômetras e é reconhecido como um dos matemáticos mais importante da Grécia e de todos os tempos. De acordo com Hefez: "A contribuição de Euclides à matemática foi considerável, tendo sido o primeiro matemático a apresentar a geometria e a aritmética como ciências dedutivas". Pouco se sabe de sua vida. Foi convidado para ensinar matemática na escola criada pelo rei Ptolomeu I, em Alexandria, conhecida por "museu". Euclides não criou muitos resultados, mas estabeleceu um padrão de apresentação e rigor na matemática, servindo como exemplo aos seus seguidores durante milênios, segundo Hefez [6]. Por volta de 300 a.C, em Alexandria, ele surge com um tratado de treze livros, *Os Elementos de Euclides* que em grego significa *"Stoikheia"* [15].

Singh [11], assim expressa:

> [...] Somente quando Alexandre morreu e Ptolomeu I subiu ao trono no Egito é que Alexandria se tornou o lar da primeira Universidade do Mundo. Matemáticos e outros intelectuais emigraram para a cidade e, embora eles fossem certamente atraídos pela reputação da universidade, a atração principal era a biblioteca de Alexandria.[...]
> [...] O sonho de Ptolomeu, de criar uma casa do conhecimento, sobreviveu até a sua morte. Depois de sua morte, outros Ptolomeus ascenderam ao trono do Egito, a Biblioteca continha cerca de 600 mil livros. Os matemáticos podiam absorver todo o conhecimento do mundo estudando em Alexandria. E lá, para ensiná-los, estavam os mais famosos professores. O primeiro diretor do departamento de matemática foi ninguém menos do que Euclides.[..]
> [...] Os Elementos de Euclides é o livro-texto mais produzido e estudado na história do mundo ocidental, o mais bem sucedido até este século, trata-se do segundo maior best seller mundial, depois da Bíblia.[...] (p.64-65)

"Os Elementos"[6] têm uma importância excepcional na Matemática. Partindo de definições, axiomas e postulados, com regras lógicas bem determinadas, admitidas sem demonstrações e as proposições e os teoremas aparecem expostos numa ordem perfeita com demonstrações rigorosas. Em particular, Euclides explorou uma lógica muito conhecida nos dias atuais como *reductio ad absurdum*, segundo Hefez[5], ou prova por contradição. Dos livros de *"Os Elementos"*, dez versam sobre geometria e três (livros: VII, VIII e IX), sobre a Teoria dos Números Naturais. Sempre com uma visão geométrica, os números representavam os segmentos de reta e os números ao quadrado representavam as áreas das figuras geométricas. No livro VII, que é o início da aritmética de Euclides, são definidos os conceitos de divisibilidade, dos números primos etc.

[5] Euclides (330 a.C - 260 a.C) - Nasceu na Síria e estudou em Atenas - Matemático.

[6] É recomendável a leitura de *Os Elementos de Euclides*, de Pitombeira, J.B., RPM, Vol 5, N.1, 1994.

Encontra-se neste mesmo livro a divisão com resto, que denominamos *Divisão Euclidiana*. *Os Elementos de Euclides* foram a base do ensino nas escolas e universidades durante dois mil anos, segundo Carvalho [1].

O último herói da tradicional matemática grega, foi Diofanto de Alexandria [16], matemático e filósofo grego, que tem seu nome ligado a cidade que foi o maior centro de atividade matemática na Grécia Antiga. Foi considerado por muitos estudiosos como *"Pai da Álgebra"*. É o mais conhecido pelos seus livros "Arithmetica" (Diophanti, Alexandrini - Arithmeticorum), que foi escrita em treze volumes, sendo que existem apenas seis dos livros originais, uma obra contendo 130 problemas algébricos. Trata-se do primeiro livro totalmente algébrico, sem nenhuma interpretação geométrica, segundo Hefez[7].

Pouco se sabe acerca de sua vida, presume-se que tenha nascido por volta do ano de 250 d.C., por uns versos encontrados no túmulo, escritos em forma de um enigmático problema, aparentemente criado por um amigo, Metrodorus, o enigma é o seguinte: "Aqui jaz o matemático que passou um sexto da sua vida como menino. Um doze avos da sua vida passou como rapaz. Depois, viveu um sétimo da sua vida antes de casar. Cinco anos após nasceu seu filho, com quem conviveu metade de sua vida. Depois da morte de seu filho, sofreu mais quatro anos antes de morrer", acredita-se que viveu 84 anos[17].

Capítulo 2

Divisibilidade e Divisão Euclidiana

2.1 Divisibilidade e suas propriedades

O uso de divisibilidade é muito comum no Ensino Básico, sua definição e propriedades enriquecem o entendimento dos números de nosso dia-a-dia.

Considera-se nesta dissertação o símbolo $\mathbb{Z}$ que representa os conjuntos dos números inteiros, $\mathbb{N}$ os conjuntos do números naturais e $\mathbb{N}^*$ os conjuntos do números naturais excluindo o zero, considere também as operações de multiplicação ($\cdot$), adição ($+$) e subtração (-). As notações que serão apresentadas tem como referenciais teóricos Hefez [7], Zuckerman [13] e Domingues [4].

Definição 2.1.1. *Um número $a \in \mathbb{Z}^*$ divide o número $b \in \mathbb{Z}$, se escreve $a \mid b$, se existe um número $c \in \mathbb{Z}$ tal que $b = a \cdot c$*

Se a divide b diremos que b é múltiplo de a.
Se a não divide b usaremos a notação $a \nmid b$.

Exemplo 2.1.1.

i) $2 \mid 10$ *pois* $10 = 2 \cdot 5$*;*

ii) $-2 \mid 10$ *pois* $10 = (-2) \cdot (-5)$.

É muito importante a aplicação da divisibilidade nas séries iniciais, no quarto e quinto ano do Ensino Fundamental, porém deve ser utilizado logo após o aluno ter aprendido as quatro operações: adição, subtração, multiplicação e divisão dos Números Naturais. Esta definição pode ser estendida para os números inteiros positivos e negativos. No sexto e sétimo anos do Ensino Fundamental, os alunos terão um melhor entendimento com os Números Inteiros.

Principais Propriedades de Divisibilidade

Proposição 2.1.1.

Sejam os números $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. Temos que:

i) $1 \mid c, \quad a \mid a \quad$ e $\quad a \mid 0$.

ii) se $a \mid b \quad$ e $\quad b \mid c, \quad$ então $\quad a \mid c$

Demonstração 2.1.1.

i) Na definição representada acima, temos:

$$c = 1 \cdot c, \quad a = a \cdot 1 \quad \text{e} \quad 0 = a \cdot 0$$

ii) Existem x, $y \in \mathbb{N}$, tais que: $b = a \cdot x$ e $c = b \cdot y$

Substituindo o valor de b da primeira equação na segunda equação, obtemos:

$c = b \cdot y = (a \cdot x) \cdot y = a \cdot (x \cdot y)$, sendo $a \mid c$

■

A conclusão do item (i) é que todo número natural diferente de zero é divisível por 1 e por si mesmo, temos assim a propriedade reflexiva. E do item (ii) temos a propriedade transitiva.

Exemplo 2.1.2.

i) $2 \mid 0$ pois $0 = 2 \cdot 0$; $\quad 5 \mid 5$ pois $5 = 5 \cdot 1$; $\quad 1 \mid 8$ pois $8 = 1 \cdot 8$.

ii) $3 \mid 15$ e $15 \mid 45$, logo $3 \mid 45$.

Proposição 2.1.2.

Se a, $c \in \mathbb{N}^*$, b, $d \in \mathbb{N}$, e $\quad a \mid b$, $c \mid d$, então $(a \cdot c) \mid (b \cdot d)$

Demonstração 2.1.2.

Se $a \mid b$, e $c \mid d$, então existem x, $y \in \mathbb{N}$, tais que $b = a \cdot x$ e $d = c \cdot y$. Portanto,

$$b \cdot d = (a \cdot x) \cdot (c \cdot y) = (a \cdot c) \cdot (x \cdot y).$$

Pela definição da divisibilidade, concluímos que $(a \cdot c) \mid (b \cdot d)$

■

Exemplo 2.1.3.

$4 \mid 12$ e $5 \mid 10 \Longrightarrow 4 \cdot 5 \mid 12 \cdot 10 \Longrightarrow 20 \mid 120$.

Proposição 2.1.3.

Se $a \in \mathbb{N}^*$ e $b, c \in \mathbb{N}$. Então:

i) Quando $a \mid (b + c)$, temos $a \mid b \quad \Longrightarrow \quad a \mid c$

ii) Quando $a \mid (b - c)$ sendo $b \geq c$, temos $a \mid b \quad \Longrightarrow \quad a \mid c$

Demonstração 2.1.3.

i) Pela hipótese, temos que $a \mid (b + c)$, logo existe um $x \in \mathbb{N}$, tal que

$$b + c = x \cdot a$$

Se $a \mid b$, existe um $y \in \mathbb{N}$ tal que

$$b = a \cdot y$$

Juntando as duas equações acima, temos:

$$a \cdot y + c = x \cdot a \quad \Longrightarrow \quad c = x \cdot a - y \cdot a$$

Como $c \in \mathbb{N}$, logo $c > 0$

$$a \cdot x - a \cdot y = a \cdot (x - y) > 0$$

portanto,

$$c = (x - y) \cdot a \quad \Longrightarrow \quad a \mid c$$

■

ii) Pela hipótese, temos que $a \mid (b - c)$, sendo $b \geq c$,
logo existe um $x \in \mathbb{N}$, tal que

$$b - c = x \cdot a$$

Se $a \mid b$, existe um $y \in \mathbb{N}$ tal que

$$b = a \cdot y$$

Juntando as duas equações acima, temos:

$$a \cdot y - c = x \cdot a \quad \Longrightarrow \quad c = y \cdot a - x \cdot a$$

Como $c \in \mathbb{N}$, logo $c > 0$

$$a \cdot y - a \cdot x = a \cdot (y - x) > 0,$$

Portanto,

$$c = (y - x) \cdot a \qquad \Longrightarrow \qquad a \mid c$$

■

Exemplo 2.1.4.

i) Se $7 \mid (84 + 56)$ e $7 \mid 140$. Então, $7 \mid 84 \iff 7 \mid 56$

ii) Se $7 \mid (84 - 56)$ e $7 \mid 28$. Então, $7 \mid 84 \iff 7 \mid 56$

Proposição 2.1.4.

Sejam $a \in \mathbb{N}$ e $b \in \mathbb{N}$, tais que $a \mid b$ e $b \mid a$, então $a = b$

Demonstração 2.1.4.

Da hipótese $a \mid b$ *e* $b \mid a$, *existem* $x, y \in \mathbb{N}$, *tais que:*

$$b = x \cdot a$$

e

$$a = y \cdot b$$

substituindo a 2^a *equação na* 1^a *equação, temos:*

$$b = x \cdot y \cdot b$$

.

i) Se $b = 0$, *qualquer que sejam* $x, y \in \mathbb{N} \Rightarrow a = 0$.

ii) Se $b \neq 0 \Rightarrow x \cdot y = 1$, *logo* $x = y = 1$ *e portanto* $b = 1 \cdot a$.

Conclusão: $a = b$.

■

Provamos assim, que a proposição 2.1.4 é anti-simétrica.

2.2 Critérios de Divisibilidade.

Um número é divisível por outro quando o resto da divisão entre eles é igual a zero [8].

Regras de Divisibilidade

i) Divisibilidades por 1

Todo número é divisível por 1.

Exemplo 2.2.1.

$\frac{12}{1} = 12; \quad \frac{8}{1} = 8$ e $\frac{26}{1} = 26.$

ii) Divisibilidades por 2

Dado o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0.$$

Observe que toda potência de $10^n = (2 \cdot 5)^n$ é divisível por 2, então,

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

$$= a_n(2q_n) + a_{n-1}(2q_{n-1}) + ... + a_1(2q_1) + a_0$$

$$= a_0 + 2(a_n q_n + a_{n-1} q_{n-1} + ... + a_1 q_1),\ q_i \in \mathbb{N}, i = \{1, 2, 3, ..., n\}$$

ou seja,

$$a = a_0 + 2m,\ m \in \mathbb{N}$$

e

$$m = a_n q_n + a_{n-1} q_{n-1} + ... + a_1 q_1,$$

como $2m$ é divisível por 2,

então, a é divisível por 2 se, e somente se, a_0 é divisível por 2.

Portanto, $a_0 \in \{0, 2, 4, 6, 8\}$.

Assim, todo número terminado em 0, 2, 4, 6 e 8, isto é, os números pares são divisíveis por 2.

Exemplo 2.2.2.

$\frac{12}{2} = 6; \quad \frac{8}{2} = 4$ e $\frac{26}{2} = 13.$

iii) Divisibilidades por 3 **e** 9

Dado o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal, temos:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0.$$

Observe que o resto da divisão de 10^n, $n \geq 0$ por 3 e por 9 é sempre igual a 1,isto é, dividindo 10 por 3, temos, $10 = 3 \cdot 3 + 1$ e o resto é 1 e dividindo 10 por 9, temos, $10 = 1 \cdot 9 + 1$ e o resto é 1.

Então,

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

$$a = a_n (3 \cdot 3 + 1)^n + a_{n-1} (3 \cdot 3 + 1)^{n-1} + ... + a_1 (3 \cdot 3 + 1)^1 + a_0$$

$$a = [a_n (3 \cdot 3)^n + a_{n-1} (3 \cdot 3)^{n-1} + ... + a_1 (3 \cdot 3)^1] + [a_n .1 + a_{n-1} .1 + ... + a_1 .1 + a_0]$$

como

$$a_n (3 \cdot 3)^n + a_{n-1} (3 \cdot 3)^{n-1} + ... + a_1 (3 \cdot 3)^1$$

é divisível por 3 ou por 9. Assim, para que o número

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

seja divisível por 3 ou por 9, temos que a soma:

$$= a_n .1 + a_{n-1} .1 + ... + a_1 .1 + a_0,$$

seja divisível por 3 ou por 9. Logo o número

$$a = a_n a_{n-1} a_{n-2} ... a_1 a_0$$

é divisível por 3 ou por 9, se, e somente se,

$$a_n + a_{n-1} + ... + a_1 + a_0$$

é divisível por 3 ou por 9.

Portanto, um número é divisível por 3 ou por 9 quando a soma dos seus algarismos é um número divisível por 3 ou por 9.

Exemplo 2.2.3.

Verificar se o número 7095 é divisível por 3.

A soma dos algarismos do número 7095 é $7+0+9+5=21$, é divisível por 3.

Portanto, o número 7095 é divisível por 3

Exemplo 2.2.4.

Verificar se o número 27495 é divisível por 9.

A soma dos algarismos do número 27495 é $2+7+4+9+5=27$, é divisível por 9.
Portanto, o número 27495 é divisível por 9

v) Divisibilidades por 5 **e por** 10

Dado o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal, temos:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0.$$

Observe que toda potência de $10^n = (2 \cdot 5)^n$ é divisível por 5 e por 10. Então,

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 = a_0 + 10(a_n q_n + a_{n-1} q_{n-1} + ... + a_1 q_1),$$

ou seja, $a = a_0 + 10q,\ q \in \mathbb{N}$, como $10q$ é divisível por 5 e por 10, então, a é divisível por 5 se, e somente se, a_0 é divisível por 5, logo, $a_0 = 0$ ou $a_0 = 5$. Por outro lado, a é divisível por 10 se, e somente se, a_0 é divisível por 10, logo, $a_0 = 0$.

Assim, todo número é divisível por 5 quando terminam em 0 ou em 5 e é divisível por 10 quando terminam em 0 .

Exemplo 2.2.5.

i) $\dfrac{205}{5} = 41;\quad \dfrac{800}{5} = 160$ e $\dfrac{155}{5} = 31.$

ii) $\dfrac{200}{10} = 20;\quad \dfrac{1800}{10} = 180$ e $\dfrac{15560}{10} = 1556.$

Existem outros critérios de divisibilidade[19], resultante da combinação entre os números apresentados, por exemplo o número 15, para que um número seja divisível por 15 ele tem que ser ao mesmo tempo divisível por 3 e por 5. Com isso, os alunos do Ensino Fundamental poderão encontrar com mais facilidades outros critérios de divisibilidade. Estes critérios de Divisibilidade envolvendo congruência modular serão apresentadas no **capítulo 3**.

2.3 Divisão Euclidiana e suas Aplicações

Segundo Hefez [7] [...] *" Mesmo que um número natural a não divide o número natural b, Euclides, nos seus Elementos, utiliza, sem enunciá-lo explicitamente, o fato de que é sempre possível efetuar a divisão de b por a, com resto.* [...]" (p.35)

Apresentaremos a seguir o Teorema da Divisão Euclidiana, com exemplos e algumas de suas aplicações.

Teorema 2.3.1. (Teorema da Divisão Euclidiana) [7]. Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais $q \in \mathbb{N}$ e $r \in \mathbb{N}$, q é o quociente e r é o resto, de modo que $b = a \cdot q + r$, com $r < a$.

Demonstração 2.3.1.

Suponha que $b > a$ e considere, enquanto fizer sentido, nos números naturais

$$b,\ \ b-a,\ \ b-2a,\ \ \ldots\ \ , b-n\cdot a,\ \ \ldots.$$

O conjunto X formado pelos elementos acima destacados é um subconjunto dos números naturais, diferente de vazio, pois $b \in X$, por exemplo, segue pelo princípio da boa ordem [9]

"Todo subconjunto não vazio do conjunto dos números naturais possui um menor elemento."

Logo, o conjunto X formado pelos elementos acima, isto é,

$$X = \{x \in \mathbb{N};\ x = b - aq,\ q \in \mathbb{N}\}$$

tem um menor elemento $r = b - q \cdot a$

i) Vamos demonstrar que $r < a$.

Se $a \mid b$, então $r = 0$ e nada mais temos a provar.
Se $a \nmid b$, então $r \neq a$, portanto, basta mostrar que não pode ocorrer $r > a$.

De fato, se isso ocorresse, existiria um número natural $c < r$ tal que $r = c + a$.

Como $r = c + a = b - q \cdot a$, teríamos: $c = b - (q+1) \cdot a \in X$, com $c < r$, e isto é uma contradição pois r é o menor elemento de X.

Portanto, temos que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

ii) Vamos demonstrar a unicidade.

Dados dois elementos distintos de X, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a.

Logo, se $r = b - a \cdot q \quad$ e $\quad r' = b - a \cdot q'$, com $r < r' < a$, teríamos $r' - r \geq a$, o que acarretaria $r' \geq r + a \geq a$, absurdo.

Portanto, $r = r'$.

Daí segue-se que: $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$.

Logo, $q = q'$.

Conclusão, r e q são únicos tais que $b = a \cdot q + r$, com $0 \leq r < a$. ■

Os livros de matemática do 3º ano do Ensino Fundamental expõe o algoritmo da divisão euclidiana (Dividendo = Divisor · quociente + resto), veja figura 2.1, da seguinte maneira:

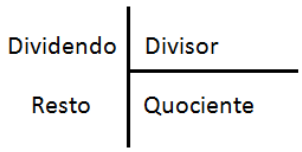

Figura 2.1: algoritmo da divisão euclidiana.

Mostraremos alguns exemplos que serão úteis em suas Aplicações no Ensino Fundamental, segundo Iezzi [8], relacionados com os números de nosso dia a dia.

Exemplo 2.3.1.

Determinar o quociente e o resto da divisão de 45 por 6.

Sejam D dividendo, d divisor, q quociente e r resto, D, d, q, $r \in \mathbb{N}$, pela divisão euclidiana, temos: $D = d \cdot q + r$, com $r < d$, então:

$$45 = 6 \cdot 7 + 3$$

Exemplo 2.3.2.

Em 28650 dias, calcule:

i) O número de anos, considerando um ano igual a 365 dias.

ii) O número de meses, considerando um mês igual a 30 dias.

Resolução:

i) $28655 = 365 \cdot 78 + 185$

Logo, 28650 corresponde a 78 anos e *sobram*(resto) 185 dias.

ii) $28655 = 30 \cdot 955 + 5$

Logo, 28655 corresponde a 955 meses e *sobram*(resto) 5 dias.

Exemplo 2.3.3.

Determinar quantos múltiplos de 7 existem entre 1 e 200?

Pelo algoritmo da divisão euclidiana, temos que

$$200 = 7 \cdot 28 + 4,$$

portanto são 28 múltiplos de 7.

Capítulo 3

Congruência Modular

3.1 Um Pouco de História da Congruência Modular

Leonard Euler[1] foi provavelmente o maior matemático de todos os tempos, escreveu mais de quinhentos livros e artigos sobre os mais diversos assuntos de Matemática, trabalhou durante 25 anos na academia de Berlim e produziu cerca de 300 trabalhos científicos. Ele foi o pioneiro na abordagem de congruência, por volta de 1750, introduziu a ideia de *congruência módulo um número natural*.

Carl Friedrich Gauss [2], foi considerado como "*o príncipe da matemática* (princeps mathematicorum)", desenvolveu a aritmética modular (aritmética dos restos), em seu livro *Disquisitiones Arithmeticae - Indagações Aritméticas*, publicado em 1801, no qual reúne as ideias que desenvolveu desde os 17 anos de idade. Observou com muita frequência frases do tipo "*a dá o mesmo resto de b quando divididos por m*", que chamamos de "*congruência*", introduziu uma notação matemática abordando o assunto com simbologia e definições utilizadas até hoje. Ele demonstrou o *Teorema Fundamental da Álgebra*, definiu o conceito de *Números Complexos*, bem como sua representação geométrica, formulou a chamada *Lei de Gauss*, conforme Eves[5].

3.2 A Aritmética Modular

É de grande importância aplicar na Teoria dos Números a Aritmética Modular, que é um sistema de aritmética para números inteiros, onde os números "voltam para trás" quando atingem certo valor, que chamamos de Módulo [18].

No dia-a-dia, aparecem números que se repetem a intervalos regulares, estes números são chamados de fenômenos periódicos, a Terra leva 24 horas para dar uma volta em torno de si mesma, sendo o seu período de rotação 24 horas.

[1]Euler, Leonhard Paul - (1707-1783) - nascido na Basiléia, Suiça - Matemático e Físico Suíço.
[2]Gauss, Johann Carl Friedrich - (1777-1855) - Matemático, Astrônomo e Físico Alemão.

Exemplo 3.2.1.

Suponha que hoje é dia 6 de novembro de 2013, quarta-feira, um aluno do ensino fundamental, pergunta ao seu professor de matemática se no dia 24 de novembro de 2013 haverá aula de matemática.

O professor, mostra matematicamente, sem olhar o calendário. Como hoje é quarta-feira 6 de novembro e $24 - 6 = 18$, faltam 18 dias para o dia 24 de novembro. Por outro lado, pelo algoritmo da divisão euclidiana, temos $18 = 2 \cdot 7 + 4$, passado $2 \cdot 7 = 14$ dias, é uma quarta-feira e a 4 dias desta quarta é um **domingo**.

Portanto não haverá aula neste dia.

No Exemplo 3.2.1 foi utilizado divisão de números inteiros com resto, o resto se comporta de maneira periódica. Os múltiplos de 2 se repetem de dois em dois. Os múltiplos de 3 se repetem de três em três. Os múltiplos de 5 se repetem de cinco em cinco. Os múltiplos de 7 se repetem de sete em sete.

Dividindo os números inteiros de 0 em diante por 7, obtêm-se os restos como na tabela de divisão por 7 3.3.

Inteiros	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Restos	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4

Tabela 3.1: Restos da divisão por 7 dos números naturais

Os restos dos inteiros sucessivos na divisão por n inteiro qualquer, se repetem com período n.

Generalizando:

Dados dois números inteiros n e d, com $d \neq 0$, efetuando a divisão de n por d obtêm dois inteiros q e r tais que $n = d \cdot q + r$ e $0 \leq r < |d|$, sendo os números n, d, q e r, nesta ordem, o dividendo, o divisor, o quociente e o resto. [3]

"Os Períodos Generalizados" no exemplo, dias da semana, 7 dias, são chamados de ***Módulos*** e envolvem ***Conceito de Congruência Modular***.

3.3 Conceito de Congruência

Congruência modular foi publicado em muitos livros de matemática principalmente nos que tratam sobre Teoria dos Números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros. O que não é muito comum e pouco utilizado em sala de aula são as aplicações no cotidiano de todas as pessoas. Este assunto, pode ser trabalhado já nas classes do Ensino Fundamental e Médio, é um gerador de excelentes oportunidades de contextualização no processo de ensino-aprendizagem de matemática.

Definição 3.3.1.

Seja m um inteiro positivo. Dois números inteiros a e b são congruentes módulo m se tiverem os mesmos restos na divisão euclidiana por m.

$$\textbf{Notação: } \boldsymbol{a \equiv b} \textbf{ (mod } m\textbf{)}$$

Quando a não é congruente a b, módulo m, é chamado de incongruente.

$$\textbf{Notação: } \boldsymbol{a \not\equiv b} \textbf{ (mod } m\textbf{)}$$

Observação 3.3.1.

Dizemos que $a \equiv b \pmod 1$, qualquer que sejam os valores de a, $b \in \mathbb{N}$, pois o resto da divisão de qualquer número por 1 é sempre zero. veja a regra de divisibilidade por 1, na secção**(2.2)**.

Exemplo 3.3.1.

O número 12 é congruente ao número 7, módulo 5. Pois 12 e 7 deixam o mesmo resto da divisão por 5 que é o número 2, veja figura 3.1, representamos esta congruência por:

$$\boldsymbol{12 \equiv 7} \textbf{ (mod } 5\textbf{)}$$

Figura 3.1: divisão euclidiana.

Exemplo 3.3.2.

O número 47 não é congruente ao número 15, módulo 6. Pois, 47 deixa resto 5 na divisão por 6 e 15 deixa resto 3 na divisão por 6, representamos esta incongruência por:

$$\boldsymbol{47 \not\equiv 15} \textbf{ (mod } 6\textbf{)}$$

3.4 Propriedades de Congruência Modular

O conhecimento das proposições nas congruências modulares, como uma relação de equivalência, são importantes nas suas aplicações dos números de nosso dia a dia, segundo Hefez[7].

Proposição 3.4.1.

Suponha que $a,\ b,\ m \in \mathbb{N}$, sendo $a \geq b$ e $m > 1$. Tem-se $a \equiv b \pmod{m}$ se, e somente se, $m \mid (a - b)$

Demonstração 3.4.1.

($\Rightarrow$)
Sejam $m,\ a,\ b,\ q_1,\ q_2$ e r números naturais.

Pela divisão euclidiana[3], temos que:

$$a = m \cdot q_1 + r,\ se\ r < m. \tag{3.1}$$

$$b = m \cdot q_2 + r,\ se\ r < m. \tag{3.2}$$

a e b são os dividendos, m o divisor, q_1 e q_2 os quocientes e r o resto.
Subtraindo (3.3) com (3.4), tem-se:

$a - b = (m \cdot q_1 + r) - (m \cdot q_2 + r) = m \cdot q_1 + r - m \cdot q_2 - r.$

$a - b = m \cdot (q_1 - q_2) + (r - r).$

Logo: $a - b = m \cdot (q_1 - q_2)$ e segue daí que:

$$m \mid (a - b)$$

($\Leftarrow$)
Suponhamos que:

$$m \mid (a - b)$$

Pela definição da divisão euclidiana, existem $q_1,\ q_2,\ r_1$ e $r_2 \in \mathbb{N}$ tais que:

$$a = m \cdot q_1 + r_1 \tag{3.3}$$

$$b = m \cdot q_2 + r_2 \tag{3.4}$$

Subtraindo (3.3) com (3.4), tem-se:

$a - b = (m \cdot q_1 + r_1) - (m \cdot q_2 + r_2) = m \cdot q_1 + r_1 - m \cdot q_2 - r_2.$

$a - b = m \cdot (q_1 - q_2) + (r_1 - r_2).$

Como, por hipótese,

$$m \mid (a - b)$$

Temos que

$$r_1 - r_2 = 0 \Rightarrow r_1 = r_2 = r$$

Logo, a e b tem ambos os mesmo resto quando divididos por m, isto é:

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

Portanto, $a \equiv b \pmod{m}$ se, e somente se, $m \mid (a - b)$, sendo $r_1 = r_2$ ■

Exemplo 3.4.1.

$36 \equiv 21 \bmod 5$, pois $36 - 21 = 15$ que é divisível por 5.
$36 \equiv 21 \bmod 5$, logo 5 | (36 - 21)

Proposição 3.4.2.

Sejam $m \in \mathbb{N}$, com $m > 1$. Para todos $a, b, c \in \mathbb{N}$, tem-se que:

i) $a \equiv a \pmod{m}$(propriedade reflexiva)

ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$ (propriedade simétrica)

iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$ (propriedade transitiva)

Demonstração 3.4.2.

i) $a \equiv a \pmod{m}$ é equivalente a dizer que $a \equiv a \pmod{m}$ se, e somente se, $m \mid (a-a)$.
Portanto, $m \mid 0$.

ii) Se $a \equiv b \pmod{m} \iff m \mid (a-b)$, se $a > b$ e $m \mid (b-a)$, se $b > a$, pela proposição 3.4.1.

Portanto,

$$b \equiv a \ (mod m).$$

iii) Pela proposição 3.4.1, temos que:

$$a \equiv b \pmod{m},\ b \text{ - } a \text{ é divisível por m}$$
$$b \equiv c \pmod{m},\ c \text{ - } b \text{ é divisível por m}$$

Então,

$$b - a = m \cdot q_1,\ q_1 \in \mathbb{N} \tag{3.5}$$
$$c - b = m \cdot q_2,\ q_2 \in \mathbb{N} \tag{3.6}$$

Somando (3.5) de (3.6), tem-se:

$$(b-a) + (c-b) = mq_1 + mq_2 = m \cdot (q_1 + q_2) \rightarrow c - a = m \cdot (q_1 + q_2)$$

Portanto, $a \equiv c \pmod{m}$ ■

Exemplo 3.4.2.

$$97 \equiv 69 \bmod 7$$
$$69 \equiv 34 \bmod 7$$

Os números 97 e 69 deixam o mesmo resto da divisão por 7 que é o número 6.
Os números 69 e 34 deixam o mesmo resto da divisão por 7 que é o número 6.
Logo, pela proposição 3.4.2 (*iii*), temos:

$$97 \equiv 34 \bmod 7$$

Uma relação entre pares de elementos de um determinado conjunto, congruência módulo m é chamada relação de equivalência, pois satisfaz as propriedades reflexiva, simétrica e transitiva.

Principais propriedades operacionais de congruência modular

Proposição 3.4.3.

Sejam $a,\ b,\ c,\ m,\ x \in \mathbb{N}$, com $m > 1$ e $x \geq 1$.

i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $(a + c) \equiv (b + d) \pmod{m}$

ii) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $(a - c) \equiv (b - d) \pmod{m}$

iii) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \cdot c \equiv b \cdot d \pmod{m}$

iv) Se $a \equiv b \ (mod$ m), então $a^x \equiv b^x \ (mod$ m)

Demonstração 3.4.3.

i) Suponha que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, sendo $b \geq a$ e $d \geq c$, pela **prop 3.4.1** temos que

$$m \mid (b-a) \text{ e } m \mid (d-c).$$

Observa-se que: $m \mid (b-a)+(d-c)$

logo,

$$m \mid (b+d)-(a+c)$$

Portanto,

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

ii) Observa=se também que: $m \mid (b-a)-(d-c)$,

logo,

$$m \mid (b-d)-(a-c)$$

Portanto,

$$(a-c) \equiv (b-d) \pmod{m}$$

iii) Note também que $bd-ac = bd-da+ad-ac = d(b-a)+a(d-c)$

logo,

$$m \mid b \cdot d - a \cdot c$$

Portanto,

$$a \cdot c \equiv b \cdot d \ (\text{mod } m)$$

iv) Como,

$$a \equiv b \ (\text{mod } m).$$

Pela proposição 3.3.3 (i), temos que,
$\underbrace{a + a + a + ... + a}_{x \ vezes} \equiv \underbrace{b + b + b + ... + b}_{x \ vezes} \ (\text{mod } m).$
Portanto,

$$a^x \equiv b^x (mod \text{m})$$

■

Exemplo 3.4.3.

Se, $68 \equiv 53 \text{ mod } 5$ e $43 \equiv 28 \text{ mod } 5$. Então:

i) $(68 + 43) \equiv (53 + 28) \text{ mod } 5 \Rightarrow 111 \equiv 81 \text{ mod } 5$.

ii) $(68 - 43) \equiv (53 - 28) \text{ mod } 5 \Rightarrow 25 \equiv 25 \text{ mod } 5$.

iii) $(68 \cdot 43) \equiv (53 \cdot 28) \text{ mod } 5 \Rightarrow 2924 \equiv 1484 \text{ mod } 5$.

Exemplo 3.4.4.

$2 \equiv 5 \ mod \ 3$
$2^2 \equiv 5^2 \ mod \ 3$
$2^3 \equiv 5^3 \ mod \ 3$
$\vdots$
$2^x \equiv 5^x \ mod \ 3$

Exemplo 3.4.5.

Determinar o resto da divisão por 3 desta expressão $(62468 + 25465 - 15463)$

Como,
$62468 \equiv 2 \text{ mod } 3$
$25465 \equiv 1 \text{ mod } 3$
$15463 \equiv 1 \text{ mod } 3$
$(62468 + 25465 - 15463) \equiv (2 + 1 - 1) \text{ mod } 3$
$(62468 + 25465 - 15463) \equiv 2 \text{ mod } 3$
Logo, o resto é 2.

Critérios de Divisibilidade Aplicando Congruência

No capítulo 2, discutimos critérios de divisibilidade por 2, 3, 5, 9 e 10. Neste capítulo, aplicaremos os critérios de divisibilidade utilizando a noção de congruência modular.

i) Divisibilidade por 2, 5 e 10

Seja o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0,$$

Observe que:

a) $n_r 10^r \equiv 0 \mod 2, \mod 5, \mod 10, r \geq 1$

b) $a \equiv a_0 \mod 2, \mod 5, \mod 10$

Conclusão: Um número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ é divisível por $2,\ 5\ ou\ 10$ se, e somente se, a_0 é divisível por $2,\ 5\ ou\ 10$.

Exemplo 3.4.1.

O número 122.960 é divisível por 2, 5 e 10,

pois, $122.960 \equiv 0 \mod 2, \mod 5, \mod 10$

ii) Divisibilidade por 3 e 9

Seja o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0.$$

Observe que o resto da divisão de $10^n,\ n \geq 0$ por 3 e por 9 é sempre igual a 1, logo,

$$10^r \equiv 1 \mod 3, \mod 9,\ r \geq 1$$

Então,

$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 = a_n.1 + a_{n-1}.1 + ... + a_1.1 + a_0.1,$

ou seja, o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ é divisível por 3 ou por 9, se, e somente se, $a_n + a_{n-1} + ... + a_1 + a_0$ é divisível por 3 ou por 9.

$$a \equiv (a_n + a_{n-1} + ... + a_1 + a_0) \mod 3, \mod 9$$

Portanto, um número é divisível por 3 ou por 9 quando a soma dos seus algarismos é um número divisível por 3 ou por 9.

Exemplo 3.4.2.

O número 560.961 é divisível por 3 e por 9, a soma de seus algarismos,

$$5 + 6 + 0 + 9 + 6 + 1 = 27,$$

é um número divisível por 3 ou por 9, pois,

$$560.961 \equiv 0 \bmod 3, \quad \bmod 9$$

iii) Divisibilidade por 4

Dado o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0,$$

observe que toda potência de $10^n,\ n \geq 2$ é divisível por 4, então,

$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 = a_0 + 10a_1 + 100(a_n q_n + a_{n-1} q_{n-1} + ... + a_2)$

ou seja, $a = a_0 a_1 + 100m,\ m \in \mathbb{N}$ e$m = a_n q_n + a_{n-1} q_{n-1} + ... + a_2$, como $100m$ é divisível por 4, então, a é divisível por 4 se, e somente se, $a_0 a_1$ é divisível por 4.

$$a \equiv a_0 a_1 \bmod 4$$

Portanto, um número é divisível por 4 quando termina em 00 ou os dois últimos algarismos é dividido por 4.

Exemplo 3.4.3.

O número 126.128 é divisível por 4, pois os dois últimos algarismos 28 é divisível por 4, logo,

$$126.128 \equiv 0 \bmod 4$$

iv) Divisibilidade por 7, 11 e 13

Dado o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ escrito na representação decimal

$$a = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10^1 + a_0 10^0,$$

observe que:

$$1000 = 10^3 \equiv -1 \ mod\ 7,\ mod\ 11,\ mod\ 13;$$
$$1000000 = 10^6 \equiv 1 \ mod\ 7,\ mod\ 11,\ mod\ 13;$$
$$10^9 \equiv -1 \ mod\ 7,\ mod\ 11,\ mod\ 13;$$
$$10^{12} \equiv 1 \ mod\ 7,\ mod\ 11,\ mod\ 13;$$
$$\vdots$$
$$(10^3)^x \equiv (-1)^x \ mod\ 7,\ mod\ 11,\ mod\ 13.$$

Portanto,

$$10^{3x} \equiv 1 \ mod\ 7,\ mod\ 11,\ mod\ 13,\ \text{se x for par;}$$
$$10^{3x} \equiv -1 \ mod\ 7,\ mod\ 11,\ mod\ 13,\ \text{se x for impar.}$$

Decompondo o número $a = a_n a_{n-1} a_{n-2} ... a_1 a_0$ em blocos de classes (unidade, dezena, centena, ...), temos:

$a \equiv (a_0a_1a_2(10^3)^0 + a_3a_4a_5(10^3)^1 + a_6a_7a_8(10^3)^2 + a_9a_{10}a_{11}(10^3)^3 + ...)\ mod\ 7,\ mod\ 11,\ mod\ 13.$

$a \equiv (\ a_0a_1a_2 - a_3a_4a_5 + a_6a_7a_8 - a_9a_{10}a_{11} + ...)\ mod\ 7,\ mod\ 11,\ mod\ 13$

ou $(a_3a_4a_5 + a_9a_{10}a_{11} + ...) \equiv (a_0a_1a_2 + a_6a_7a_8 + ...)\ mod\ 7,\ mod\ 11,\ mod\ 13$

Conclusão:

Um número a é divisível por 7, 11 ou 13 quando a soma das classes ímpares menos a soma das classes pares for um número divisível por 7, 11 ou 13.

Exemplo 3.4.4.

Determinar o resto da divisão de 2279788 por 7

(A soma das classes ímpares) − (a soma das classes pares) $= (788 + 2) - 279 = 511$, logo,

$$2279788 \equiv 511\ mod\ 7 \equiv\ 0\ mod\ 7$$

Portanto, o resto da divisão é igual a 0.

Exemplo 3.4.5.

Verificar se o número 514781575 é divisível por 11

(A soma das classes ímpares)−(a soma das classes pares)$= (575 + 514) - 781 = 308$, logo,

$$514781575 \equiv 308\ mod\ 11 \equiv\ 0\ mod\ 11$$

Portanto, 514781575 é divisível por 11.

Exemplo 3.4.6.

Determinar o resto da divisão de 475662395 por 13

(A soma das classes ímpares)−(a soma das classes pares) = $(475 + 395) - 662 = 208$, logo,

$$4756623958 \equiv 208 \; mod \; 13 \equiv \; 0 \; mod \; 13$$

Portanto, o resto da divisão é igual a 0.

Exemplo 3.4.7.

Qual é o resto da divisão de 2^{2013} por 7?

$2 \; \equiv \; 2 \; mod \; 7$

$2^2 \; \equiv \; 4 \; mod \; 7$

$2^3 \; \equiv \; 1 \; mod \; 7$

$2^2 \; \cdot \; 2^2 \; \equiv \; 4 \; \cdot 4 \; mod \; 7 \implies \; 2^4 \; \equiv \; 2 \; mod \; 7$

$2^3 \; \cdot \; 2^2 \; \equiv \; 1 \; \cdot 4 \; mod \; 7 \implies \; 2^5 \; \equiv \; 4 \; mod \; 7$

$2^5 \; \cdot \; 2^5 \; \equiv \; 4 \; \cdot 4 \; mod \; 7 \implies \; 2^{10} \; \equiv \; 2 \; mod \; 7$

$2^{10} \; \cdot \; 2^3 \; \equiv \; 2 \; \cdot 1 \; mod \; 7 \implies \; 2^{13} \; \equiv \; 2 \; mod \; 7$

$(2^{10})^{200} \equiv \; 2 \; mod \; 7 \implies 2^{2000} \; \equiv \; 2 \; mod \; 7$

$2^{2000} \; \cdot \; 2^{13} \; \equiv \; 2 \; \cdot 2 \; mod \; 7 \implies \; 2^{2013} \; \equiv \; 4 \; mod \; 7$

Portanto o resto da divisão é o número 4

Exemplo 3.4.8.

Qual é o último algarismo do número 3^{50}?

Observe as primeiras potências na base 3:

$3^1 = 3, \; 3^2 = 9, \; 3^3 = 27, \; 3^4 = 81, \; 3^5 = 243, \; 3^6 = 729, \; ...$ Os últimos algarismos das primeiras 4 potências de 3 são: $3, \; 9, \; 7$ *e* 1. Elas se repetem periodicamente, de 4 em 4. Logo, para calcular o último algarismo de 3^{50} é só determinar o resto da divisão de 50 por 4, isto é, $50 \; \equiv \; 2 \; mod \; 4$. resto 2

Portanto, $3^{50} \; \equiv 3^2 = 9$.

Concluímos então que o último algarismo é o número 9.

Exemplo 3.4.9.

Verifique se $2339^{2012} + 1541^{2013} + 3329^{2014} + 1253^{2015}$ é divisível por 6.

Calculando as potências 2339^{2012}, 1541^{2013}, 3329^{2014} *e* 1253^{2015}, para depois dividir o resultado por 6, é muito trabalhoso e não é recomendável, Faremos então por congruência modular. Observe que:

$2339 \equiv -1 \ mod\ 6 \implies 2339^{2012} \equiv (-1)^{2012} \ mod\ 6 \implies 2339^{2012} \equiv 1 \ mod\ 6$

$1541 \equiv -1 \ mod\ 6 \implies 1541^{2013} \equiv (-1)^{2013} \ mod\ 6 \implies 1541^{2013} \equiv -1 \ mod\ 6$

$3329 \equiv -1 \ mod\ 6 \implies 3329^{2014} \equiv (-1)^{2014} \ mod\ 6 \implies 3329^{2014} \equiv 1 \ mod\ 6$

$1253 \equiv -1 \ mod\ 6 \implies 1253^{2015} \equiv (-1)^{2015} \ mod\ 6 \implies 1253^{2015} \equiv -1 \ mod\ 6$

Então, $2339^{2012} + 1541^{2013} + 3329^{2014} + 1253^{2015} \equiv (1 - 1 + 1 - 1) \ mod\ 6$.

Logo, $2339^{2012} + 1541^{2013} + 3329^{2014} + 1253^{2015} \equiv 0 \ mod\ 6$, resto 0.

Portanto, $2339^{2012} + 1541^{2013} + 3329^{2014} + 1253^{2015}$ é divisível por 6.

Capítulo 4

Aplicações de Congruência Para o Ensino Básico

Segundo[20], as Aplicações de Congruências modulares , que envolvem fenômenos periódicos no nosso dia-a-dia serão exemplificados a seguir. Estes fenômenos são encontrados nos sistemas de identificação que utilizam diversos códigos numéricos como os códigos de barras, criptografia, documentos de identidade, CPF, CNPJ, ISBN, calendários e diversos outros sistemas numéricos.

4.1 Relógio Analógico

Um relógio analógico, tem o intuito de contar o tempo. As horas, minutos e segundos, embora conte o tempo ininterruptamente, o relógio nunca atinge grandes números, pois ele vai de 0(zero)hora à 12 horas, este processo chamamos de "Aritmética do relógio", que aplicamos na Aritmética Modular. É um caso de congruência módulo 12 ($x \equiv y \ mod \ 12$), para as horas e congruência módulo 60 ($x \equiv y \ mod \ 60$), para os minutos e segundos. Observe que 15 horas é congruente a 3 horas, no módulo 12, ambos divididos por 12, deixam resto 3. E 22 horas (10 horas da noite) é congruente a 10 horas, módulo 12, tanto 22, como 10, divididos por 12, deixam resto 10 e assim em diante.

$$3 \equiv 15 \equiv 27... \ (mod \ 12)$$
$$10 \equiv 22 \equiv 34... \ (mod \ 12)$$

Exemplo 4.1.1.

Num relógio analógico, que horas estará marcando se forem transcorridas 46 horas, depois das 7 horas da manhã?

$7+46 = 53$ horas, dividindo 53 por 12, é igual a 4 e tem resto 5. Logo, $53 \equiv 5 \ (mod \ 12)$. O relógio estará marcando 5 horas, como as 7 horas citadas é da manhã, a resposta é 5 horas da manhã, se fosse 19 horas (7 horas da noite) então seria 5 horas da tarde.

4.2 Teia de Aranha

Exemplo 4.2.1.

A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura 4.1. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118? OBMEP-2010 (Olimpíada Brasileira de Matemática das Escolas Públicas)

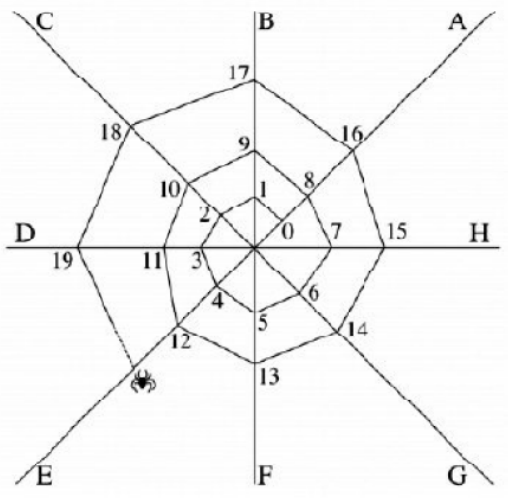

Figura 4.1: Teia de aranha

Aplicando no Ensino Médio, o aluno poderá observar que os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentam de oito em oito e os números divididos por 8 deixam resto zero, que representa o fio A $(8 \cdot n)$. O fio B corresponde aos números que são múltiplos de 8, mais 1, ou seja, números que divididos por 8 deixam resto 1 $(8 \cdot n + 1)$. O fio C corresponde aos números que são múltiplos de 8, mais 2, ou seja, números que divididos por 8 deixam resto 2 $(8 \cdot n + 2)$, e assim até o fio H, definido pelos números que divididos por oito que deixam resto 7 $(8 \cdot n + 7)$.

É claro que para saber sobre qual fio estará o número 118, basta verificar qual dessas famílias tal número pertence e, isso pode ser facilmente obtido ao dividir 118 por 8, que é igual a 14 e obtém resto 6. Tem-se: $118 = 8 \cdot 14 + 6$. Como o resto da divisão é igual a 6, então, sobre o fio G de apoio estará o número 118.

Todos os números, do **exemplo 4.2.1**, que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8, logo, são congruentes entre si, no módulo 8.

O número 118 é congruente ao número 14, no módulo 8, e isso significa que esses dois números deixam o mesmo resto 6, quando divididos por 8

Notação: $118 \equiv 14\ (mod\ 8)$

4.3 ISBN

Um dos exemplos mais antigos é o sistema International Standard Book Number (ISBN) de catalogação de livros, CD-Roms e publicações em braile, que foi criado em 1969. A necessidade que as editoras têm de catalogar os seus livros e informatizar o sistema de encomendas serviu de motivação na geração desse código.

A vantagem é que, por ser um código numérico, ultrapassa as dificuldades geradas pelos diversos idiomas do mundo, bem como a grande diversidade de alfabetos existentes. Dessa forma, pode ser identificado através do ISBN um livro japonês.

Em tal sistema, as publicações são identificadas através de 10 algarismos, sendo que o último (dígito de controle) é calculado através da aritmética modular envolvendo operações matemáticas com os outros nove dígitos. Esses nove primeiros dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

Por exemplo, a língua inglesa é identificada somente pelo algarismo 0 e a editora McGraw-Hill tem um código de 2 algarismos que a identifica, dessa forma, restam ainda 6 algarismos para a identificação de suas publicações, havendo pois a possibilidade de $10^6 = 1000000$ de títulos.

Como se processa o cálculo do dígito final do ISBN (controle).

Representando por $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base 10, 9, 8, 7, 6, 5, 4, 3, 2 e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{10}$ deve ser múltiplo de 11, ou seja,

$$S + a_{10} \equiv 0, mod 11.$$

Exemplo 4.3.1.

Na contracapa do livro Temas e Problemas Elementares, da Coleção Professor de Matemática, da SBM, temos o seguinte código do ISBN: 85-85818-29-8. O dígito de controle é o algarismo 8.

$$\begin{array}{c} 8\ 5\ 8\ 5\ 8\ 1\ 8\ 2\ 9 \\ 10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2 \end{array}$$

Efetuando as multiplicações correspondentes e somando os produtos, tem-se:

$8{\cdot}10+5{\cdot}9+8{\cdot}8+5{\cdot}7+8{\cdot}6+1{\cdot}5+8{\cdot}4+2{\cdot}3+9{\cdot}2 = 80+45+64+35+48+5+32+6+18 = 333$

Dividindo 333 por 11 é igual a 30 e o resto é 3 e $333 = 11 \cdot 30 + 3$

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, ele terá de ser igual a $11 - 3 = 8$. O que confere o valor apresentado no código dado. Isso significa dizer que $333 + 8 = 341$ é um múltiplo de 11, ou ainda, que

$$341 \equiv 0\ mod 11.$$

4.4 Cadastro da Pessoa Física

Uma outra aplicação de Congruência Modular é o Cadastro das Pessoas Físicas da Receita Federal - CPF. O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são chamados de dígitos de controle ou de verificação, como no ISBN. A determinação desses dois dígitos de controle é feita através da congruência aritmética. No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Se $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base 1, 2, 3, 4, 5, 6, 7, 8 e 9, e somar os produtos obtidos.

O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $(S - a_{10})$ deve ser múltiplo de 11, ou seja,

$$(S - a_{10}) \equiv 0 \ mod \ 11.$$

Note que tal número será o próprio resto da divisão por 11 da soma obtida. A determinação do segundo dígito de controle (o último dígito) é feita de modo similar, sendo que agora acrescenta o décimo dígito (que é o que foi calculado) e usa uma base de multiplicação de 0 a 9.

Exemplo 4.4.1.

Os nove primeiros dígitos do CPF é 411 134 977

Calculando o primeiro dígito verificador, escrevendo os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

$$\begin{array}{c} 4\ 1\ 1\ 1\ 3\ 4\ 9\ 7\ 7 \\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{array}$$

Efetuando as multiplicações correspondentes:

$$4 \cdot 1 + 1 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + 9 \cdot 7 + 7 \cdot 8 + 7 \cdot 9 = 234.$$

Logo, dividindo 234 por 11 é igual a 21 e o resto é 3 e $234 = 11 \cdot 21 + 3$. Temos então,

$$m \equiv 0 \bmod 11.$$

Dessa forma, o primeiro dígito de controle será o algarismo 3. A determinação do último dígito de controle(o décimo primeiro dígito) é feita de modo similar, sendo que agora acrescenta o décimo dígito (que foi calculado) e usa uma base de multiplicação de 0 a 9.

$$\begin{matrix} 4\ 1\ 1\ 1\ 3\ 4\ 9\ 7\ 7\ 3 \\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{matrix}$$

Efetuando as multiplicações correspondente:

$$4 \cdot 0 + 1 \cdot 1 + 1 \cdot 2 + 1 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + 9 \cdot 6 + 7 \cdot 7 + 7 \cdot 8 + 3 \cdot 9 = 224.$$

Logo, dividindo 224 por 11 é igual a 20 e o resto é 4 e $224 = 11 \cdot 20 + 4$. Temos,

$$m \equiv 0 \bmod 11.$$

Logo, o segundo dígito de controle é o 4. Conclui-se então que, o meu CPF completo é:

411 134 977 - 34

Se o resto da divisão fosse 10 em vez de 4, ou seja, se o número obtido fosse congruente a 10 módulo 11, utilizaria, nesse caso, o dígito zero.

4.5 Cadastro Nacional da Pessoa Jurídica

Outra aplicação de Congruência Modular é o Cadastro Nacional de Pessoa Jurídica - CNPJ. O número de CNPJ de uma empresa, no Brasil, é constituído de 14 dígitos, sendo um primeiro bloco com 12 algarismos(os primeiros oito dígitos são o número-base, os quatro seguintes, o número de ordem das filiais da empresa) e um segundo bloco, com mais dois algarismos, que são chamados de dígitos de controle ou de verificação.

No caso do CNPJ, o décimo terceiro dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros doze algarismos.

Se $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}$ é a sequência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8 e 9 e somar os produtos obtidos.

O dígito que está faltando, representado por a_{13} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S - a_{13}$ deve ser múltiplo de 11, ou seja,

$$(S - a_{13}) \equiv 0, mod 11.$$

Note que tal número será o próprio resto da divisão por 11 da soma obtida. A determinação do segundo dígito de controle (o último dígito verificador) é feita de modo similar, sendo que agora acrescenta o décimo terceiro dígito (o que foi calculado anteriormente) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros treze algarismos.

Se $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$ é a sequência formada pelos 13 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base 5, 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8 e 9 e somar os produtos obtidos.

O dígito que está faltando, representado por a_{14} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S - a_{14}$ deve ser múltiplo de 11, ou seja,

$$(S - a_{14}) \equiv 0, mod 11.$$

Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Exemplo 4.5.1.

Veja o cálculo do dígito verificador do CNPJ: 47.333.034/0001−??.

Obtém-se o primeiro dígito de controle, escrevendo os doze primeiros e, abaixo deles, a base de multiplicação com os dígitos 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8 e 9 .

$$\begin{array}{c} 4\ 7\ 3\ 3\ 3\ 0\ 3\ 4\ 0\ 0\ 0\ 1 \\ 6\ 7\ 8\ 9\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{array}$$

Efetuando as multiplicações correspondentes:

$$4 \cdot 6 + 7 \cdot 7 + 3 \cdot 8 + 3 \cdot 9 + 3 \cdot 2 + 0 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + 0 \cdot 6 + 0 \cdot 7 + 0 \cdot 8 + 1 \cdot 9 = 171.$$

Logo,
dividindo 171 por 11 é igual a 15 e o resto é 6 e $171 = 11 \cdot 15 + 6$.
Dessa forma, o primeiro dígito de controle será o algarismo 6.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescenta o décimo terceiro dígito(que foi calculado) e usa uma base de multiplicação os dígitos 5, 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8 e 9 .

$$\begin{array}{c} 4\ 7\ 3\ 3\ 3\ 0\ 3\ 4\ 0\ 0\ 0\ 1\ 6 \\ 5\ 6\ 7\ 8\ 9\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \end{array}$$

Efetuando as multiplicações correspondentes:

$$4 \cdot 5 + 7 \cdot 6 + 3 \cdot 7 + 3 \cdot 8 + 3 \cdot 9 + 0 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 0 \cdot 5 + 0 \cdot 6 + 0 \cdot 7 + 1 \cdot 8 + 6 \cdot 9 = 221.$$

Dividindo 221 por 11 é igual a 20 e o resto é 1, logo

$$221 = 11 \cdot 20 + 1.$$

o segundo dígito de controle é o 1. Conclui-se então que, o dígito verificador é o 61. Portanto, o CNPJ completo é:

$$47.333.034/0001 - 61$$

Observação 4.5.1.

Se o resto da divisão for 10 em vez de 1, é considerando 0, ou seja, se o número obtido for congruente a 10, módulo 11, utilizaríamos, nesse caso, o dígito zero(algumas instituições tratam o 10 como X).

4.6 Código de Barras

Hoje em dia, com avanço de novas tecnologias, tornando relativamente baratos e acessíveis os aparelhos de leitura óptica e computadores, tornou-se mais viável o uso dos códigos de barras, que são utilizados para representar a identificação dos produtos, unidades logísticas, localizações, documentos, contêineres, cargas etc. Com a praticidade dos serviços, facilitando a captura de dados através de leitores (scanners) e coletores de código de barras, que o transmite para o computador, propiciando a automação de processos, trazendo a eficiência, o maior controle e a confiabilidade para a empresa.

Mesmo assim, o estudo dos Códigos de Barras estão ausentes nas escolas do Ensino Básico. Sua estrutura é muito simples e certamente poderiam ser usados para motivar estudos sobre divisibilidade com números inteiros e até mesmo ter conhecimento sobre os principais códigos que nos cercam no dia-a-dia.

O Código de Barras (BARCODE) obteve a primeira patente em outubro de 1952 - figura 4.2 (EUA 2.612.994 - Método e Aparato de Classificação) , por Norman Joseph woodland [1] e Bernard Silver [2][21].

[1] woodland, Norman J. (1921-2012) - EUA - Físico e Engenheiro Mecânico
[2] Silver, Bernard - (1924 - 1963) - Bacharel em Ciências em Engenharia Elétrica e Física

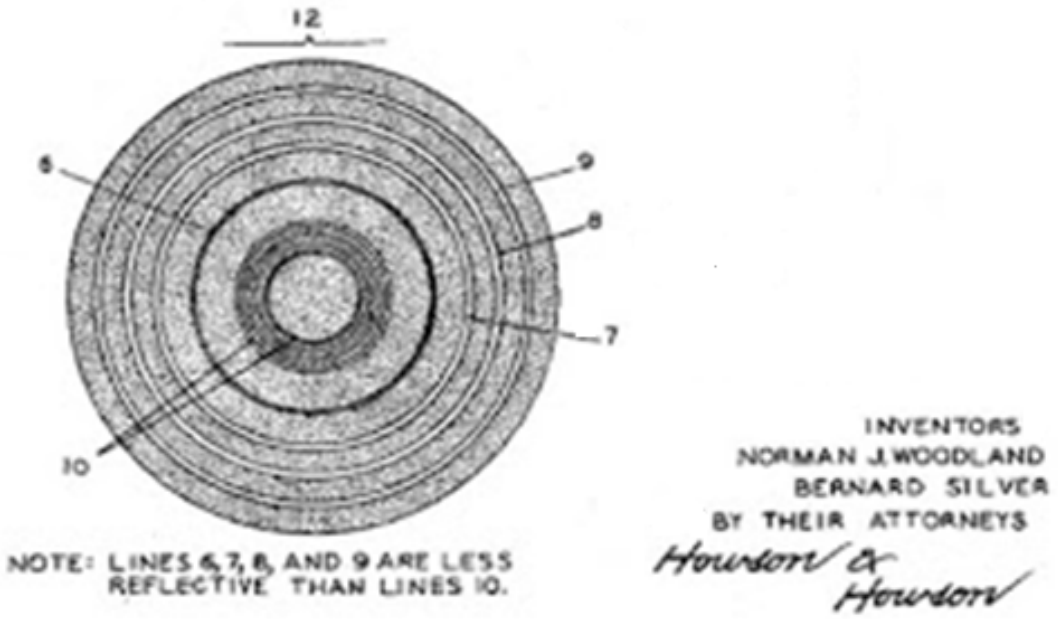

Figura 4.2: primeiro Barcode

No início da década de 1970, George J. Laurer [3], um colega de Woodland na IBM (onde o Engenheiro entrou em 1951 e permaneceu até a sua reforma em 1987) aperfeiçoou o código de barras, desenhando o retângulo com as barras a preto e os espaços a branco, constituía uma sequência de 12 dígitos, que seria lido por *scanner de laser*, o método só funcionou graças às tecnologias do laser e dos microprocessadores.

Laurer inventou o primeiro código de barras, veja figura 4.3, o Código Universal de Produtos (UPC), adaptado para Indústria nos Estados Unidos e no Canadá, maio 1973, onde foi vendido o primeiro produto com código de barras - era um pacote de pastilhas elásticas a 67 cêntimos (*Guardian*- Jornal Britânico)[21].

Figura 4.3: 1º UPC - Laurer, G. J.

[3]Laurer, George Joseph (1623-1662) - Matemático, Físico, Filósofo e Pesquisador Francês.

O Código de Barras European Article Number (EAN) é um Código de Barras definido pela GS1, que é uma organização internacional, sem fins lucrativos, dedicada ao desenvolvimento e implantação de globais para a gestão eficientes de cadeias de suprimento, registrado pelos princípios da ISO/IEC 15459-2, utilizados em mais de 140 países, para a identificação dos itens, principalmente nos pontos de venda a varejo. O EAN-13 codifica 13 números divididos em quatro partes, doze são dados referentes ao produto e um é o dígito verificador (Codificação EAN-13, 2007).

Por isso que a EAN tem um dígito a mais em relação a UPC, permitindo a identificação do país de origem do produto, de tal forma que a máquina leitora pudesse ler indistintamente códigos UPC e EAN. Observe que na figura 4.4, representa o mesmo código numérico escrito em ambos sistemas, com um 0 a mais no início da sequência que representa os países EUA e Canadá, que são identificados com um 0, na frente, e o resto da codificação é a mesma do sistema anterior da UPC [21].

Figura 4.4: Códigos de Barras - UPC e EAN-13

Outros países, os primeiros dois ou três dígitos, identificam o país, como exemplo temos o código de Barras de todos os produtos produzidos no Brasil (decreto-lei instituindo o código de barras no País assinado pelo então Presidente João Batista de Oliveira Figueredo em 29 de novembro de 1984), que ficou estabelecida a sequência 789 (Números Identicadores de cada País), que é a identificação do país, como exemplo, o código 7898357410015, como vemos na figura 4.5 que começa com a sequência 789 (País de origem Brasil)[22].

Figura 4.5: Código de Barras - Brasil

Exemplo 4.6.1.

Para calcular o dígito verificador do Código de Barras do EAN - 13, tomando como exemplo o número 789100031550-?. Multiplicam-se os dígitos por 1 ou 3, em sequência repetitiva:

$$7 \cdot 1 = 7,\ 8 \cdot 3 = 24,\ 9 \cdot 1 = 9,\ 1 \cdot 3 = 3,\ 0 \cdot 1 = 0,\ 0 \cdot 3 = 0,$$
$$0 \cdot 1 = 0,\ 3 \cdot 3 = 3,\ 1 \cdot 1 = 1,\ 5 \cdot 3 = 15,\ 5 \cdot 1 = 5,\ 0 \cdot 3 = 0.$$

Depois somamos os resultados da multiplicação (S), e encontramos o múltiplo de 10 maior ou igual, neste caso, a soma é igual a 73 e o múltiplo maior é o 80.

Subtraindo 80 - 73 = 7.

Logo, o dígito verificador é o $a_{13} = 7$.

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

Portanto, o Código de Barras completo do EAN-13 é o 7891000315507.

O Código de barras UPC tem 12 dígitos, um a menos EAN que tem 13 dígitos, seu cálculo é semelhante ao EAN.

4.7 Criptografia

Criptografia, vem do Grego, *cryptós* que representa secreto, oculto, escondido, e *gráphein* que representa escrita, de acordo com Severino Coutinho [2]. É o estudo dos princípios, métodos e técnicas para codificar uma mensagem de modo que só seu destinatário consiga interpretar, chamado de *decriptação* que decifra os códigos criptográficos. *Criptoanálise* é a ciência que estuda as formas de decifrar tais informações.

O objetivo da criptografia é transformar um conjunto de informação legível, como um e-mail, por exemplo, em um emaranhado de caracteres impossível de ser compreendido, apenas quem tem a chave de decriptação é capaz de recuperar o e-mail em formato legível. Mesmo conhecendo todos o processo para esconder e recuperar os dados, a pessoa não consegue descobrir a informação sem a chave de decriptação, veja figura 4.6 [23].

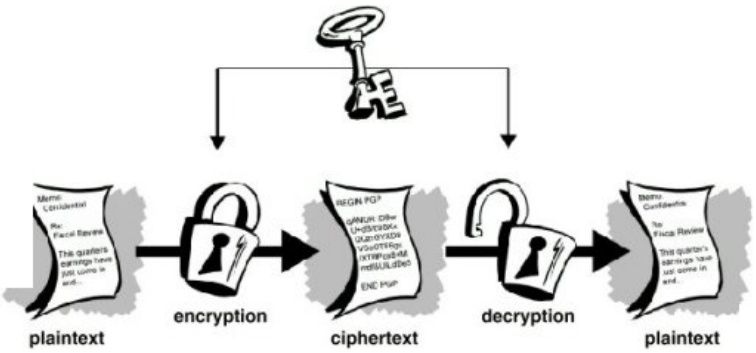

Figura 4.6: Criptação - decriptação

Desde a antiguidade o homem tem interesse em enviar mensagens protegidas por códigos, como os Egípcios, Gregos e Romanos que utilizavam técnicas tanto inteligentes quanto criativas, prevenindo que caísse em mãos erradas, em assuntos ligados com à guerra, à religião, ao amor e à diplomacia. Por volta de 3000 a.C, no Egito, escribas usavam hieróglifos[4], escrita de difícil interpretação, que constitui provavelmente o mais antigo sistema escrito organizado do mundo, feito nas paredes de templos e túmulos.

Entre 600 a.C e 500 a.C, os hebreus utilizavam substituição simples, os caracteres são trocados um a um por outros, e com ela escreveram o Livro de Jeremias que é considerado o segundo dos livros dos principais profetas da Bíblia, no seu livro foi utilizado métodos criptográficos.

Segundo Ricardo Vianna[23], *O Código de César* [5]como era chamado de Codificador de Júlio César ou cifra de César, seu funcionamento era básico, é um exemplo de substituição simples, que substituía as letras do alfabeto avançando 3 casas, o codificador trocava cada letra por outra situada a três posições à frente no alfabeto, deslocando as letras do alfabeto, de acordo com a figura 4.7, transformava a letra A em D, a letra B em E e assim sucessivamente. Esse algoritmo, durante a guerra, foi responsável por enganar muitos inimigos do Império Romano. No entanto, é extremamente inseguro, pois existem apenas 26 variações possíveis, dado que o alfabeto tem 26 letras, após ter sido descoberta a chave, como todas, perdeu sua funcionalidade. Se trocarmos as letras do alfabeto por números utilizando código com números, $A-1$, $B-2$, $C-3$, $D-4$, $E-5, ...$, $Z-26$, com

[4] *hieróglifos - é um termo originário de duas palavras gregas - hierós: sagrado e glýphein: escrita*
[5] Júlio César - (100-44 a.C) - Imperador de Roma.

os números maiores que 26 teríamos um caso de congruência modular, $X \equiv 0\ (mod\ 26\ )$, como o número 28 é maior que 26, temos, $28 \equiv 2\ (\ mod\ 26\ )$, que representa a letra B do nosso alfabeto e o mesmo caso o número 62, temos, $62 \equiv 10\ (\ mod\ 26\ )$, que representa a letra J.

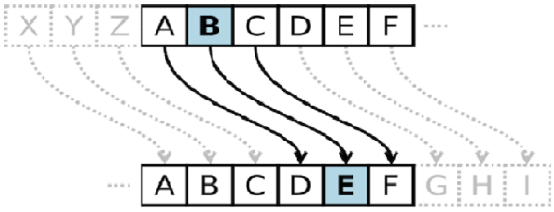

Figura 4.7: Código de César

Procurou-se uma forma de aumentar a segurança do Código de César, baseado em permutar, que representa troca de posição das letras, todas as 26 letras do alfabeto e encontrou-se 26! (lê-se: vinte e seis fatorial). Fatorial de um número natural $n > 0$ é o produto de todos seus antecessores, incluindo si próprio e excluindo o zero, representado por: $n! = n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot (n-4) \cdot ... \cdot 3 \cdot 2 \cdot 1$, logo, $26! = 26 \cdot 25 \cdot 24 \cdot 23 \cdot ... \cdot 3 \cdot 2 \cdot 1$, que é muito maior.

Uma outra maneira para criptografar uma mensagem, que é chamado de **Códigos em Bloco**, que consiste no seguinte:

Exemplo 4.7.1.

MESTRADO PROFISSIONAL EM MATEMÁTICA

Criptografando esta frase nos códigos em bloco, temos:

1º Passo: elimina os espaços e completa a mensagem com a letra A no final, caso tenha uma quantidade ímpar de letras;

MESTRADOPROFISSIONALEMMATEMATICA

2º Passo: subdivide a mensagem em bloco de duas letras

ME-ST-RA-DO-PR-OF-IS-SI-ON-AL-EM-MA-TE-MA-TI-CA

3º Passo: reflete cada bloco

EM-TS-AR-OD-RP-FO-SI-IS-NO-LA-ME-AM-ET-AM-IT-AC

4º Passo: permuta os blocos, trocando o primeiro com o último, o terceiro com o antepenúltimo, e assim sucessivamente, deixando os outros blocos como estão

AC-TS-AM-OD-AM-FO-LA-IS-NO-SI-ME-RP-ET-AR-IT-EM

5º Passo: Por fim, retira-se os espaços e têm-se a mensagem codificada

ACTSAMODAMFOLAISNOSIMERPETARITEM

De fato, estes códigos são melhores que o Código de César, mas, para as aplicações comerciais, os Códigos em Blocos apresentam uma grande desvantagem. Vejamos neste exemplo.

Exemplo 4.7.2.

Uma pessoa pretende fazer uma compra em uma loja, pela primeira vez, por meio da internet. Esta compra é feita com o cartão de crédito, sendo fornecido os dados do cartão, números e data de vencimento, ao ser enviados para loja, o computador do cliente codifica os dados. e a loja tem acesso da codificação e decodifica a mensagem. Como foi dito, os Códigos em Bloco, não são aplicados neste caso, sendo utilizados em linha telefônica ou em banda larga, pois se fossem transmitidos em blocos, facilmente uma outra pessoa conseguiria decodificar a mensagem e ler os dados do cartão.

Um outro processo chamado de chave de codificação ou chave pública é o mais viável para ser utilizado no exemplo anterior, pois, mesmo que o computador seja invadido por um "hacker", interceptando a mensagem codificada teria um trabalho enorme para decodificar e levaria muito tempo.

A Criptografia, sempre esteve subordinada a fins militares. Nos dias de hoje está sendo muito utilizada em transações bancárias e comerciais entre computadores em rede. Tal mudança tornou necessária a criação de uma chave pública (chave pública - é um método de criptografia que envia uma mensagem codificada ao destinatário, onde o destinatário cifra a mensagem) idealizado em 1976 por Whitfield Diffie[6] e Edward Martin Hellman[7], da Universidade de Stanford - EUA.

A Criptografia de Chave Pública ou Assimétrica é um método utilizado por um par de chaves: uma chave pública, que é distribuída a todos os correspondentes via e-mail, e outra chave privada, que deve ser conhecida apenas pelos seus donos.

Em 1977, Ronald (Ron) **R**ivest Linn[8], Adi **S**hamir [9] e Max Leonard **A**dleman[10], que trabalhavam no Institute of Technology - em Massachussets - EUA, inventaram a Criptografia RSA, este simbolo representa iniciais das letras dos inventores, é o mais conhecido método de chave-pública utilizado em todo mundo.

[6]Diffie, Whitfield - nascido nos EUA, em 5 de junho de 1944 - Matemático e criptógrafo.
[7]Hellman, E. Martin - nascido nos EUA, em 02 de outubro de 1945 - Matemático e criptógrafo.
[8]Rivest, Ron L. - nascido nos EUA, em 1947 - Matemático e criptógrafo.
[9]Adi Shamir - nascido em Tel Aviv, Israel, em 1952 - criptógrafo.
[10]Adleman, M. Leonard - nascido nos EUA, em 1945 - criptógrafo.

RSA funciona com um par de chaves, uma pública, que todos podem ter conhecimento, e uma privada, que se mantém em sigilo, Atuando diretamente na internet, por e-mails, compras e outras transações, sendo codificado e recodificado pela criptografia.

Para entender o funcionamento RSA, que estão relacionados com os números, serão utilizadas várias técnicas matemáticas. Como exemplo, uma loja comercial quer fazer a codificação dos dados de um cliente pela internet, primeiro escolhe dois números naturais primos distintos e multiplica-os, obtém-se um número natural composto, veja Teorema 4.7.1. A loja manterá secreta a informação sobre os números primos escolhidos, visto que é necessário para codificar as mensagens enviadas pelo RSA. O número inteiro resultante do produto dos números primos será enviado por qualquer pessoa que compre na loja pela web, porque são os dados do cartão de crédito que o computador precisa. Uma chave segura de RSA é gerada por números primos, muito grandes, de 100 algarismos cada e o produto 200 algarismos. Isto pode levar muitos anos para fatorar[11], mesmo utilizando os computadores mais poderosos.

Logo, o problema é "fácil de fazer e difícil de desfazer"

Definição 4.7.1. *Números Primos:*

"Todo número natural maior que 1, que só é divisível por um e por si próprio é chamado de número primo." [12]

Teorema 4.7.1. *Teorema Fundamental da Aritmética[7].*

Todo número natural $\boldsymbol{n}$ *maior do que 1 ou é primo ou se escreve de modo único como um produto de números primos(números compostos).*

Demonstração 4.7.1.

Usando o Princípio de Indução Completa:

Para $n = 2$, o resultado é obviamente verificado, pois o número *2* é o único número primo par, ele é divisível por um e por ele mesmo.

Para $n > 2$. Se n é um número primo, nada temos a demonstrar, pela definição **4.7.1**. Suponha que n é um número que não seja primo, existem números naturais n_1 e n_2, chamados de números compostos, tais que $n = n_1 \cdot n_2$, $1 < n_1 < n$ e $1 < n_2 < n$. Então, pela hipótese de indução, existem números primos $p_1, ..., p_r$ e $q_1, ..., q_s$ de modo que $n_1 = p_1...p_r$ e $n_2 = q_1...q_s$.

Portanto, $n = p_1...p_r \cdot q_1...q_s$.

Provar agora que esta decomposição é única. Suponha que $n = p_1...p_r = q_1...q_s$, sendo p_i e q_j números primos.

Como $p_1 \mid q_1...q_s$, temos que $p_1 = q_j$, para algum j, supõe-se que seja q_1.

[11] A Decomposição de um Número Natural em produtos de fatores primos é chamada de fatoração.

Portanto, $p_2...p_r = q_2...q_s$.

Como, $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

Exemplo 4.7.3.

Sejam dois números primos distintos 53 e 37.

Os divisores de 53 são 1 e 53.

Os divisores de 37 são 1 e 37.

O produto de 53 e 37 é igual a 1961.

Os divisores de 1961 são 1, 37, 53 e 1961.

Exemplo 4.7.4.

O número 9638129, ao fazer a decomposição em fatores primos verificou-se que não é divisível por $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ..., 997, ..., 1657, ...$

Depois de muitos cálculos, verificou-se que os divisores de 9638129 são 1, 2699, 3571 e 9638129.

Escolhemos um número natural de 200 ou mais algarismos, sabendo que o produto dos outros dois são números primos, como encontrar os dois números primos de 100 algarismos que se multiplicam e dá este resultado?

Portanto, vimos que o problema é fácil de fazer e difícil de desfazer no exemplo anterior.

Para implementar o sistema RSA:

1º - Escolhe dois números primos p e q distintos muito grandes, no mínimo 100 algarismos cada.

2º - Multiplica estes números $p \cdot q$ e obtêm n, isto é, $n = p \cdot q$

3º - Para codificar uma mensagem usa-se n.

4º - Para decodificar uma mensagem usam-se p e q.

5º - n pode tornar público.

6º - p e q devem ser mantidos em segredo.

7º - Quebrar o RSA consiste em fatorar n, que leva muito tempo.

Para que isso aconteça, a mensagem deve ser um número inteiro, nem sempre é um número, a maior parte das mensagens é um texto.

Utilizando o exemplo anterior:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	X	W	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 4.1: pré-codificação

Fazendo a pré-codificação, convertendo as letras em números, de pelo menos dois algarismos para que não haja ambiguidades, de acordo com a tabela abaixo:

Acrescenta o número 99 no espaço entre duas palavras, logo:

$$221428292710132499252724151828281824231021991422992210291422102918121 0$$

No sistema RSA, ao escolher os dois números inteiros primos, cujo resto da divisão por 6 tem que ser 5, exemplo: $53 \equiv 5 \ mod \ 6$, pelo menos maior de 100 algarismos cada, a codificação da mensagem do exemplo acima, é menor que $n = p \cdot q$:

$$221428292710132499252724151828281824231021991422992210291422102918121 0$$

Fica difícil fazer o cálculo do cubo deste número módulo n, representado abaixo:

$$221428292710132499252724151828281824231021991422992210291422102918121 0^3 mod(n)$$

Codificar uma mensagem no RSA é calcular sua potência de um número muito grande, com módulo n maior ainda, relativamente a um expoente escolhido, que utiliza aritmética modular. Uma estimativa baseada em métodos de análise de algoritmos nos diz que o tempo necessário para um computador moderno fatorar um número de 100 algarismos é de aproximadamente 74 anos, enquanto um de 200 algarismos é da ordem de $3,8 \cdot 10^8$ anos.

Capítulo 5

Os Números nos Calendários

5.1 Introdução

É comum aparecer em programas de televisão pessoas que apresentam "habilidades especiais" para memorizar dias da semana de anos anteriores. Estas pessoas não tem nada de especial, elas têm facilidade em utilizar algoritmos, que é acessível para qualquer pessoa que saiba fazer as quatro operações básicas. O desafio, na verdade, é criar uma sequência de passos que direcionem o exercício mental. Com pouco treino é possível até impressionar seus amigos e familiares.

Saber criar e lidar com algoritmos é interessante e pode ser útil no mundo informatizado de hoje.

5.2 Um Breve Histórico dos Números nos Calendários

A Data Juliana foi inventada pelo estudioso francês José Justo Escalígero (1540-1609) e provavelmente recebeu este nome devido ao pai de Escalígero, o estudioso italiano Júlio César Escalígero (1484-1558). Os astrônomos têm utilizado a Data Juliana para atribuir um número único para cada dia a partir de 1 de janeiro de 4713 a.C. Esta é a tão falada Data Juliana (DJ). DJ 0 (zero) designa as 24 horas que vão do meio-dia de 1 de janeiro de 4713 a.C até o meio-dia de 2 de janeiro de 4713 a.C.

O calendário juliano foi implantado pelo líder romano Júlio César, em 46 a.C, como uma importante e substancial alteração no calendário romano, Júlio César, percebendo que as festas romanas em comemoração à estação mais florida do ano, marcadas para março (que era o primeiro mês do ano), caíam em pleno Inverno, determinou que o astrônomo alexandrino Sosígenes corrigisse o calendário.

As modificações realizadas a partir desses estudos modificaram radicalmente o calendário romano: dois meses, Unodecembris e Duocembris foram adicionados ao final do ano de 46 a.C, deslocando assim Januarius e Februarius para o início do ano de 45 a.C.

Os dias dos meses foram fixados numa sequência de 31, 30, 31, 30... de Januarius a Decembris, à exceção de Februarius, que ficou com 29 dias e que, a cada três anos, teria 30 dias. Em 44 a.C, o líder Júlio César foi homenageado pelo senado, que mudou o nome do mês Quintilis para Julius, um mês de 31 dias. Foi modificado ainda mais em 8 d.C., pelo imperador Augusto, e os nomes dos meses sofreram ainda várias mudanças ao longo do Império Romano.

O senado romano decidiu também homenagear seu primeiro imperador através da mudança do nome do mês Sextilis para Augustus. O mês de Februarius passou de 29 para 28 dias, cedendo um dia para o mês em homenagem a Augusto, que passou de 30 para 31 dias, com mudança também nos demais meses, de 31 para 30 e vice e versa até o fim do ano. Veja como ficaram os meses após 8 d.C na figura 5.1.

No.	Mês	Dias
1	*Januarius*	31
2	*Februarius*	28 ou 29
3	*Martius*	31
4	*Abrilis*	30
5	*Maius*	31
6	*Junius*	30
7	*Julius*	31
8	*Augustus*	31
9	*September*	30
10	*October*	31
11	*November*	30
12	*December*	31

Figura 5.1: meses romano

No Calendário Juliano, o ano tropical é aproximado como 365 1/4 dias = 365,25 dias. Isto ocasiona um erro de aproximadamente um dia a cada 128 anos. O calendário Juliano continuou em uso corrente até 1582, vigorou até a Idade Média quando alguns países começaram a mudar para o Calendário Gregoriano.

O erro acumulado fez com que o Papa Gregório XIII, Em 1582, convocasse uma equipe de matemáticos e astrônomos para criar um calendário que se adequasse melhor à quantidade de tempo que nosso planeta leva para dar uma volta completa em torno do Sol. Depois de muitas propostas apresentadas, foi adotado o seguinte procedimento, com o ano bissexto de 366 dias e ano normal de 365 dias. No Calendário Gregoriano o ano tropical é aproximado como 365 + 97 / quatrocentos dias = 365,2425 dias.

Leva aproximadamente 3.300 anos para o ano tropical se deslocar um dia em relação ao Calendário Gregoriano. A aproximação 365+97/400 é obtida colocando 97 anos bissextos

a cada quatrocentos anos, utilizando as seguintes regras:

- Todo ano divisível por 4 é um ano bissexto.
- Entretanto, todo ano divisível por 100 não é um ano bissexto.
- Entretanto, todo ano divisível por 400 é um ano bissexto sempre.

Portanto, 1700, 1800, 1900, 2100 e 2200 não são anos bissextos. Porém, 1600, 2000 e 2400 são anos bissextos. Contrapondo, no antigo Calendário Juliano todos os anos divisíveis por 4 são bissextos.

A Bula Papal de fevereiro de 1582 decretou que deveriam ser retirados 10 dias de outubro de 1582, fazendo com que 15 de outubro viesse imediatamente após 4 de outubro, conforme demonstrado, veja figura 5.2.

Outubro 1582

Dom	Seg	Ter	Qua	Qui	Sex	Sáb
	1	2	3	4	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Figura 5.2: Bula Papal

Sendo assim, o calendário gregoriano é respeitada na Itália, Polônia, Portugal e Espanha. Outros países católicos seguiram logo após, mas os países protestantes relutaram em mudar. Os países ortodoxos gregos não mudaram até o início do século XX. A reforma foi seguida pela Inglaterra e seus domínios, incluindo os EUA, em 1752.

Foram elaborados calendários diferentes em várias partes do mundo. Muitos eram anteriores aos sistema Gregoriano, mas a importância desse calendário católico reside no fato de incluírem um referencial que é a data de nascimento de Jesus Cristo. Diferentemente, o Calendário Chinês, que remontaria ao século XIV a.C, só atendia o tempo de existência de cada imperador. Duravam da posse até a morte do imperador; após a morte paravam de contar e só reiniciavam a contagem após a posse do novo imperador. Nesse caso os historiadores tiveram que somar os dias da semana até que conseguiram chegar ao Imperador Huangdi que não inventou um calendário mas com certeza tomou posse em 2637 a.C . A República Popular da China utiliza o Calendário Gregoriano para as finalidades civis.

Em 2004, foi descoberto o calendário mais antigo, com pelo menos dez mil anos de existência, na região de Aberdeen, na Escócia. Por arqueólogos britânicos, chefiada pelo

professor de arqueologia Vince Gaffney. O monumento do período mesolítico capaz de medir as fases da lua e os meses do ano. Um artigo publicado pela primeira vez na revista "Internet Archaeology"

Segundo o professor, as evidências sugerem que essas sociedades tinham necessidade e a sofisticação de medir o tempo através dos anos, de corrigir as diferenças sazonais do ano lunar. E isso aconteceu cinco mil anos antes dos primeiros calendários formais conhecidos pelo homem, encontrados na antiga Mesopotânia. Ele conta que os pesquisadores encontraram um conjunto de 12 pedras bastante peculiares de tamanhos diferentes, que parecem as fases da lua, elas estava arrumadas por tamanhos, desde as menores às maiores, voltando as menores novamente. E estavam orientadas em direção ao lugar onde o sol nascia, de uma passagem entre duas montanhas.

Ele afirma que os calendários recém-descobertos podem não ter apenas a divisão do tempo em meses, mas em dias. No entanto, destacou que é necessário encontrar provas disso.

Considerações Finais

Esta dissertação assumiu como principal objetivo propor alguns tópicos de congruência modular que podem ser aplicados no Ensino Básico. Os temas escolhidos foram a divisibilidade e a congruência modular com seus conceitos e propriedades. Esta ferramenta permitirá ao aluno tanto do Ensino Fundamental como do Ensino Médio, fazer investigações matemáticas, com seus fundamentos, como por exemplo, a divisibilidade e seus critérios, permitindo uma melhor compreensão deste assunto sobre os números inteiros, através do estudo de congruência módulo m.

Com este trabalho, observamos a necessidade e a viabilidade do aprofundamento significativo da divisão euclidiana e seu desenvolvimento para congruência modular, que pouco é comentado no Ensino Básico. A divisão com resto bem conceituada, pode o professor enfim apresentar o método de Euclides abertamente e utilizar de forma consciente.

Nos números no nosso dia a dia apresentamos diversas aplicações de congruência modular, o ISBN, o cadastro de pessoa física e jurídica, o código de barras, a criptografia e muitos outros. Enfim, apresentamos os números nos calendários, com os anos normais e bissexto.

Acreditamos que este trabalho possa servir como um material de apoio para o docente de matemática da educação básica, que possa sanar algumas dificuldades na área da Aritmética. Servindo enfim de apoio, motivação e inspiração para um futuro aperfeiçoamento nos curso de pós-graduação, podendo assim surgir contribuições para o Ensino e Aprendizagem de Matemática, em particular, nas aplicações da Aritmética ao nosso cotidiano.

Referências Bibliográficas

[1] CARVALHO, J. B. P. *Os Elementos de Euclides*. Cadernos da RPM-Revista do Professor de Matemática, vol.05, nº 1, 1994.

[2] COUTINHO, Severino C. *Criptografia*. Programa de Iniciação Científica - OBMEP. IMPA - Rio de Janeiro, 2008.

[3] Divisão Euclidiana. Mestrado Profissional em Matemática - PROFMAT - MA14 - U2 - 2011.

[4] DOMINGUES, Higino H. *Fundamentos de Aritmética* .São Paulo: Atual, 1991.

[5] EVES, Howard.*Introdução à História da Matemática*, tradução Domingues, Higyno H. . São Paulo: Editora da Unicamp, 2004.

[6] HEFEZ, Abramo *Curso de Álgebra*, v.1, 3ª ed. - Sociedade Brasileira de Matemática-SBM, Rio de Janeiro. 2002.

[7] HEFEZ, Abramo *Elementos da aritmética*, 2ª ed. - Sociedade Brasileira de Matemática-SBM, Rio de Janeiro, 2011.

[8] IEZZI, Gelson.*Matemática e Realidade*, 5ª/8ª séries, 4ª ed. - São Paulo, SP: Atual, 2000.

[9] LIMA, Elon Lages.*Curso de Análise*, v.1, 14ª ed. - Rio de Janeiro. Associação Instituto Nacional de Matemática Pura e Aplicada. Projeto Euclides. 2012.

[10] Platão, *A república, Introdução e notas de Maria Helena da Rocha Pereira*, 5ª ed.Lisboa: Fundação Calouste Gulbenkian, 1987, p. 513.

[11] SINGH, S. *O Último Teorema de Fermat*. tradução CALIFE, Jorge L., 13ª ed. Rio de Janeiro: Record, 2008.

[12] Teorema Fundamental da Aritmética. Mestrado Profissional em Matemática - PROFMAT - MA14 - U12 - 2011.

[13] ZUCKERMAN, Herbert S.; NIVEN, Ivan *Introduccion a la Teoria de los Numeros*. Mexico: Editorial Limusa, 1976.

[14] _____. *Tales de Mileto*. Disponível em: <http://www.educ.fc.ul.pt/icm/icm99/icm28/tales.htm.> Acesso em: 15 de Agosto de 2013.

[15] _____. *Euclides*. Disponível em: <http://www.educ.fc.ul.pt/docentes/opombo/seminário/euclides/euclides.htm.> Acesso em: 10 de Setembro de 2013.

[16] _____. *Diofanto de Alexandria*. Disponível em: <http://pt.wikipedia.org/wiki/Diofanto_de_Alexandria>. Acesso em: 12 de Setembro de 2013.

[17] _____. *Diofanto*. Disponível em: <http//www.somatematica.com.br/biograf/diofanto.php> Acesso em: 12 de Setembro de 2013.

[18] _____. *Aritmética modular*. Disponível em: <http://pt.wikipedia.org/wiki/Aritmética _modular> Acesso em: 17 de Setembro de 2013.

[19] _____. *Critérios de Divisibilidade*. Disponível em: <http://brasilescola.com/matematica/criterios_divisibilidade.htm> Acesso em: 8 de Outubro de 2013.

[20] _____. *Aritmética modular e algumas aplicações no cotidiano*. Disponível em: <http://magiadamatematica.com/unifeso/1-aritmodular.pps> Acesso em: 10 de Outubro de 2013.

[21] _____. *primeiro código de barra*. Disponível em: <http://maiseducativa.com/2012/10/09/o-mundo-as-riscas/> Acesso em: 11 de Outubro de 2013.

[22] _____. *barcode - números indicadores de cada País*. Disponível em: <http://barcodeisland.com//ean13.phtml.> Acesso em: 11 de Outubro de 2013.

[23] _____. *Criptografia*. Disponível em: <http://prof-ricardovianna.blogspot.com/2011/05/criptografia-parte-i-historia-da.htm> Acesso em: 14 de Outubro de 2013.