INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA

MESTRADO EM MATEMÁTICA - PROFMAT

Iury Kersnowsky de Sant'Anna

A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental

Rio de Janeiro - RJ

1º semestre/2013

Iury Kersnowsky de Sant'Anna

A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática (PROFMAT), ministrado pelo Instituto Nacional de Matemática Pura e Aplicada, como requisito para a obtenção do Grau de Mestre.

Área de atuação: Ensino da Matemática

Orientador: Prof. Dr. Roberto Imbuzeiro Oliveira

Rio de Janeiro - RJ

1º semestre/2013

Iury Kersnowsky de Sant'Anna

A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática (PROFMAT), ministrado pelo Instituto Nacional de Matemática Pura e Aplicada, como requisito para a obtenção do Grau de Mestre. Área de atuação: Ensino da Matemática

Aprovada em _____ de 2013

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. ROBERTO IMBUZEIRO – IMPA

_____

Prof. Dr. _____ – _____

_____

Prof. Dr. _____ – _____

Rio de Janeiro - RJ

1º semestre/2013

Dedicatória

Este trabalho é dedicado à maravilhosa família que Deus me deu: meus pais Paulo César e Tamara, por sempre me apoiarem nas decisões mais difíceis; à minha irmã Ludmila, por ser uma grande amiga; à minha esposa Amanda, meu amor e companheira no sentido mais amplo da palavra e à minha filha Laís, o meu maior presente.

Agradecimentos

Agradeço primeiramente aos excelentes professores de matemática que tive o prazer de ter no decorrer dos ensinos fundamental e médio: Ivan Figueira Mendes, Sérgio Lins, Lincoln Abrantes, Brandão (in memoriam), Benjamin e José Ricardo. Obrigado por despertarem a paixão pela matemática dentro de mim.

Agradeço também a todos os professores que tive no decorrer do mestrado, em especial a Roberto Imbuzeiro, por ser tão compreensivo quanto às nossas aflições e anseios e por sempre estar disposto a colaborar.

Agradeço ainda a Anderson Carvalho, Paulo César Antunes, Rodrigo Fraga e Welbert Moutta, companheiros de turma de mestrado que se tornaram grandes amigos.

Em especial agradeço a Lúcia Maria Aversa Villela, por suas dicas valiosas e palavras de conforto e entusiasmo, sempre na hora correta.

Resumo

Esta dissertação aborda a aritmética modular, também conhecida como “Teoria das Congruências”, como uma ferramenta valiosa de ensino para as séries finais do ensino fundamental. Apresenta um breve embasamento teórico, pautado nas propriedades operatórias da congruência, porém sempre com o cuidado de não se exceder quanto ao que é realmente necessário absorver nesta etapa do aprendizado. Justifica propor o ensino deste tópico, o que não é feito tradicionalmente nessa faixa etária, através de exemplos do cotidiano e das provas dos critérios de divisibilidade.

Palavras chave: aritmética modular, congruência, séries finais do ensino fundamental, critérios de divisibilidade.

Abstract

This dissertation addresses the modular arithmetic, also known as “congruences theory”, as a valuable tool for teaching the upper grades of elementary school. Presents a brief theoretical foundation, based on the properties of congruence operative, but always being careful not to exceed as to what is really necessary to absorb this stage of learning. Justify proposing the teaching of this topic, which is not traditionally done in this age group, using examples from everyday life and the evidence of the criteria of divisibility.

Keywords: modular arithmetic, congruence, upper grades of elementary school, criteria of divisibility.

SUMÁRIO

1. INTRODUÇÃO

A palavra **aritmética,** proveniente do grego arithmetiké, significa “ciência dos números”. É conhecida como um dos ramos mais antigos e elementares da matemática, tendo surgido com a necessidade do homem de contar e evoluído com sua necessidade de calcular.

> Mestre: **"O que é Aritmética?"**
> Discípulo: **"É a arte de contar, ou a ciência dos números, que considera sua natureza e propriedades, possibilitando meios mais simples para expressá-los, compreendê-los, resolvê-los, que é o que chamamos calcular".**
> ***(PEANO, Giuseppe,* Principia de Arithmetices, 1889)**
>
> Pergunta: **"O que é aritmética?"**
> Resposta: **"A ciência que trata da quantidade discreta".**
> P.: **"Que é quantidade?"**
> R.: **"Tudo o que pode aumentar ou diminuir".**
> P.: **"Sob este ponto de vista, tudo o que existe no universo é quantidade?"**
> R.: **"Sim, senhor. Tudo é quantidade, exceto Deus"**
> **(A. GALLEGO CHAVES, Aritmética para niños, 1876, Madrid)**

O prefixo 'ar' significa reunir, ou seja, a aritmética é a ciência que reúne - soma, subtrai, multiplica, divide - os números. Trata-se, portanto, da parte da matemática que estuda as operações numéricas.

Dentre essas operações, esta dissertação tem como foco as divisões nos naturais e seus respectivos restos, caracterizando assim a chamada Aritmética Modular, cujas bases teóricas tiveram início com trabalhos do matemático suiço Euler, por volta de 1750. Posteriormente, grandes matemáticos como Lagrange e Legendre também produziram trabalhos sobre o assunto. Porém a “Teoria das Congruências” se tornou mais explícita através do livro *Disquisitiones Arithmeticae,* publicado em 1801 pelo matemático alemão Carl Friedrich Gauss, abordando o assunto com a simbologia e definições utilizadas até hoje.

O estudo da aritmética faz parte do currículo obrigatório do ensino fundamental brasileiro, o mesmo não acontecendo especificamente com a aritmética modular, conteúdo que acaba sendo visto apenas por estudantes que seguem alguns ramos das ciências exatas no ensino superior.

Utilizando como motivação o ensino da matemática como ferramenta de formação de um cidadão crítico, capaz de compreender pensamentos conceituais, o presente trabalho tem como objetivo propor a inserção de uma introdução à “Teoria das Congruências” nas séries finais do Ensino Fundamental, discutindo suas aplicações aos conhecidos (mas raramente demonstrados nesse nível) critérios de divisibilidade.

A metodologia utilizada para justificar tal escolha será apresentar uma breve fundamentação teórica no capítulo 2 e argumentar utilizando dois enfoques específicos: no capítulo 3, através das demonstrações dos critérios de divisibilidade mais utilizados, o que não é tradicionalmente feito no Ensino Fundamental, pela falta de um arcabouço teórico que torne tais demonstrações viáveis; e no capítulo 4, através de exemplos de Aritmética Modular aplicados ao cotidiano. No capítulo 5, apresentaremos e resolveremos questões recentes de concursos de acesso ao nível médio que, ao utilizarmos a Aritmética Modular, tornam-se mais simples.

Pretendemos chegar a um material que possa servir de ponto de apoio ao professor, com um caráter de “formação continuada”, e que também se mostre aplicável em sala de aula, que estimule o raciocínio lógico como ponto chave do aprendizado da matemética, em detrimento de assimilar métodos ou fórmulas preestabelecidas.

Temos também como meta obter conclusões sobre a validade e adequação do ensino da Aritmética Modular nesta fase de aprendizado, se realmente é condizente e útil com a maturidade e necessidades dos alunos nesse ponto do ciclo escolar.

2. FUNDAMENTAÇÃO TEÓRICA

A “Teoria das Congruências” é um vasto campo da matemática, inserido na Teoria dos Números. Abrange propriedades e teoremas cujo entendimento e aplicabilidade variam dos níveis mais básicos aos mais avançados. Porém como o escopo deste trabalho é um incremento no arcabouço teórico de professores e alunos do Ensino Fundamental, nos restringiremos apenas a itens úteis para esse fim. As escolhas feitas serão justificadas nos capítulos seguintes, na observação das aplicações e demonstrações pertinentes a esta faixa etária. Os resultados abaixo também podem ser vistos no livro Elementos da Aritmética (Hefez,Abramo), 2ª edição, SBM, 2005.

2.1. Definição

Sejam dois números naturais **a** e **b** que, após efetuadas as divisões Euclidianas por outro número natural **m**, não nulo, produzem o mesmo resto. Dizemos então que “**a** é congruente com **b** módulo **m**”. Simbologia: $\boxed{a \equiv b \mod m}$.

Por exemplo, sejam os números 58 e 43. Efetuando a divisão de ambos por 5, observamos que

Concluímos então que $58 \equiv 43 \mod 5$.

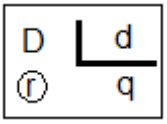
2.2. Proposições

Para todas as proposições abaixo, considere **m** um número natural não nulo. Observe que se torna desinteressante discutir a congruência mod 1, pois a divisão de qualquer número inteiro por 1 deixa resto 0. Todas as proposições estão seguidas de suas respectivas demonstrações.

I. *Sejam* ***a*** *e* ***b*** *números inteiros e* $b \geq a$. *Então* $a \equiv b \mod m$ *se e somente se m for divisor de b – a.*

Demonstração:

A divisão Euclidiana é estruturada da seguinte forma:



E vale a relação D = d.q + r. $(0 \leq r < m)$

As divisões de a e b por m podem ser reescritas como: $\begin{cases} a = m.q_a + r_a \\ b = m.q_b + r_b \end{cases}$

Efetuando a subtração, encontramos:

$$b - a = m.(q_b - q_a) + (r_b - r_a). \qquad (0 \leq r_a < m \text{ e } 0 \leq r_b < m)$$

Logo $0 \leq |r_a - r_b| < m$

Assim, se torna simples observar que, para b – a ser divisível por m, $r_b - r_a$ também deve ser divisível por m. Como este número está entre –m e m (exclusive), resulta que ele deve ser nulo, ou seja, $r_b = r_a$. Então $a \equiv b \mod m$.

Ex: $58 \equiv 43 \mod 5$, pois 58 – 43 = 15, que é divisível por 5.

II. *Sejam* ***a***, ***b*** *e* ***c*** *números inteiros tais que* $a \equiv b \mod m$ *e* $b \equiv c \mod m$. *Então* $a \equiv c \mod m$.

Demonstração:

Utilizando (**I**), se

$a \equiv b \mod m$, b – a é divisível por m.

$b \equiv c \mod m$, c – b é divisível por m.

Então $\begin{cases} b-a=mq_1 \\ c-b=mq_2 \end{cases}$ e, efetuando a subtração dos termos, obtemos:

$$(c-b)-(b-a)=m(q_2-q_1)\rightarrow c-a=m(q_2-q_1)$$

Ou seja, c – a é divisível por m, então por (**I**) $a\equiv c \mod m$.

Ex: $58\equiv 43 \mod 5$ e $43\equiv 18 \mod 5 \rightarrow$ Logo $58\equiv 18 \mod 5$

III. *Sejam* ***a****,* ***b,*** ***c*** *e* ***d*** *números inteiros tais que* $a\equiv b \mod m$ *e* $c\equiv d \mod m$. *Então* $a+c\equiv b+d \mod m$.

Demonstração:

Suponhamos, sem perda de generalidade, que $b\geq a$ *e* $d\geq c$. Utilizando **(I)**, se

$a\equiv b \mod m$, b – a é divisível por m.

$c\equiv d \mod m$, d – c é divisível por m.

Assim $\begin{cases} b-a=mq_1 \\ d-c=mq_2 \end{cases}$ e, efetuando a soma dos termos, obtemos:

$$(b-a)+(d-c)=m(q_2+q_1)\rightarrow (b+d)-(a+c)=m(q_2+q_1)$$

Então $(b+d)-(a+c)$ é divisível por m. Por **(I)** $a+c\equiv b+d \mod m$.

IV. *Sejam* ***a****,* ***b,*** ***c*** *e* ***d*** *números inteiros tais que* $a\equiv b \mod m$ *e* $c\equiv d \mod m$. *Então* $a-c\equiv b-d \mod m$.

Demonstração:

Suponhamos, sem perda de generalidade, que $b\geq a$ *e* $d\geq c$. Utilizando **(I)**, se

$a\equiv b \mod m$, b – a é divisível por m.

$c\equiv d \mod m$, d – c é divisível por m.

Assim $\begin{cases} b-a=mq_1 \\ d-c=mq_2 \end{cases}$ e, efetuando a subtração dos termos, obtemos:

$$(b-a)-(d-c)=m(q_1-q_2)\rightarrow(b-d)-(a-c)=m(q_1-q_2)$$

Então $(b-d)-(a-c)$ é divisível por m. Por **(I)** $a-c\equiv b-d \mod m$.

As propriedades **(III)** e **(IV)** têm grande utilidade na resolução de expressões que envolvam somas e subtrações e a respectiva divisão do resultado por um número **m**. Suponha que **a** deixe resto R e **b** deixe resto r na divisão por m. Utilizando a notação de congruências, escrevemos:

$$\begin{cases} a\equiv R \mod m \\ b\equiv r \mod m \end{cases}$$

Então, sem perda de generalidade, supondo $a\geq b$, podemos afirmar, utilizando **(III)** e **(IV)** respectivamente, que

$$\boxed{\begin{array}{l} a+b\equiv R+r \mod m \\ a-b\equiv R-r \mod m \end{array}}$$

Isto significa dizer que *"o resto deixado pela soma ou pela subtração de dois números, quando divididos por **m**, é dado pela soma ou pela subtração, respectivamente, dos restos deixados por esses números na divisão por **m**"*. A relevância deste resultado está em tornar desnecessário somar ou subtrair todos os números de uma expressão para posteriormente efetuar a divisão e calcular o resto.

Exemplo: A expressão (52678 + 24569 – 39806), ao ser dividida por 5, deixa que resto?

Solução:

O critério de divisão por 5, que será justificado posteriormente, consiste em dividir o último algarismo do número por 5, e o resto deixado será o mesmo que o deixado por esse algarismo.

52678 dividido por 5 deixa resto 3 → $52678\equiv 3 \mod 5$

24569 dividido por 5 deixa resto 4 → $24569\equiv 4 \mod 5$

39806 dividido por 5 deixa resto 1 → $39806\equiv 1 \mod 5$

Substituindo os restos, obtemos:

$$52678+24569-39806\equiv(3+4-1)\bmod 5$$
$$52678+24569-39806\equiv 6\bmod 5$$
$$52678+24569-39806\equiv 1\bmod 5$$

Assim, o resto procurado é 1.

V. *Sejam* ***a, b, c*** *e* ***d*** *números inteiros tais que* $a\equiv b \bmod m$ *e* $c\equiv d \bmod m$. *Então* $ac\equiv bd \bmod m$.

Demonstração:

Suponhamos, sem perda de generalidade, que $b\geq a$ *e* $d\geq c$. Utilizando **(I)**, se

$a\equiv b \bmod m$, b – a é divisível por m.

$c\equiv d \bmod m$, d – c é divisível por m.

Assim: $\begin{cases} b-a=mq_1 \\ d-c=mq_2 \end{cases}$

Observe a validade da identidade $d(b-a)+a(d-c)=bd-ac$

Logo: $bd-ac=dmq_1+amq_2=m(dq_1+aq_2)$

Então $bd-ac$ é divisível por m. Por **(I)** $ac\equiv bd \bmod m$.

VI. *Sejam* ***a*** *e* ***b*** *números inteiros tais que* $a\equiv b \bmod m$ *e* ***n*** *natural não nulo. Então* $a^n\equiv b^n \bmod m$.

Demonstração:

Considere “n congruências” $a\equiv b \bmod m$:

$$\begin{cases} a\equiv b \bmod m \\ a\equiv b \bmod m \\ \quad\quad ... \\ \quad\quad ... \\ a\equiv b \bmod m \end{cases}$$

Utilizando **(V)**, podemos multiplicar cada lado da congruência, obtendo $\underbrace{a \times a \times ... \times a}_{n} \equiv \underbrace{b \times b \times ... \times b}_{n} \bmod m \rightarrow a^n = b^n \bmod m$.

As propriedades **(V)** e **(VI),** aliadas ao que foi citado pelas propriedades **(III) e (IV),** têm grande utilidade na resolução de expressões que envolvam produtos e potências e a respectiva divisão do resultado por um número **m**. Suponha que **a** deixe resto R e **b** deixe resto r na divisão por m. Utilizando a notação de congruências, escrevemos:

$$\begin{cases} a \equiv R \bmod m \\ b \equiv r \bmod m \end{cases}$$

Então podemos afirmar, utilizando **(V)**, que: $\boxed{ab \equiv Rr \bmod m}$

Sem perda de generalidade, utilizando **(VI)**, podemos afirmar que $\boxed{a^n = R^n \bmod m}$.

Isto significa dizer que:

*1º) o resto deixado pelo produto de dois números, quando divididos por **m**, é dado pelo resto do produto dos restos deixados por esses números na divisão por **m**.*

*2º) o resto deixado pela potência **n** de um número na divisão por **m**, é o resto deixado pelo resto da divisão do número por **m**, elevado a **n**.*

A relevância destes resultados está em tornar desnecessário multiplicar ou efetuar potências desnecessariamente, para posteriormente efetuar a divisão.

> ***Exemplo*:** A expressão (52678 x 24569 + 39807^5), ao ser dividida por 5, deixa que resto?
>
> <u>*Solução:*</u>
>
> 52678 dividido por 5 deixa resto 3 → $52678 \equiv 3 \bmod 5$
>
> 24569 dividido por 5 deixa resto 4 → $24569 \equiv 4 \bmod 5$
>
> 39807 dividido por 5 deixa resto 1 → $39807 \equiv 2 \bmod 5$

Substituindo os restos, obtemos:

$$52678 \times 24569 + 39807^5 \equiv \left(3 \times 4 + 2^5\right) \bmod 5$$
$$52678 \times 24569 + 39807^5 \equiv (12 + 32) \bmod 5$$
$$52678 \times 24569 + 39807^5 \equiv 44 \bmod 5$$
$$52678 \times 24569 + 39807^5 \equiv 4 \bmod 5$$

Assim, o resto deixado é 4.

Demonstradas as proposições, torna-se evidente que não é necessário nenhum conhecimento que não esteja diretamente ligado as operações fundamentais para manipulá-las, ou seja, estão ao alcance dos alunos das séries finais do Ensino Fundamental.

Com as proposições citadas, atingimos o objetivo de fazer uma "Introdução à Teoria das Congruências". Assuntos como *Teorema de Fermat*, *Teorema de Euler* e *Teorema de Wilson,* que também fazem parte desse conteúdo, não serão abordados nesta etapa, devido a maior complexidade de suas demonstrações e a falta de necessidade frente aos problemas pertinentes a esta faixa etária.

3. CRITÉRIOS DE DIVISIBILIDADE

O ensino da aritmética elementar, em vigência nas escolas de Ensino Fundamental, aborda o assunto “critérios de divisibilidade” como um conjunto de regras a serem memorizadas e aplicadas de maneira direta. Inegavelmente, tais “atalhos” se mostram muito úteis na resolução de problemas, mas a maneira como esse conhecimento chega ao aluno levanta algumas questões. Segundo Santaló (2008,p.11)

> **“A missão dos educadores é preparar as novas gerações para o mundo em que terão de viver. Isto quer dizer proporcionar-lhes o ensino necessário para que adquiram as destrezas e habilidades que vão necessitar para seu desempenho, com comodidade e eficiência, no seio da sociedade que enfrentaram ao concluir sua escolaridade”.**

Então entendemos que a atual metodologia preconiza o produto imediato e acaba deixando em segundo plano o desenvolvimento do pensamento analítico no aluno. Nesta faixa etária, a falta de justificativas em relação a procedimentos acaba provocando preconceitos em relação à disciplina, pois acabam por desestimular os discentes.

Resultados que surgem por “passe de mágica” mascaram o real sentido de se estudar matemática: estimular o raciocínio lógico. O aluno perde autonomia, pois não tem ferramentas necessárias para especular sobre outros critérios, a não ser os ensinados pelo seu professor.

Baseado nesses fatos, faremos um estudo das demonstrações dos critérios de divisibilidade, via “Teoria das Congruências”, com a intenção de justificar tais critérios. O objetivo é que funcione como guia para os professores das séries finais do Ensino Fundamental.

SANTALÓ, Luis Antonio (2009), Naveira, Antonio M.; Reventós, Agustí; Birman, Graciela S. et al., eds., *Luis Antonio Santaló selected works*, Berlin, New York:

Para as demonstrações abaixo, considere, sem perda de generalidade, $N = a_{n-1}...a_2a_1a_0$ um número com **n** algarismos, que pode ser reescrito, decompondo suas ordens, como $N = a_{n-1} \times 10^{n-1} + ... + a_2 \times 10^2 + a_1 \times 10 + a_0$.

3.1. Critério de divisibilidade por 2

"Um número é divisível por 2 se e somente se seu último algarismo for par".

Demonstração:

Como 10 = 2 x 5, ao substituir em N obtemos:

$$N = a_{n-1} \times 2^{n-1} \times 5^{n-1} + ... + a_2 \times 2^2 \times 5^2 + a_1 \times 2 \times 5 + a_0$$

$$N = 2 \times \left(a_{n-1} \times 2^{n-2} \times 5^{n-1} + ... + a_2 \times 2 \times 5^2 + a_1 \times 5 \right) + a_0$$

Utilizando **(2.2.5)**

$$N \equiv \underbrace{0 \times \left(a_{n-1} \times 2^{n-2} \times 5^{n-1} + ... + a_2 \times 2 \times 5^2 + a_1 \times 5 \right)}_{0} + a_0 \bmod 2$$

$$N \equiv a_0 \bmod 2$$

Como a_0 é um algarismo e 0, 2, 4, 6 e 8 são divisíveis por 2 e 1, 3, 5, 7 e 9 não são, está provado que $N = a_{n-1}...a_2a_1a_0$ é divisível por 2 se seu ultimo algarismo for par.

3.2. Critério de divisibilidade por 2^x

"Um número é divisível por 2^x se e somente se seus x últimos algarismos formarem um número divisível por 2^x".

Demonstração:

Adotando uma decomposição alternativa de N como

$N = (a_{n-1}...a_x) \times 10^x + (a_{x-1}...a_1a_0)$ e utilizando **(2.2.5)**

$$N \equiv \underbrace{2^x \times \left(a_{n-1} \times 2^{n-x} \times 5^{n-x} + ... + a_2 \times 2 \times 5^2 + a_1 \times 5 \right)}_{0} + a_{x-1}...a_1a_0 \bmod 2^x$$

$N \equiv a_{x-1}...a_1a_0 \bmod 2^x$, número formado pelos x últimos algarismos de N, confirmando a proposição.

Exemplo: Que resto deixa 2.439.243.475, ao ser dividido por 8?

Solução:

Como 8 = 2^3, utilizando **(3.2)**, observamos que para verificar se o número é divisível por 8, basta utilizar o número formado pelos seus 3 últimos algarismos.

$$\begin{array}{r|l} 475 & 8 \\ \hline ③ & 59 \end{array}$$

Logo a divisão não é exata, produzindo resto 3.

3.3. Critério de divisibilidade por 5

"Um número é divisível por 5 se e somente se seu último algarismo for 0 ou 5".

Demonstração:

Como 10 = 2 x 5, ao substituir em N obtemos:

$$N = a_{n-1} \times 2^{n-1} \times 5^{n-1} + ... + a_2 \times 2^2 \times 5^2 + a_1 \times 2 \times 5 + a_0$$

$$N = 5 \times \left(a_{n-1} \times 2^{n-1} \times 5^{n-2} + ... + a_2 \times 2^2 \times 5 + a_1 \times 2 \right) + a_0$$

Utilizando **(2.2.5)**

$$N \equiv \underbrace{0 \times \left(a_{n-1} \times 2^{n-1} \times 5^{n-2} + ... + a_2 \times 2^2 \times 5 + a_1 \times 2 \right)}_{0} + a_0 \bmod 5$$

$$N \equiv a_0 \bmod 5$$

Como a_0 é um algarismo e os únicos que são divisíveis por 5 são 0 e 5, está provada a proposição.

3.4. Critério de divisibilidade por 5^x

"Um número é divisível por 5^x se e somente se seus x últimos algarismos formarem um número divisível por 5^x".

Demonstração:

Adotando uma decomposição alternativa de N como

$N = (a_{n-1}...a_x) \times 10^x + (a_{x-1}...a_1a_0)$ e utilizando **(2.2.5)**

$$N \equiv \underbrace{5^x \times \left(a_{n-1} \times 5^{n-x} \times 2^{n-x} + ... + a_2 \times 5 \times 2^2 + a_1 \times 2\right)}_{0} + a_{x-1}...a_1a_0 \bmod 5^x$$

$N \equiv a_{x-1}...a_1a_0 \bmod 5^x$, número formado pelos x últimos algarismos de N, confirmando a proposição.

Exemplo: O número 12.459.273.375 é divisível por 125?

Solução:

Como $125 = 5^3$, utilizando **(3.4)**, observamos que para verificar se o número é divisível por 125, basta utilizar o número formado pelos seus 3 últimos algarismos.

$$\begin{array}{r|l} 375 & 125 \\ \hline (0) & 3 \end{array}$$

Logo a divisão é exata.

3.5. Critério de divisibilidade por 3

"Um número é divisível por 3 se e somente se a soma dos seus algarismos formar um número divisível por 3".

Demonstração:

Seja $N = a_{n-1} \times 10^{n-1} + ... + a_2 \times 10^2 + a_1 \times 10 + a_0$.

Utilizando **(2.2.1)**, observamos que $10 \equiv 1 \bmod 3$ e, através de **(2.2.6)**, $10^x \equiv 1^x \bmod 3 \rightarrow 10^x \equiv 1 \bmod 3$. Substituindo esta congruência em N, obtemos:

$$N \equiv \left(a_{n-1} \times 1 + ... + a_2 \times 1 + a_1 \times 1 + a_0\right) \bmod 3$$

$N \equiv \left(a_{n-1} + ... + a_2 + a_1 + a_0\right) \bmod 3$, confirmando a proposição.

3.6. Critério de divisibilidade por 9

"Um número é divisível por 9 se e somente se a soma dos seus algarismos formar um número divisível por 9".

Demonstração:

Seja $N = a_{n-1} \times 10^{n-1} + ... + a_2 \times 10^2 + a_1 \times 10 + a_0$.

Utilizando **(2.2.1)**, observamos que $10 \equiv 1 \bmod 9$ e, através de **(2.2.6)**, $10^x \equiv 1^x \bmod 9 \rightarrow 10^x \equiv 1 \bmod 9$. Substituindo esta congruência em N, obtemos:

$$N \equiv \left(a_{n-1} \times 1 + ... + a_2 \times 1 + a_1 \times 1 + a_0\right) \bmod 9$$

$N \equiv \left(a_{n-1} + ... + a_2 + a_1 + a_0\right) \bmod 9$, confirmando a proposição.

Exemplo: O número 583ab é divisível por 9. O valor máximo da soma dos algarismos de a e b é:

Solução:

Como 5+8+3+a+b=16+a+b, utilizando **(3.6)**, observamos que para verificar se o número é divisível por 9, basta que 16 + a + b = x seja múltiplo de 9.

A primeira opção seria x = 18 e, então, a + b = 2.

A segunda opção seria x = 27 e, então, a + b = 11.

A terceira opção seria x = 36 e, então, a + b = 20, que é impossível, pois a e b são algarismos.

Qualquer múltiplo maior que este geraria a + b maiores e, consequentemente, também impossíveis.

Assim o valor máximo de a + b é 11.

3.7. Critério de divisibilidade por 11

"Um número é divisível por 11 se e somente se a soma de suas ordens ímpares, subtraída da soma de suas ordens pares, formar um número divisível por 11".

Demonstração:

Seja $N = a_{n-1} \times 10^{n-1} + \ldots + a_2 \times 10^2 + a_1 \times 10 + a_0$.

Utilizando **(2.2.1)**, observamos que $10 \equiv -1 \bmod 11$ e, através de **(2.2.6)**,

$$10^x \equiv (-1)^x \bmod 11 \rightarrow \begin{cases} 10^x \equiv 1 \bmod 11, \text{ se x for par} \\ 10^x \equiv -1 \bmod 11, \text{ se x for ímpar} \end{cases}.$$

Substituindo esta congruência em N, obtemos:

$$N \equiv \left(a_{n-1}(-1)^{n-1} + \ldots - a_3 + a_2 - a_1 + a_0\right) \bmod 11$$

$N \equiv \left[\left(a_0 + a_2 + a_4 + \ldots\right) - \left(a_1 + a_3 + a_5 + \ldots\right)\right] \bmod 11$, ou seja, a soma das ordens ímpares menos a soma das ordens pares, confirmando a proposição.

Exemplo: O número 123.436.729 é divisível por 11?

Solução:

Utilizando **(3.7)** para verificar se o número é divisível por 11, basta calcular (9+7+5+3+1) - (2+3+4+2). O resultado é 14, que não é um número divisível por 11. Logo o número não é divisível por 11 e como $14 \equiv 3 \bmod 11$, o resto da divisão é 3.

3.8. Critério de divisibilidade por 7

"Um número é divisível por 7 se e somente se a soma de suas classes ímpares, subtraída da soma de suas classes pares, formar um número divisível por 7".

Demonstração:

Seja $N = a_{n-1} \times 10^{n-1} + ... + a_2 \times 10^2 + a_1 \times 10 + a_0$. Utilizando **(2.2.1)**, observamos que $1.000 \equiv -1 \bmod 7$, ou seja, $(10)^3 \equiv -1 \bmod 7$. Através de **(2.2.6)**

$$(10^3)^x \equiv (-1)^x \bmod 7 \rightarrow \begin{cases} 10^{3x} \equiv 1 \bmod 7, \text{ se x for par} \\ 10^{3x} \equiv -1 \bmod 7, \text{ se x for impar} \end{cases}.$$

Decompondo N em blocos de classes e substituindo esta congruência, obtemos:

$$N \equiv \left(... + a_8 a_7 a_6 \times (10^3)^2 + a_5 a_4 a_3 \times (10^3)^1 + a_2 a_1 a_0 \times (10^3)^0 \right) \bmod 7$$

$$N \equiv \left(... + a_8 a_7 a_6 - a_5 a_4 a_3 + a_2 a_1 a_0 \right) \bmod 7$$

Ou seja, a soma das classes ímpares menos a soma das classes pares, confirmando a proposição.

Diversos critérios de divisibilidade se mostram como combinações entre outros critérios. Por exemplo, 6 = 2 x 3 e, então, para um número ser divisível por 6, deve ser divisível por 2 e 3 ao mesmo tempo.

Além disso, cabe citar que os critérios de divisibilidade demonstrados, aliados a ideia da combinação entre os mesmos, constitui a base tradicionalmente ensinada nas escolas do Ensino Fundamental, porém de forma bem fundamentada, apoiados em uma base teórica sólida. É dada a possibilidade ao aluno de investigar sobre outros métodos, não os deixando presos unicamente aos conhecimentos transmitidos pelo professor.

4. A ARITMÉTICA MODULAR NO COTIDIANO

4.1 Sistemas de Identificação

Nosso cotidiano está repleto de aplicações simples, porém úteis, da Aritmética Modular. Indubitavelmente, as mais frequentes são os chamados Sistemas de Identificação, que atendem desde produtos até documentos.

Um desses casos é o Cadastro de Pessoas Físicas **(*CPF*)**, documento cuja numeração possui 11 dígitos, sendo os dois últimos chamados dígitos de controle ou verificação. Eles têm a função de evitar fraudes e enganos e são encontrados em função dos 9 primeiros, seguindo a seguinte regra:

> *"Sejam $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ os 9 primeiros dígitos. Para encontrar o primeiro dígito verificador devemos multiplicá-los, ordenadamente, por {1,2,3,4,5,6,7,8,9} e somar os resultados (S). O décimo dígito (a_{10}) é o resto da divisão de S por 11, com a exceção do caso aonde o resto é 10, quando será utilizado o dígito zero. Para encontrar o segundo dígito verificador, devemos multiplicar, ordenadamente, os dígitos de $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ por {0,1,2,3,4,5,6,7,8,9} e somar os resultados (S'). O décimo primeiro dígito (a_{11}) é o resto da divisão de S' por 11, com a exceção do caso aonde o resto é 10, quando será utilizado o dígito zero."*
>
> *(http://imasters.com.br/artigo/2410/javascript/algoritmo-do-cpf/)*

Em outras palavras, os dígitos verificadores do CPF são encontrados através de duas congruências módulo 11: $S - a_{10} \equiv 0 \bmod 11$ e $S' - a_{11} \equiv 0 \bmod 11$, salvo a exceção supracitada.

Por exemplo, seja o CPF iniciado por 054.894.927. Seu primeiro dígito verificador é dado por

$$S = 0\times1+5\times2+4\times3+8\times4+9\times5+4\times6+9\times7+2\times8+7\times9$$
$$S = 0+10+12+32+45+24+63+16+63 = 265$$
$$\text{Então: } 265 - a_{10} \equiv 0 \bmod 11 \rightarrow \boxed{a_{10} = 1}$$

Consequentemente, segundo dígito verificador é

$$S = 0\times 0 + 5\times 1 + 4\times 2 + 8\times 3 + 9\times 4 + 4\times 5 + 9\times 6 + 2\times 7 + 7\times 8 + 1\times 9$$
$$S = 0 + 5 + 8 + 24 + 36 + 20 + 54 + 14 + 56 + 9 = 226$$
$$\text{Então: } 226 - a_{11} \equiv 0 \bmod 11 \rightarrow \boxed{a_{11} = 6}$$

Então o CPF completo é 054.894.927-16. Um conhecedor da regra, ao observar dígitos verificadores diferentes de 16, saberia que o CPF é falso.

Existem outras aplicações amplamente utilizadas dos chamados Sistemas de identificação, que se apoiam na Aritmética Modular: os *códigos de barras* e o *ISBN* dos livros são dois exemplos, que acabam criando um sistema simples e preciso, independente da língua, utilizando apenas a linguagem dos números, que é universal.

4.2 Criptografia

Há outras aplicações menos populares da Aritmética Modular, mas que possuem um caráter motivador e didático interessante. Uma delas é a chamada *criptografia*, que tem como propósito o envio de mensagens a um destinatário final, sem que intermediários sejam capazes de interpretá-la. Há vários níveis de complexidade para produzir mensagens criptografadas, mas nos prenderemos a casos simples que se utilizam da Aritmética Modular. Por exemplo, o que está escrito abaixo?

“HNCOGPIQ JGZC ECORGCQ DTCUKNGKTQ”

Sem uma chave que faça a correspondência com as letras corretas fica difícil dizer de imediato. Poderíamos até conseguir fazê-lo por tentativas, mas seria uma tarefa cansativa. Porém conhecendo a chave e a sequência do alfabeto

posição da letra correta = posição da letra utilizada – 2

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

torna-se muito simples decodificar a mensagem, que na verdade é

"FLAMENGO HEXA CAMPEÃO BRASILEIRO"

Na verdade, o processo descrito acima consiste em transformar a letra em seu número correspondente no alfabeto e efetuar a congruência $L-2 \equiv L_R \bmod 26$, sendo L a letra exibida e L_R a letra real.

4.3 Como descobrir o dia da semana em que alguém nasceu?

Outra das aplicações com caráter motivador é, dada uma data, descobrir que dia da semana caiu. Aos olhos dos leigos, parece obra de adivinhação ou de uma memória formidável, mas na verdade se trata de um processo que se baseia em uma congruência módulo 7.

Observando um calendário antigo, podemos ver que o dia 1^o de janeiro de 1900 caiu em uma segunda-feira. Utilizaremos esse dia como ponto de partida, pois é bastante improvável que alguém que nos questione sobre o dia da semana de seu nascimento tenha nascido antes dessa data.

Como um ano não bissexto tem 365 dias e $365 \equiv 1 \bmod 7$, significa que uma data cai um dia da semana depois no ano seguinte, para anos não bissextos.

Para descobrirmos a quantidade de anos bissextos (múltiplos de 4 mas não de 100, a exceção de ser múltiplo de 400) pós 1900, basta dividirmos o quanto o ano exceder 1900 por 4: o quociente exato será quantos anos bissextos ocorreram no período e, para esses anos, $366 \equiv 2 \bmod 7$, ou seja, no ano seguinte a mesma data cai dois dias da semana à frente.

Resumindo, dado um ano, já somos capazes de descobrir quando caiu 1^0 de janeiro nesse ano. Basta somar (ano – 1900) com a quantidade de anos bissextos, para descobrirmos "quantos dias para frente" a data se deslocou.

Encontrando esse número, basta dividi-lo por 7 e o resto dará o deslocamento de dias da semana. Por exemplo, no ano de 2013:

$$(2013-1900)+\left[\frac{113}{4}\right]=141$$

que dividido por 7, deixa resto 1. Logo ocorreu apenas um deslocamento, ou seja, 1º de janeiro de 2013 caiu em uma terça-feira.

JANEIRO						
Dom	Seg	Ter	Qua	Qui	Sex	Sáb
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

http://www.calendario2013.com.br/

Em relação ao deslocamento provocado pelo mês, devemos entender a tabela abaixo, formulada para anos não bissextos.

Tabela dos meses			
Janeiro	0	Julho	6
Fevereiro	3	Agosto	2
Março	3	Setembro	5
Abril	6	Outubro	0
Maio	1	Novembro	3
Junho	4	Dezembro	5

O mês de janeiro desloca 1º de fevereiro em 3 dias da semana para frente, pois são 31 dias e dividindo por 7, obtemos 4 semanas e 3 dias. O mês de fevereiro, para anos não bissextos, não provoca deslocamento, pois são exatas 4 semanas. O mês de março provoca 3 dias de deslocamento em abril, pelo mesmo motivo citado para janeiro. Já são 6 dias acumulados de deslocamento. O mês de abril provoca 2 dias de deslocamento em maio, pois são 30 dias e, dividindo por 7, são 4 semanas e 2 dias. São 8 dias de deslocamento acumulados, e 8 dividido por 7 deixa resto 1, ou seja,

efetivamente o deslocamento na data da semana é de um dia. E assim por diante.

Assim, estamos capacitados a descobrir quando foi o dia 1^o em um referido mês de um ano. Por exemplo, o dia 1^o de fevereiro de 2013 caiu em uma sexta, pois 1^o de janeiro de 2013 foi terça e o mês de janeiro provoca 3 dias de deslocamento em fevereiro (vide tabela): terça mais três dias resulta em sexta.

FEVEREIRO						
Dom	Seg	Ter	Qua	Qui	Sex	Sáb
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

http://www.calendario2013.com.br/

Em relação ao deslocamento provocado pelo dia, observe que tomando dia 1^o como referência, a cada 7 dias voltamos a cair no mesmo dia da semana. Então os dias 8, 15, 22 e 29 (exceto fevereiro não bissexto) serão o mesmo dia da semana que o dia 1^o. É de simples observação então que sendo *n* o dia, *n – 1* é múltiplo de 7 e cai no mesmo dia da semana que o dia 1^o. Assim, o resto deixado na divisão de *n – 1* por 7 sinaliza o número de deslocamento nos dias da semana provocado pela data. Por exemplo, 13 de fevereiro de 2013 foi uma quarta, pois 1^o de fevereiro de 2013 caiu em uma sexta e 13 – 1 = 12 deixa resto 5 na divisão por 7, e 5 deslocamentos aplicados a sexta resultam em quarta-feira.

Mas seria pouco estimulante apresentar esta justificativa aos alunos para depois utilizá-la, pois deixaria de os instigar quanto a motivação. Primeiro devemos aplicá-la repetidas vezes para aproveitar a curiosidade dos alunos para justificá-lo. Um rápido roteiro para fazer mentalmente esse processo seria:

"Para encontrar o dia da semana que caiu a data ***A/ B/ C****, faça:*

1^o) Encontre x = C – 1900;

2^o) Encontre y, a parte inteira do quociente de x por 4;

3º) Encontre z, recordando da tabela dos meses;

4º) Encontre w, tal que seja o resto da divisão de n - 1 por 7, ou seja, $w \equiv n-1 \bmod 7$ *e*

5º) Calcule x + y + z + w= r, divida por 7 e obtenha seu resto. Esse número indica o número de deslocamentos em relação à segunda feira. Ou seja, $x+y+z+w \equiv r \bmod 7$*."*

Que dia da semana foi 20 de julho de 1984?

1º) 1984 – 1900 = 84

2º) 84 dividido por 4 resulta na parte inteira 21

3º) pela tabela, julho vale 6

4º) 20 -1= 19, que dividido por 7 gera resto 5

5º) 84 + 21 + 6 + 5 = 116, que dividido por 7 deixa resto 4.

Aplicando 4 deslocamentos à segunda feira, observamos que 20 de julho de 1984 foi uma sexta feira.

Julho 1984

Nº	Se	Te	Qu	Qu	Se	Sá	Do
26							1
26	2	3	4	5	6	7	8
27	9	10	11	12	13	14	15
28	16	17	18	19	20	21	22
29	23	24	25	26	27	28	29
30	30	31					

http://www.calendario-365.com.br/calend%C3%A1rio-1984.html

Os exemplos citados, relativos a sistemas de identificação, criptografia e descoberta de dia da semana de uma determinada data, mostram-se contextualizados e condizentes com a faixa etária dos alunos das séries finais do ensino fundamental. São de fácil compreensão e não exigem conhecimentos matemáticos fora das operações fundamentais, ou seja, são uma ótima oportunidade para introduzir e mostrar a relevância da "Teoria das Congruências".

5. A ARITMÉTICA MODULAR NOS CONCURSOS DE ADMISSÃO ÀS ESCOLAS MILITARES DE NÍVEL MÉDIO

Os concursos de acesso ao nível médio das Escolas Militares abordam questões ligadas à divisibilidade com frequência. Algumas delas são facilmente resolvidas através da maneira tradicionalmente ensinada, porém outras se tornam bastante trabalhosas. Assim a Teoria das Congruências mostra-se útil como ferramenta facilitadora da aprendizagem da divisibilidade, pois apresenta soluções comparativamente sucintas, ou seja, menos cansativas e trabalhosas.

1. (Colégio Militar de Fortaleza – 2011) Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:

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

Solução tradicional:

$$\rightarrow \left.\begin{matrix} a = 7q + 6 \\ b = 7q' + 5 \end{matrix}\right| \rightarrow somando - os:$$

$$\rightarrow a + b = 7q + 7q' + 6 + 5 = 7(q + q') + 11 = 7(q + q') + 7 + 4$$

$$= 7(q + q' + 1) + 4, ou\ seja,\ deixa\ resto\ 4.$$

Solução via aritmética modular:

$$\rightarrow \left.\begin{matrix} a \equiv 6 \bmod 7 \\ b \equiv 5 \bmod 7 \end{matrix}\right| \rightarrow somando - os\ (utilizando\ III)$$

$$\rightarrow a + b \equiv (6 + 5) \bmod 7 \rightarrow a + b \equiv 11 \bmod 7$$

$$\rightarrow 11\ dividido\ por\ 7\ deixa\ resto\ 4.$$

2. (Colégio Naval – 2007) Qual será o dia da semana na data 17 de setembro de 2009?

a) segunda-feira b) terça-feira c) quarta-feira

d) quinta-feira e) sexta-feira

Solução tradicional:

A prova do Colégio Naval neste ano ocorreu em um domingo, dia 29 de julho de 2007; logo esta data funcionava como referência para os candidatos.

Contando os dias que faltam para terminar o ano de 2007, obtemos: 2 + 31 + 30 + 31 + 30 + 31 = **155** dias; o ano de 2008, que foi bissexto, teve então **366** dias e, o no ano de 2009, foram 31 + 28 + 31 + 30 + 31 + 30 + 31 + 31 + 17 = **260** dias. Então no total são 155 + 366 + 260 = 781 dias.

Ao dividir 781 por 7 encontramos quociente 111 e resto 4, significando que se passaram 111 semanas completas e mais 4 dias. Passando exatamente 111 semanas, voltaríamos à um domingo e, com os quatro dias a mais, encontramos ***quinta – feira***.

Solução via aritmética modular:

Segundo **4.3**:

1^o) x = 2009 – 1900 = 109

2^o) 109 dividido por 4 dá quociente y = 27

3^o) z = 5, referente ao mês de setembro.

4^o) 17 – 1 = 16. Logo o resto na divisão por 7 é 2, e então w = 2.

5^o) x + y + z + w= 143, que dividido por 7 deixa resto 3. Esse número indica o número de deslocamentos em relação à segunda-feira, ou seja, 17 de setembro de 2009 cairá em uma ***quinta-feira.***

Observe que na segunda solução tornou-se desnecessário saber o dia e o dia da semana da realização da prova para resolver a questão. O método utilizado funcionaria com a mesma eficiência para datas mais distantes da data da prova, enquanto a solução tradicional se tornaria cada vez mais trabalhosa.

3. (Colégio Naval – 2011) É correto afirmar que o número $5^{2011} + 2 \times 11^{2011}$ é múltiplo de:

a) 13 b) 11 c) 7 d) 5 e) 3

Não há maneira evidente de resolver tal questão sem utilizar as propriedades operatórias da aritmética modular, apesar de se tratar de uma prova que, na teoria, aborda apenas conteúdos de ensino fundamental.

Solução via aritmética modular:

→Utilizando as alternativas como base, observamos na letra (e) que $5 \equiv 2 \bmod 3$ e $11 \equiv 2 \bmod 3$, pois utilizando (**I**) tem-se que 5 – 2 = 3 e 11 – 2 = 9, ambos divisíveis por 3.

→Utilizando (**VI**), obtemos: $\begin{cases} 5 \equiv 2 \bmod 3 \rightarrow 5^{2011} \equiv 2^{2011} \bmod 3 \\ 11 \equiv 2 \bmod 3 \rightarrow 11^{2011} \equiv 2^{2011} \bmod 3 \end{cases}$.

→Substituindo na expressão: $5^{2011} + 2 \times 11^{2011} \equiv 2^{2011} + 2 \times 2^{2011} \bmod 3$

→Colocando 2^{2011} em evidência:

$2^{2011} + 2 \times 2^{2011} \equiv 2^{2011} \times (1+2) \bmod 3 \rightarrow 2^{2011} + 2 \times 2^{2011} \equiv 2^{2011} \times 3 \bmod 3.$

→Utilizando **(V)** e o fato de que $3 \equiv 0 \bmod 3$, obtemos:

$2^{2011} \times 3 \equiv 2^{2011} \times 0 \bmod 3 \rightarrow 2^{2011} \times 3 \equiv 0 \bmod 3.$

Então a expressão é divisível por 3.

Por tentativas, para todas as outras alternativas encontramos números que não dividem a expressão.

4. (Colégio Naval – 2003) O resto da divisão de $5^{131} + 7^{131} + 9^{131} + 15^{131}$ por 12 é igual a:

a) 0 b) 2 c) 7 d) 9 e) 11

Novamente, não há maneira evidente de resolver tal questão sem utilizar as propriedades operatórias da aritmética modular, apesar de se tratar de uma prova que, na teoria, aborda apenas conteúdos de 1º grau.

Solução via aritmética modular:

→Utilizando **(I)**, obtemos: $\begin{cases} 5 \equiv -7 \bmod 12 \\ 9 \equiv -3 \bmod 12 \\ 15 \equiv 3 \bmod 12 \end{cases}$.

→Substituindo na expressão:

$$5^{131} + 7^{131} + 9^{131} + 15^{131} \equiv (-7)^{131} + 7^{131} + (-3)^{131} + 3^{131} \bmod 12$$

→Observe que os termos se anulam e, então:

$5^{131} + 7^{131} + 9^{131} + 15^{131} \equiv 0 \bmod 12$.

Logo a expressão deixa resto ***zero*** ao ser dividida por 12.

Estes são alguns exemplos que ilustram a utilidade do ensino da aritmética modular como ferramenta para o Ensino Fundamental, pois esta já vem sendo cobrada de forma implícita, em questões que sem sua utilização exigem malabarismos matemáticos que poucos alunos possuem a perspicácia de enxergar.

Tomando como exemplo turmas preparatórias para os concursos militares de acesso ao nível médio, tal conteúdo já é estudado em grande parte das instituições, criando assim uma vantagem para seus alunos em detrimento dos alunos do ensino regular. Até itens como os Teoremas de Fermat e Euler são vistos.

Assim, devido a uma vasta aplicabilidade e a simplicidade do conteúdo, inserir uma “Introdução à Aritmética Modular” nas séries finais do Ensino Fundamental se mostra muito coerente.

6. CONCLUSÃO

As proposições básicas da Aritmética Modular apresentadas se mostraram de fácil entendimento, mesmo se tratando de um púbico jovem, na faixa dos 14 anos, pois envolvem apenas as operações fundamentais. Uma vez compreendidas as proposições, uma gama de regras de divisibilidade, antes apresentadas de forma obscura e sem justificativas pertinentes, passam a ser bastante claras. Além disso, criam suporte para investigação de outras regras, não necessariamente apresentadas pelo professor.

Aplicações no cotidiano como os Sistemas de Identificação e Criptografia, aliado a “truques” interessantes como descobrir o dia da semana de nascimento de uma pessoa, criam um ambiente propício para o ensino contextualizado da Teoria das Congruências.

A união de um arcabouço teórico condizente com o que se deve ensinar e a fácil contextualização atendem a atual tendência de ensino da matemática básica: raciocínio em detrimento de memorização, aplicabilidade em lugar de profundidade. Assim, apresentadas e fundamentadas as justificativas, a inserção do tópico “Introdução a Aritmética Modular” nas séries finais do Ensino Fundamental mostra-se coerente, pois desenvolve o raciocínio lógico e se torna uma ferramenta para futuras conjecturas por parte dos alunos. Além disso, atingimos o objetivo de esquematizar um material passível e interessante de ser utilizado em formação inicial e continuada de docentes, e que também pode ser usado em sala, com atividades adequadas ao público alvo.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, RPM, *Revista do Professor de Matemática.* Volumes 12 e 45. Sociedade Brasileira de Matemática.

BUCHMANN, J. *Introdução à Criptografia.* São Paulo: Berkeley, 2002.

BURNETT, S. **& PAINE,** S. *Criptografia e Segurança: o Guia Oficial RSA.* São Paulo: Campus, 2002.

CRATO, N,. Alice e Bob. *Expresso / Revista*, 22 de Setembro, pp. 118-120. (2001)

MARTINI, R. *Criptografia e Cidadania Digital.* Rio de Janeiro: Ciência Moderna, 2001.

SINGH, S. *O Livro dos Códigos.* São Paulo: Record, 2001.

TERADA, R. *Segurança de Dados: Criptografia em Redes de Computadores.* São Paulo: Edgard Blucher, 2000.

HEFEZ, Abramo. Elementos da Aritmética, 2ª edição, SBM, 2005.