Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Departamento de Matemática
Mestrado Profissional de Matemática em Rede Nacional - PROFMAT

CONGRUÊNCIA MODULAR NO ENSINO BÁSICO

Rosiane Barros Ferreira

Janeiro de 2018

São Luis - MA

Rosiane Barros Ferreira

CONGRUÊNCIA MODULAR NO ENSINO BÁSICO

Dissertação apresentada ao Programa de Pós-graduação PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) na Universidade Federal do Maranhão oferecido em associação com a Sociedade Brasileira de Matemática, como requisito para obtenção do Título de Mestre em Matemática.

Janeiro, 2018

São Luis - MA

Elaborada pela Biblioteca da Universidade Federal do Maranhão

Ferreira, Rosiane Barros

Congruência modular no Ensino Básico

Rosiane Barros Ferreira . 2018. 46f.

Impresso por Computador (Fotocopia)

Orientadora: Valdiane Sales Araújo

Dissertação (Mestrado) – Universidade Federal do Maranhão, Programa de Mestrado Profissional em Rede Nacional, 2018.

1.Congruêcia 2.Aritmética Modular 3.Matemática 4. Resolução de problemas

I. Titulo.

Rosiane Barros Ferreira

CONGRUÊNCIA MODULAR NO ENSINO BÁSICO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT) do Departamento de Matemática da Universidade Federal do Maranhão, como parte dos requisitos para obtenção do título de Mestre em Matemática.

COMISSÃO EXAMINADORA

Prof(a). Dra. Valdiane Sales Araujo (Orientadora)
Universidade Federal do Maranhão

Prof. Dr. Flausino Lucas Neves Spindola
Universidade Federal do Maranhão

Prof. Dr. José Antonio Pires Ferreira Marão
Universidade Estadual do Maranhão

São Luis

2018

AGRADECIMENTO

A Deus por sua infinita bondade e inúmeras bênçãos recebidas.

A minha família e amigos que sempre mantiveram-me em suas orações, em especial, ao meu pai Dilermando e minha mãe Rutinéa, que trabalham todos os dias para garantir os meus estudos e o futuro dos meus três amados irmãos.

Ao colega e namorado professor Orlando que nunca mediu esforços para ajudar-me sendo sempre muito companheiro.

A turma PROFMAT 2015, pelo companheirismo e amizade em todos os momentos. Com eles o caminho tornou-se mais leve e mais bonito, pela amizade que construímos.

Aos meus professores, de forma especial a minha orientadora Valdiane, profissional extremamente competente, lutadora e humana.

Aos meus alunos, os quais me fazem sentir realizada quando aprendem.

RESUMO

Esta dissertação aborda a Aritmética Modular como uma ferramenta possível de ser utilizada nas séries iniciais do ensino básico, a partir do sexto ano. O embasamento teórico será pautado nas propriedades operatórias elementares de congruência, com o cuidado de não excedermos ao que é realmente necessário, nesta etapa do aprendizado. Esta proposta baseia-se no fato de que, desde as séries iniciais, os alunos têm contato com conceitos relacionados a Aritmética Modular. A formalização destes conceitos tornaria possível um aprendizado mais concreto, bem como, a utilização destes conceitos na resolução de problemas dos mais variados desde os anos iniciais.

Palavras-chave: Congruência modular. Resolução de problemas. Aritmética . Ensino Básico.

ABSTRACT

This text deals with modular arithmetic as a possible tool to be used since the initial grades of elementary education, from the sixth year. The theoretical basis is based on the elementary properties of congruence. This proposal is based on the fact that, from the initial stages, students have contact with concepts related to modular arithmetic. The formalization of these concepts would make possible a more concrete learning as well as the use of these concepts in the resolution of more varied problems from the initial years.

Keywords: Modular Arithmetic, resolution problems, elementary education

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

A Teoria dos Números constitui um dos ramos mais antigos da Matemática e tem como objetivo principal o estudo das propriedades dos números em geral. Uma das suas principais vertentes é a Aritmética que é o ramo da matemática que estuda as propriedades dos números inteiros. A palavra Aritmética é proveniente do grego *arithmetiké* que significa *"ciência dos números"*.

A Aritmética se desenvolveu a partir do processo de evolução do ser humano em sociedade que, aos poucos, criou métodos de contagem. No início, para auxiliar no processo de contagem, usavam pedaços de paus, pedras e ossos para registrar quantidades. Dessa forma, a ideia de contagem surge antes mesmo da definição formal de número. Os números e os símbolos que os representavam sofreram grandes transformações ao longo dos séculos até chegarem ao modo como são conhecidos atualmente. Devido a constante evolução do ser humano e das várias atividades que este desenvolveu ao longo do tempo, entre elas o comércio, o conceito de número se ampliou surgindo então a ideia de número negativo.

Definidos os conceitos de contagem e de número aos poucos surgem sobre eles as primeiras operações que foram sendo denominadas operações aritméticas. Diferentes civilizações ao longo da história criaram a Aritmética sob denominações e roupagens diferentes utilizando essencialmente os mesmos processos matemáticos. Em algumas culturas a palavra aritmética tornou-se sinônimo de matemática.

A Aritmética se ocupa das quatro operações básicas mas, nesta dissertação daremos uma atenção especial a divisão de números inteiros e a seus respectivos restos. Neste texto ressaltaremos uma vertente da Teoria dos Números conhecida como Aritimética Modular cujas bases teóricas tiveram início por volta dos anos de 1750 com os trabalhos do matemático suiço Leonhard Euler(1707-1783). No entanto, uma das contribuições mais fecundas, a "Teoria das Congruências", foi introduzida em 1801, por *Carl Friederich Gauss*(1777-1855) um dos maiores matemáticos de todos os tempos, no seu livro *Disquisitiones Arithmeticae*, no qual deu sequência aos estudos de Euler sobre a divisão euclidiana de um inteiro por um número fixo, ao qual chamou de *módulo*. Em sua obra Gauus adotou simbologia e definições que são utilizadas até hoje.

Embora o termo Aritmética ainda seja usado em referência a *Teoria dos Números*, esta foi dividida em vários campos de estudo e o termo passou a se referir apenas ao ramo da matemática que estuda os números inteiros, suas propriedades e operações. Dessa forma, é o ramo da matemática que usamos todos os dias em tarefas do cotidiano, cálculos científicos ou negócios. A Aritmética faz parte do currículo do Ensino Fundamental e é ensinada com o objetivo de promover um embasamento teórico voltado para a produção de significados, para que assim, o estudante possa desenvolver habilidades que contribuam para sua vida social e escolar.

Apesar das muitas utilidades da Aritmética a sua aprendizagem em nossas escolas ainda não alcançou um nível satisfatório e pesquisas vêm constantemente alertando para o baixo rendimento dos alunos em matemática. Com relação ao assunto, O jornal *Opinião Estadão* divulgou recentemente um relatório, encomendado pelo movimento *Todos Pela Educação* [3], o qual revela que

> "*...de cada 100 crianças que ingressam no ensino fundamental, somente 65 concluem o ensino médio. E entre estas o panorama é ainda mais grave: apenas 7% com aprendizagem adequada em Matemática e 28% em Português. Entre essas 65, só 7 dão sequência à sua trajetória escolar e rumam para o ensino superior. O restante fica pelo caminho".(CRUZ, 2018)*

Isso nos leva a concluir que, a grande maioria dos alunos durante a sua formação inicial, do Ensino Fundamental ao Médio, deixa de aprender conceitos básicos de Matemática. Isso nos alerta para a necessidade de um ensino mais eficaz onde os alunos compreendam conceitos importantes como os conceitos aritméticos, que são essencias para a aprendizagem de outros conteúdos, e dessa forma fazer com que o ensino da matemática avance. No atual momento evolutivo do planeta não há como vivermos num país socialmente justo, economicamente mais competitivo, inovador e ético sem educação de qualidade para todos. Apesar de ser considerada área de extrema importância na formação de um cidadão pois, bem sabemos que é difícil sobreviver dignamente ou buscar equidade sem ter o domínio de competências básicas como aquelas que o ensino da matemática proporciona, o panorama atual reflete anos de descaso e negligência com o ensino da matemática e com a Educação como um todo.

Em entrevista concedida a *Revista do Professor de Matemática*, o professor Elon Lima afirma:

> " *O conhecimento matemático é, por natureza, encadeado e cumulativo. Um aluno pode, por exemplo, saber praticamente tudo sobre Proclamação da República brasileira e ignorar completamente as Capitanias Hereditárias mas, não será capaz de estudar Trigonometria se não conhecer os fundamentos da Álgebra, nem entenderá essa última se não souber as operações aritméticas, etc. Esse aspecto de dependência acumulada dos assuntos matemáticos leva à uma sequência necessária, que torna difícil pegar o bonde andando"(LIMA, 1995).*

De fato, é o conhecimento das propriedades e operações dos números inteiros proporcionados pela Aritmética que prepara o aluno para o aprendizado da Álgebra, da Geometria e outros ramos da Matemática.

Reconhecer a pertinencia do ensino das Congruências Modulares no ensino básico, foi a principal motivação para a escolha do tema Congruência Modular no Ensino Básico para esta dissertação, pois seus conceitos poderiam contribuir muito para a aprendizagem do aluno além do que, possuem diversas aplicações em problemas atuais além de estarem presentes no crescente uso das tecnologias.

Neste trabalho veremos como a Aritmética Modular, seus conceitos e propriedades contribuem para a dinâmica da vida moderna. Ela é utilizada, por exemplo, nos diferentes códigos numéricos de identificação como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, criptografias, calendários entre outros.

Devido a importância do estudo e aplicabilidade das congruências modulares que estimulam o desenvolvimento de habilidades essenciais na formação do aluno, propomos o ensino de Congruências Modulares a partir do 6^o ano do Ensino Fundamental. O conhecimento dessa teoria poderia contribuir para que a matemática se aproxime de um dos principais objetivos do ensino, nesta fase escolar, que é fazer com que os alunos sejam capazes de *"saber utilizar diferentes fontes de informação e recursos tecnológicos para adquirir e construir conhecimentos"*(BRASIL, 1998, p.7).

Dessa forma, para atingirmos este objetivo propomos fazer a introdução da teoria das Congruências Modulares através do uso de tabelas de divisibilidade, além de demonstrar algumas de suas aplicações no dia a dia para que os alunos possam perceber o quanto a Aritmética esta presente na vida das pessoas proporcionando mais praticidade.

Esta dissertação é constituida de quatro capítulos. No capítulo 1, para favorecer uma melhor compreensão do tema, trazemos para o leitor conceitos teóricos importantes e propriedades de congruência modular, o pequeno Teorema de Fermat, critérios de divissibilidade e resto de potências. No capítulo 2, apresentaremos aplicações de

congruências no Ensino Fundamental. Apresentaremos a nossa proposta de introduzir o conceito de congruência através de tabelas, como é feita pela apostila do PIC(Programa de Iniciação Cientifica da OBMEP), "Divisibilidade e Números inteiros". Mostraremos como é possível usar o relógio analógico para ensinar conceitos básicos de congruências. No capítulo 3, destacamos algumas das aplicações mais conhecidas da aritmética modular no nosso cotidiano, como por exemplo, diferentes códigos numéricos de identificação além dos dígitos verificadores de Código de Barras, CPF, CNPJ, International Standard Book Number(ISBN). No Captulo 4, faremos uma análise geral dos temas propostos bem como resaltaremos a sua relevância e aplicabilidade para o aluno do Ensino Fundamental.

Capítulo 1

Congruências

Neste capítulo apresentaremos conceitos e definições que serão utilizados nos próximos capítulos. Todas as definições e resultados apresentados aqui podem ser encontrados em Santos(2009). Também apresentaremos alguns resultados importantes inerentes à teoria como o Pequeno Teorema de Fermat, critérios de divissibilidade e restos de potências.

Definição 1. *Se a e b são inteiros dizemos que a é congruente a b módulo m, $m > 0$, se $m|(a-b)$, lê-se: "m divide $a-b$". Denotamos isto por $a \equiv b(mod\ m)$.*

Exemplo 1.1. $8 \equiv 3(mod\ 5)$, $12 \equiv 2(mod\ 10)$, $27 \equiv 1(mod\ 13)$.

Caso a congruência não se verifique escrevemos $a \not\equiv b(mod\ m)$

Proposição 1.1. *Se a e b são inteiros temos que $a \equiv b(mod\ m)$ se, e somente se, existir k tal que $a = b + km$.*

Demonstração. Se $a \equiv b(mod\ m)$ então $m|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. Reciprocamente, se existe k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, $m|(a-b)$ isto é, $a \equiv b(mod\ m)$. □

O próximo resultado nos diz que a relação de congruência, definida no conjunto dos números inteiros é uma relação de equivalência, pois ela é reflexiva, simétrica e transitiva.

Proposição 1.2. *Sejam $m \in \mathbb{Z}$, $m > 0$. Para todo a, b e $c \in \mathbb{Z}$ temos as seguintes relações de equivalência que também são propriedades das congruências:*

1. *Reflexiva: $a \equiv a(mod\ m)$.*
2. *Simétrica: se $a \equiv b(mod\ m)$ então $b \equiv a(mod\ m)$.*
3. *Transitiva: se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$ então $a \equiv c(mod\ m)$.*

Demonstração. 1. $a \equiv a \ (mod\ m) \Leftrightarrow m|(a-a) \Leftrightarrow a - a = m0$. O que prova a reflexividade da congruência, pois zero é múltiplo de qualquer número.

2. $a \equiv b(mod\ m) \Leftrightarrow a - b = km, k \in \mathbb{Z}$. Multiplicando $a - b = km$ por -1 obtemos $b - a = (-k)m$ e assim $b \equiv a(mod\ m)$. O que equivale dizer que se um dado número é divisível por m seu simétrico também o é.

3. $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$. Escrevendo na forma de igualdades temos: $a - b = k_1 m$ e $b - c = k_2 m$, com k_1 e $k_2 \in \mathbb{Z}$. Somando as equações

$$a - b + b - c = k_1 m + k_2 m$$
$$a - b + b - c = m(k_1 + k_2),$$

obtemos

$$a - c = m(k_1 + k_2)$$

que equivale a

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

□

Proposição 1.3. *Se a, b, c e m são inteiros tais que $a \equiv b(mod\ m)$, então:*

1. $a + c \equiv b + c(mod\ m)$
2. $a - c \equiv b - c(mod\ m)$
3. $ac \equiv bc(mod\ m)$

Demonstração. 1. De $a \equiv b(mod\ m)$ temos $a - b = km$ e como $a - b = (a + c) - (b + c)$ resulta que $a + c \equiv b + c(mod\ m)$.

2. Como $(a - c) - (b - c) = a - b$ e $a - b = km$ temos $a - c \equiv b - c(mod\ m)$.

3. De $a \equiv b(mod\ m)$ temos $a - b = km$ então $ac - bc = ckm$, com $c \in \mathbb{Z}$, o que implica $m|(ac - bc)$, logo $ac \equiv bc(mod\ m)$.

□

Proposição 1.4. *Se a, b, c, d e m são inteiros tais que $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então:*

1. $a + c \equiv b + d(mod\ m)$
2. $a - c \equiv b - d(mod\ m)$

3. $ac \equiv bd(mod\ m)$

Demonstração. 1. De fato, como $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, temos $a - b = k_1 m$ e $c - d = k_2 m$. Somando-se membro a membro, obtemos

$$a - b + c - d = k_1 m + k_2 m$$

$$a + c - b - d = k_1 m + k_2 m$$

$$a + c - (b + d) = (k_1 + k_2)m$$

o que resulta

$$a + c \equiv b + d(mod\ m).$$

2. Para provar o item 2 basta subtrair membro a membro $a - b = k_1 m$ e $c - d = k_2 m$ e obtemos

$$a - b - c + d = k_1 m - k_2 m$$

$$a - c - b + d = k_1 m - k_2 m$$

$$a - c - (b - d) = (k_1 - k_2)m$$

logo

$$a - c \equiv b - d(mod\ m).$$

3. Multiplicamos ambos os membros de $a - b = k_1 m$ por c e ambos os lados de $c - d = k_2 m$ por b. Obtemos $ac - bc = ck_1 m$ e $bc - bd = bk_2 m$. Basta agora somarmos membro a membro estas últimas igualdades:

$$ac - bc + bc - bd = ac - bd = (ck_1 + bk_2)m$$

o que implica

$$ac \equiv bd\ (mod\ m).$$

□

Este resultado é de grande valia, pois considerando quaisquer dois inteiros $a = k_1 m + r_1$ e $b = k_2 m + r_2$, onde r_1 e r_2 são os restos da divisão, pela Proposição temos que $a \pm b \equiv r_1 \pm r_2(mod\ m)$ o que verifica que o resto de $a \pm b$ depende apenas dos restos da divisão de a e b por m.

Proposição 1.5. *Se a, b, c e m são inteiros e $ac \equiv bc(mod\ m)$, então*

$a \equiv b(mod\ m/d)$ *onde* $d = mdc(c, m)$.

Demonstração. De $ac \equiv bc(mod\ m)$ temos $ac - bc = c(a - b) = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a - b) = k(m/d)$. Logo $(m/d)|(c/d)(a - b)$ e, como $(m/d, c/d) = 1$, temos que $(m/d)|(a - b)$ o que implica $a \equiv b(mod\ m/d)$. □

Outro resultado muito útil e importante dessa teoria é dado pela seguinte proposição.

Proposição 1.6. *Sejam a* m, $b \in \mathbb{Z}$ *com* $m > 0$. *Se* $a \equiv b(mod\ m)$, *então tem-se que* $a^n \equiv b^n(mod\ m)$.

Demonstração. A prova segue diretamente da identidade

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{k-2} + b^{k-1})$$

□

Vejamos alguns exemplos:

Exemplo 1.2. *Calcule o resto das divisões de* $15^6 + 9^{10}$, $9^{10} - 15^6$ *e* $15^6 \cdot 9^{10}$ *por 7.*

Solução. Usando as proposições apresentadas podemos obter os resultados facilmente.
Sabemos que $15 \equiv 1(mod\ 7)$ e $9 \equiv 2(mod\ 7)$.
Daí temos, $15^6 \equiv 1^6 \equiv 1(mod\ 7)$ e $9^{10} \equiv 2^{10} \equiv 1024 \equiv 2(mod\ 7)$.
Somando membro a membro as congruências acima, temos:

$$15^6 + 9^{10} \equiv 1 + 2 \equiv 3(mod\ 7)$$

.

Logo, o resto da divisão da soma $15^6 + 9^{10}$ por 7 é 3.
Da mesma forma, podemos subtrair as congruências obtidas:

$$9^{10} - 15^6 \equiv 2 - 1 \equiv 1(mod\ 7)$$

logo, o resto da divisão da diferença de $9^{10} - 15^6$ por 7 é 1.
Finalmente obtemos $9^{10} \cdot 15^6 \equiv 1 \cdot 2 \equiv 2(mod\ 7)$. □

Exemplo 1.3. *Sejam a e b dois números inteiros cujos restos da divisão por 13 são, respectivamente, 7 e 5. Determine os restos da divisão de* $a + b$, $a - b$ *e* $a \cdot b$ *por 13.*

Solução. Escrevendo os dados do problema em forma de congruência, temos

$$a \equiv 7\ (mod\ 13) \text{ e } b \equiv 5\ (mod\ 13).$$

Assim,

$$a+b \equiv 7+5 \equiv 12 \ (mod\ 13); \quad a-b \equiv 7-5 \equiv 2 \ (mod\ 13)$$

e

$$a \cdot b \equiv 7 \cdot 5 \equiv 35 \equiv 9 \ (mod\ 13).$$

Logo os restos da divisão de $a+b$, $a-b$ e $a \cdot b$ por 13 são, respectivamente, 12, 2 e 9. □

1.1 O Pequeno Teorema de Fermat

O próximo resuldado nos diz que se p é primo e p não divide a, então p divide $a^{p-1}-1$. De fato, isso é facilmente constatado se considerarmos, por exemplo, $p = 11$ e $a = 5$. Assim teremos:

$$\begin{aligned}
1 \times 5 &\equiv 5(mod 11) \\
2 \times 5 &\equiv 10(mod 11) \\
3 \times 5 &\equiv 4(mod 11) \\
4 \times 5 &\equiv 9(mod 11) \\
5 \times 5 &\equiv 3(mod 11) \\
6 \times 5 &\equiv 8(mod 11) \\
7 \times 5 &\equiv 2(mod 11) \\
8 \times 5 &\equiv 7(mod 11) \\
9 \times 5 &\equiv 1(mod 11) \\
10 \times 5 &\equiv 6(mod 11)
\end{aligned}$$

Observe que 11 não divide nenhum dos produtos que estão na coluna da esquerda nas congruências acima. Observe, também, que todos eles são incongruêntes módulo 11. Logo, como nenhum é conguente a zero módulo 11 e todos são incongruentes módulo 11 entes si, eles devem ser congruentes a diferentes números dentre 1, 2, 3, ..., 10. Observe que todos estes números aparecem, sem repetições, na coluna da direita nas congruências acima. Agora podemos multiplicar, membro amembro estas congruências e obter

$$(1 \times 5)(2 \times 5) \cdots (10 \times 5) \equiv 5 \times 10 \times 4 \times 9 \times 3 \times 8 \times 2 \times 7 \times 6(mod 11)$$

e, portanto, $5^{10}10! \equiv 10!(mod 11)$. Mas, como $mdc(10!, 11) = 1$ temos, pelo Teorema 1.5, que

$$5^{10} \equiv 1(mod 11)$$

o que mostra a validade do próximo resultado no caso particular quando $a = 5$ e $p = 11$.

Teorema 1.7 (Fermat)**.** *Se p é um número primo e $a \in \mathbb{N}$, então $a^p \equiv a \ mod \ p$ e se, além disso, a e p forem primos entre si então $a^{p-1} \equiv 1 \ (mod \ p)$.*

Demonstração. Se $a^p \equiv a \ mod \ p \Leftrightarrow p|a(a^{p-1} - 1) \Rightarrow p|a$ ou $p|(a^{p-1} - 1)$. Mas, como $p \nmid a$ tem-se $p|(a^{p-1} - 1) \Rightarrow a^{p-1} \equiv 1 \ mod \ p$. □

Vejamos a seguir alguns exemplos em que obtemos o resultado mais facilmente pela aplicação do Teorema de Fermat.

Exemplo 1.4. *Calcule o resto da divisão de 2^{100} por 7.*

Solução. Como 7 e 2 são números primos temos, pelo Teorema de Fermat, a congruência $2^6 \equiv 1 \ mod \ 7$. Dessa forma, usando o teorema e as propriedades de multiplicação e potenciação de congruências podemos chegar facilmente ao resultado. Logo, é conveniente fazer a divisão Euclidiana do expoente 100 por 6, $100 = 16 \times 6 + 4$. Elevando os dois membros da congruência $2^6 \equiv 1 \ mod \ 7$ ao expoente 16 encontramos $(2^6)^{16} \equiv 1 \ mod \ 7$ e, multiplicando-a por 2^4, obtemos:

$$(2^6)^{16} \cdot 2^4 \equiv 2^3 \cdot 2 \equiv 8 \cdot 2 \equiv 2 \ mod \ 7$$

que nos leva ao resto da divisão que é 2. □

Exemplo 1.5. *Calcule o resto da divisão de 13^{51} por 5.*

Solução. Como 13 e 5 são números primos, portanto primos entre si, temos pelo Teorema de Fermat a congruência $13^4 \equiv 1 \ mod \ 5$. Dessa forma, usando o teorema e as propriedades de multiplicação e potenciação de congruências podemos chegar facilmente ao resultado. Logo, nos é conveniente fazer a divisão euclidiana do expoente 51 por 4 o que nos fornece $51 = 12 \times 4 + 3$. E assim, elevando os dois membros da congruência $13^4 \equiv 1 \ mod \ 5$ ao expoente 12 encontramos $(13^4)^{12} \equiv 1 \ mod \ 7$ e, multiplicando-a por 13^3, obtemos: $(13^4)^{12} \cdot 13^3 \equiv 13^3 \equiv 13 \cdot 13 \cdot 13 \equiv 3 \cdot 3 \cdot 3 \equiv 27 \equiv 2 \ mod \ 5$ que nos leva ao resto 2. □

Exemplo 1.6. *Calcule o resto da divisão de 8^{75} por 11.*

Solução. Como 8 e 11 são números primos entre si, temos pelo Teorema de Fermat a congruência $8^{10} \equiv 1 \ (mod \ 11)$. Dessa forma, usando o teorema e as propriedades de multiplicação e potenciação de congruências podemos chegar facilmente ao resultado. Fazendo a divisão Euclidiana do expoente 75 por 10 temos $75 = 7 \times 10 + 5$. Agora, elevando os dois membros da congruência $8^{10} \equiv 1 \ (mod \ 11)$ ao expoente 7 encontramos $(8^{10})^7 \equiv 1 \ (mod \ 11)$ e, multiplicando a nova congruência por 8^5, obtemos $(8^{10})^7 \cdot 8^5 \equiv$

$8^5 \equiv 8^2 \cdot 8^2 \cdot 8 \equiv 64 \cdot 64 \cdot 8 \equiv (-2) \cdot (-2) \cdot 8 \equiv 32 \equiv -1 \equiv 10$ $(mod\ 11)$ que nos leva ao resto da divisão que é 10.

□

1.2 Critérios de Divisibilidade

Algumas regras nos permitem determinar se um número $n \in \mathbb{N}$ é divisível ou não por outro, e evidentemente, a um custo bem menor que efetuar a divisão. Dessa forma, as congruências associadas a escrita de todo número $n = a_r \ ... \ a_2a_1a_0$ em sua forma decimal $n = a_r10^r + \ ... \ + a_210^2 + a_110^1 + a_0$ é uma ferramenta muito útil na determinação dos **critérios de divisibilidade**. Descreveremos a seguir algumas dessas regras.

1.2.1 Divisibilidade por 2 e por 5

A partir da escrita decimal de n, podemos colocar 10 em evidência a partir do algarismo das dezenas e escrever: $n = (a_r10^{r-1} + \ ... \ + a_210^1 + a_1)10 + a_0$, onde a_0 é o algarismo das unidades. Observando, que no segundo membro o primeiro valor é divisível por 2, 5 e 10. Portanto, para um n qualquer sua divisão por 5 ou por 2 só vai depender do seu algarismo das unidades e, dessa forma, temos dois casos a considerar:

- Se a_0 for 0 ou 5, n é divisível por 5, logo: *todo número que termina em 0 ou 5 é divisível por 5.*
- Se a_0 for 0, 2, 4, 6 ou 8, n é divisível por 2, logo: *todo número que termina em 0, 2, 4, 6 ou 8 é divisível por 2.*

1.2.2 Divisibilidade por 3 e por 9

Inicialmente temos as seguintes congruências:

$$\begin{gathered} 10 \equiv 1\ mod\ 3 \text{ e } 10 \equiv 1\ mod\ 9 \\ 10^2 \equiv 1\ mod\ 3 \text{ e } 10^2 \equiv 1\ mod\ 9 \\ 10^3 \equiv 1\ mod\ 3 \text{ e } 10^3 \equiv 1\ mod\ 9 \\ \vdots \qquad\qquad \vdots \\ 10^r \equiv 1\ mod\ 3 \text{ e } 10^r \equiv 1\ mod\ 9 \end{gathered}$$

o que nos diz que para qualquer valor de r, $10^r - 1$ é divisível por 3 e 9. De fato,

$$10 - 1 = 9 = 1 \times 9,$$

$$10^2 - 1 = 100 - 1 = 99 = 11 \times 9,$$

$$10^3 - 1 = 1000 - 1 = 999 = 111 \times 9,$$

$$\vdots \qquad \vdots$$

$$10^n - 1 = \underbrace{11\cdots1}_{nvezes} \times 9.$$

Agora, subtraindo de $n = a_r 10^r + \ ... \ + a_2 10^2 + a_1 10^1 + a_0$ a soma dos algarismos $a_r, \ldots, a_2, a_1, a_0$, temos:

$$\begin{aligned} n - (a_r + \ldots + a_2 + a_1 + a_0) &= a_r 10^r - a_r + \ldots + a_1 10^1 - a_1 + a_0 - a_0 \\ &= (10^r - 1)a_r + \ldots + (10^1 - 1)a_1 \end{aligned}$$

Note que a última expressão é sempre um múltiplo de 9 (e portanto, de 3). Assim, temos que n é multiplo de 9, ou de 3 se, e somente se, o número $a_r + \cdots + a_1 + a_0$ é multiplo de 9 ou de 3.

Portanto, provamos que: *um número n é divisível por 3, ou por 9, quando a soma de seus algarismos resulta em um número divisível por 3, ou por 9.*

1.2.3 Divisibilidade por 6

Observando as congruências:

$$\begin{aligned} 10 &\equiv 4 \ (mod\ 6) \\ 10^2 \equiv 16 &\equiv 4 \ (mod\ 6) \\ 10^3 \equiv 64 &\equiv 4 \ (mod\ 6) \\ \vdots &\qquad \vdots \\ 10^r &\equiv 4 \ (mod\ 6) \end{aligned}$$

Percebemos que para qualquer valor de r as potencias de base 10 deixam resto 4 na divisão por 6. Logo, podemos escrever:

$$n = (a_r 10^r + \ ... \ + a_2 10^2 + a_1 10^1 + a_0) \equiv (4a_r + \ldots + 4a_2 + 4a_1 + a_0)$$

$$n \equiv (4a_r + \ldots + 4a_2 + 4a_1 + a_0) \ (mod\ 6)$$

$$n \equiv (4(a_r + \ldots + a_2 + a_1) + a_0) \ (mod\ 6)$$

Dessa forma, fica provado que: *um número é divisível por 6 se, e somente se, o algarismo das unidades mais o produto da soma dos outros algarismos por quatro for divisível por 6.*

1.2.4 Divisibilidade por 7

Consideremos n na sua forma decimal $n = (a_r 10^{r-1} + \ ... \ + a_2 10^1 + a_1)10 + a_0$ e $b = (a_r 10^{r-1} + \ ... \ + a_2 10^1 + a_1)$. Então, podemos escrever $n = 10b + a_0$.

Da congruência $10 \equiv 3 \ (mod\ 7)$ resulta que

$$n \equiv 10b + a_0 \equiv 3b + a_0 \ (mod\ 7).$$

Podemos multiplicar a congruência acima por $-2 \equiv -2 \ (mod\ 7)$ o que resulta

$$-2n \equiv -6b - 2a_0 \ (mod\ 7).$$

Como $6 \equiv -1 \ (mod\ 7)$, podemos escrever

$$-2n \equiv b - 2a_0 \ (mod\ 7).$$

Desse modo, se n é divisível por 7 temos $0 \equiv b - 2a_0 \ (mod\ 7)$.

Daí, concluímos que: *"um número é divisível por 7 se, e somente se, o dobro do algarismo das unidades subtraído da soma dos demais algarismos resultar em um número divisível por 7".*

1.2.5 Divisibilidade por 11

Observando as congruências abaixo percebemos que o resto de uma potência de base 10 por 11 depende da paridade do expoente para ser 1 ou -1.

$$\begin{aligned} 10 &\equiv -1 \ (mod\ 11) \\ 10^2 &\equiv +1 \ (mod\ 11) \\ 10^3 &\equiv -1 \ (mod\ 11) \\ \vdots \qquad &\qquad \vdots \\ 10^r &\equiv +1 \ (mod\ 11) \end{aligned}$$

Logo, se n é divisível por 11, pelas congruências acima podemos escrever n da seguinte forma

$$n = (a_r 10^r + \ ... \ + a_2 10^2 + a_1 10^1 + a_0) \equiv (a_r - a_{r-1} + \ldots - a_3 + a_2 - a_1 + a_0) \ (mod\ 11)$$

Assim,

$$n \equiv (a_r - a_{r-1} + \ldots - a_3 + a_2 - a_1 + a_0) \ (mod\ 11)$$

o que podemos escrever ainda como

$$n \equiv (\ldots + a_4 + a_2 + a_0) - (\ldots a_5 + a_3 + a_1) \ (mod\ 11).$$

Portanto, *"um número n é divisível por 11 se, e somente se, o número* $a_0 - a_1 + a_2 - \cdots$ *é divisível por 11."*

Outros critérios de divisibilidade podem ser deduzidos a partir de congruências.

1.3 Congruência Modular e fenômenos periódicos

A Congruência Modular é uma ferramenta poderosa na resolução de problemas envolvendo fenômenos periódicos. Os exemplos a seguir mostram como o uso congruência e suas propriedades podem simplificar a resolução de problemas envolvendo tempo.

Exemplo 1.7 (Encontros de Aritmética)**.** *Ana decidiu nadar de três em três dias. O primeiro dia que ela nadou foi sábado, o segundo dia foi terça-feira, o terceiro dia foi uma sexta-feira, e assim por diante. Em qual dia da semana Ana estará nadando pela centésima vez?*

Solução. Na tabela a seguir, listamos os dias da semana que Ana está nadando pelas primeiras 21 vezes.

dom	seg	ter	qua	qui	sex	sab
6	4	2	7	5	3	1
13	11	9	14	12	10	8
20	18	16	21	19	17	15

Analisando a tabela vemos que os múltiplos de 7 sempre estão na quarta-feira, que os números que deixam resto 1 quando divididos por 7 estão no sábado e que os números que deixam resto 2 quando divididos por 7 estão na terça-feira. Dividindo 100 por 7 obtemos quociente 14 e resto 2 ($100 = 14 \times 7 + 2$). Daí concluímos que na centésima vez, Ana estará nadando em uma terça-feira.

Solução utilizando congruência

Podemos resolver o problema de maneira mais fácil. Basta utilizar congruência *mod* 7,

pois a semana tem 7 dias. Assim,

$$100 \equiv a(mod\ 7)$$

fazendo a divisão de 100 por 7 encontramos $a = 2$. Isso significa que Ana nadará pela centésima vez no mesmo dia da semana em que nadou pela segunda vez, ou seja, terça-feira.

□

Um fato surpreendente, principalmente para as pessoas mais leigas em matemática, é constatar a facilidade "extraordinária"de alguns indivíduos em calcular o dia da semana em que ocorreu algum evento passado, como data de nascimento e fatos históricos. Alguns indivíduos, até mesmo, deixam transparecer a outros que se trata de um dom especial, como se fossem "adivinhas" ou, no mínimo, detentores de uma memória formidável. Mas, na verdade, o que provavelmente ocorre, é o conhecimento de algum algorítmo por parte do individuo, através do qual, sem grandes dificuldades, ele consegue calcular o dia da semana em que ocorreu qualquer data passada, bastando para isso, ter alguns conhecimentos, como:

- Conhecer o dia da semana em que ocorreu alguma data anterior. De preferência, saber que dia da semana foi 1^o de janeiro de algum ano anterior, a essa data chamaremos de data fixa.
- Saber que um evento, a cada ano comum(365 dias), acontece em um dia da semana a frente e que, em anos bissextos (366 dias), ocorrem dois dias a frente.

O fato se evidencia quando dividimos o número de dias de um ano em semanas. Como sabemos, uma semana completa inicia em um dado dia e termina em um dia anterior, por exemplo, se uma semana começar no domingo ela termina no sábado; se começar na terça feira termina na segunda feira, e assim segue. Logo, se um ano comum, por exemplo, se inicia em uma segunda feira, fazendo a divisão euclidiana dos 365 dias do ano pelos 7 dias de uma semana obtemos $365 = 52 \times 7 + 1$ donde concluímos que, o ano comum tem 52 semanas completas, ou seja, semanas que começam, por exemplo, na segunda feira e terminam no domingo. No entanto, como a divisão não é exata, o resto 1, indica que além das 52 semanas ainda há um dia a mais a ser cumprido e, no caso, do nosso ano hipotético ocorre na segunda. Portanto, todo ano comum começa e termina no mesmo dia da semana, dessa forma, o próximo ano vai iniciar um dia a frente, ou seja, começará na terça e terminará na terça, se for comum. Pelo mesmo motivo, os anos bissextos, que deixam resto 2 na divisão dos 366 dias por 7, iniciam em um determinado dia da semana

e terminam um dia após, ou seja, dois dias após o último dia da semana, por exemplo, se um ano bissexto iniciar na quarta feira a semana termina na terça, logo o último dia do ano será dois dias após terça, portanto na quinta.

- Sabermos que um mês inicia em um dado dia da semana e termina tantos dias depois do último dia da semana quanto for o valor do resto da divisão do número de dias desse mês por 7. Por exemplo, os meses do ano no nosso calendário Gregoriano têm 31, 30, 29(em anos bissextos) e 28 dias. Fazendo a divisão dos 31, 30, 29 e 28 dias por 7 obtemos respectivamente: $31 = 4 \times 7 + 3$, $30 = 4 \times 7 + 2$, $29 = 4 \times 7 + 1$ e $28 = 4 \times 7 + 0$.

Dessa forma, verificamos que:

1. Se um mês de 31 dias inicia no domingo, este mês terá 4 semanas completas que se iniciarão no domingo e terminarão no sábado mais 3 dias portanto, esse mês terminará na terça feira.

2. Se um mês de 30 dias inicia no domingo, este mês terá 4 semanas completas que se iniciarão no domingo e terminarão no sábado mais 2 dias portanto, esse mês terminará na segunda-feira.

3. Se um mês de 29 dias inicia no domingo, este mês terá 4 semanas completas que se iniciarão no domingo e terminarão no sábado mais 1 dia portanto, esse mês terminará no domingo.

4. Se um mês de 28 dias inicia no domingo, este mês terá apenas 4 semanas completas que se iniciarão no domingo e terminarão no sábado. Essa observação é importante porque nos mostra que o 1^o dia da semana de cada mês, a partir do 2^o mês do ano, é "empurrado para frente" em relação ao dia da semana em que ocorreu o primeiro dia do ano, 1^o de Janeiro, de acordo com a soma dos restos da divisão por 7 do número de dias de cada mês anterior. Por exemplo, em um ano comum hipotético, onde 1^o de janeiro é um domingo, como Janeiro tem 31 dias e deixa resto 3 na divisão por 7, este mês, "empurrará" o inicio de fevereiro para três dias após o domingo(1^o de janeiro), ou seja, fevereiro iniciará na quarta-feira. Assim, fevereiro(28 dias), em anos comuns, deixa resto 0 na sua divisão por 7, isso significa que no nosso ano hipotético, este começa na quarta e termina na terça, não "empurrando para frente"o próximo mês, março, em nenhum dia, que se iniciara também na quarta-feira, pois a soma dos restos da divisão dos meses anteriores por 7, de janeiro e fevereiro, permanece $3(3 + 0 = 3)$. Se fevereiro fosse ano bissexto, como os 29 dias deixam resto 1 na divisão por 7, março iria se deslocar mais 1 dia a frente, além dos

3 dias deixados por janeiro, ou seja, o mês de março avançaria $(3+1=4)$ 4 dias após o 1^o dia do ano(domingo), portanto se começaria na quinta. Mas, continuando com um ano hipotético comum, março(31 dias) deixa resto 3 na divisão por 7, significa que somando os restos das divisões por 7 dos meses de janeiro, fevereiro e março, temos que o número de dias da semana que abril irá se deslocar é $6(3+0+3=6)$, ou seja, o 1^o dia da semana de abril é sábado.

Com certeza, os exemplos nos fizeram atentar para o fato de que os restos dos meses anteriores deslocam o dia do inicio de um dado mês em questão. Por isso, sabendo qual foi o dia da semana em que o ano se iniciou é possível calcular que dia da semana se iniciou qualquer mês posterior. Na verdade, é fácil observar que o resto da divisão de cada mês por 7 é o mesmo valor dos dias de cada mês que ultrapassa 28 dias. Dessa forma, podemos usar uma congruência módulo 7 para nos ajudar a calcular a soma dos restos do número de dias de cada mês do ano por 7 de maneira mais prática, usando o algoritmo abaixo.

$$(dias\ de\ janeiro-28)+(dias\ de\ fevereiro-28)+\cdots+(dias\ de\ dezembro-28) \equiv r(mod\ 7).$$

Vejamos um exemplo:

Exemplo 1.8. *Se 1^o de janeiro de 1984 foi domingo, que dia da semana foi 1^o de setembro do mesmo ano.*

Solução. Dado que o ano é bissexto e sabendo que os meses que antecedem setembro com seus respectivos números de dias são: Janeiro(31), fevereiro(29), março(31), abril(30), maio(31), junho(30), julho(31) e agosto(31), usando o algoritmo temos

$$(31-28)+(29-28)+(31-28)+(30-28)+(31-28)+(30-28)+(31-28)+(31-28) \equiv r\ (mod\ 7)$$

$$20 \equiv r\ (mod\ 7)$$

$$6 \equiv (r\ mod\ 7)$$

Assim, 1^o de setembro do ano de 1984 foi 6 dias após domingo, o 1^o dia do ano. Portanto foi sábado. □

Exemplo 1.9. *Se 1^o de janeiro de 2000 foi sábado, que dia da semana foi 1^o de novembro do mesmo ano.*

Solução. $(31-28)+(29-28)+(31-28)+(30-28)+(31-28)+(30-28)+(31-28)+(31-28)+(30-28)+(31-28)+(30-28)+(31-28) \equiv r(\ mod\ 7)$

$$(3+1+3+2+3+2+3+3+2+3) \equiv r\ (mod\ 7)$$

$$25 \equiv r\ mod\ 7$$

Assim,1^o de novembro do ano de 2000 ocorreu 4 dias após o sábado que foi o 1^o dia do ano. Portanto foi quarta. □

No entanto, nem sempre a data que se quer saber é o primeiro dia de um dado mês. Sendo assim, é importante lembrar que se o 1^o dia da semana, por exemplo, foi domingo, também serão domingo os dias 1, 8, 15, 22 e 29 do mesmo mês. Isso nos ajuda a nos aproximarmos da data que procuramos.

Exemplo 1.10. *O ano de 2014 começou em uma quarta-feira. Em que dia da semana cairá o último dia deste ano?*

Capítulo 2

Aritmética Modular no Ensino Fundamental

A Aritmética Modular abrange propriedades e teoremas referentes ao conjunto dos números inteiros que variam dos níveis mais elementares aos mais avançados. Neste trabalho, estamos interessados nos resultados que possibilitam resolver problemas básicos como aqueles abordados no ensino fundamnetal. Pretendemos estimular o ensino de congruência a partir do 6^o ano do ensino básico já que, nessas séries os alunos já se deparam com situações problemas que envolvem divisibilidade de números inteiros, requisito básico para o estudo de congruências. Inserir os conceitos e métodos da Congruência Modular poderia ser muito pertinente pois possibilitaria a utilização de conceitos já conhecidos sob uma nova abordagem, promovendo um aprendizado mais consistente com a realidade que lhes é apresentada hoje.

Os alunos que participam do PIC, o Programa de Iniciação Científica Jr. da OBMEP, que estudam desde o sexto ano os conceitos e propriedades referentes a Aritmética Modular, têm tido grande êxito na compreensão e aplicação de tais conceitos desenvolvendo sua capacidaade de interpretar e resolver problemas matemáticos que vão do nível elementar até problemas mais complexos.

Uma introdução bastante simples é feita pela apostila do PIC, Divisibilidade e Números Inteiros de Samuel Jurkiewicz(2006), no qual através do uso de tabelas explora vários conceitos como adição, multiplicação, divisibilidade relacionados a Congruências Modulares.

Nas séries iniciais, ao trabalhar as horas utilizando um relógio analógico o professor trabalha os fundamentos básicos da congruência modular.

A figura abaixo corresponde a um relógio analógico comum. O professor poderá colocar para os alunos questões do tipo:

Se uma pessoa começa sua jornada de trabalho às sete horas da manhã e trabalha seis

horas seguidas, que horas ela concluirá sua jornada de trabalho?

A resposta é simples, se a pessoa começou a trabalhar as sete horas da manhã e trabalhou seis horas seguidas, ela terminará as treze horas.

Note que treze horas é **equivalente** a uma hora no relógio. Da mesma forma, se a pessoa tiver iniciado seu turno de trabalho as oito horas da manhã ela terminará as quatorze horas, ou seja, as 2:00 horas da tarde. Assim, temos as seguintes relações de congruência:

$$13 \equiv 1(mod\ 12) \quad e \quad 14 \equiv 2(mod\ 12)$$

Figura 2.1: Relógio analógico
Fonte:https://pixabay.com/relógios-analógicos

O conceito de *Congruência* pode ser introduzindo de forma bastante natural através do uso de tabelas. Na tabela 2.1 estão distribuídos os números naturais que vão de 0 a 54 organizados em colunas de acordo com o valor de seus respectivos restos na divisão euclidiana por 5. Os números que deixam restos iguais estão organizados na mesma coluna.

Observa-se facilmente que a primeira coluna é a coluna dos múltiplos de 5 incluindo o 0, ou seja, nessa coluna estão todos os valores que deixam 0 como resto na sua divisão por 5. Dessa forma, percebe-se que as demais colunas formam conjuntos numéricos que deixam como resto de sua divisão por 5 os valores 1, 2, 3 e 4, que são os possíveis restos de uma divisão por 5.

Depois de compreendido pela turma a distribuição dos números na tabela, o professor poderá fazer questionamentos como por exemplo:

1. Em que coluna você colocaria os valores 75, 61, 72, 83 e 94 ?
2. Fazendo a adição entre dois números da mesma coluna em que coluna ficaria o resultado?
3. Fazendo a adição entre dois números de colunas diferentes em que coluna ficaria o resultado?

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
30	31	32	33	34
35	36	37	38	39
40	41	42	43	44
45	46	47	48	49
50	51	52	53	54

Tabela 2.1: Tabela de divisibilidade por 5

4. Fazendo a subtração entre um valor maior e um menor da mesma coluna em que coluna ficaria o resultado?

5. Quais números ficariam imediatamente abaixo da última linha?

Como vimos, o uso de tabelas pode ajudar a compreender e a formalizar conceitos relativos à Congruência Modular. Usando os valores de uma tabela de restos como a do exemplo 2.1. Denominando o divisor em questão como *módulo*, e tirando dois valores quaisquer de uma mesma coluna podemos estabelecer a congruência entre esses dois valores. Por exemplo, 52 e 12 pertencem a mesma coluna, por isso podemos conceituar 52 e 12 como números congruentes módulo 5, já que deixam restos iguais na divisão por 5. Isso pode ser representado por $52 \equiv 12(mod\ 5)$. Assim, introduz-se a notação formal de congruência entre dois números.

2.1 Adição Modular

Depois de compreender os fundamentos da Congruência Modular, os alunos estarão aptos a dar um passo à frente. Poderão efutar operações, não apenas com números inteiros, mas também com símbolos que os representem.

No Capítulo 2 vimos que, se $a \equiv r_1(mod\ d)$ e $b \equiv r_2(mod\ d)$, então $a + b \equiv r_1 + r_2(mod\ d)$. Assim, o resto da soma de dois valores na divisão por um número d depende apenas da soma de seus restos:

$$a + b \equiv r_1 + r_2 \equiv r(mod\ d)$$

Para ilustrar essa propriedade é interessante a construção e o uso de tabelas de adição de restos, como a tabela a 2.2, onde estão representados os possíveis restos deixados pela

divisão da soma de dois números naturais quaisquer, a e b, por um divisor $d > 0$, isso facilita o cálculo de resultados e soluções de problemas.

Na tabela 2.2, estão representados todos os possíveis restos da divisão de uma soma $(a + b)$ por 5. Observe que o traço acima dos valores $(\bar{r})$ indica que não se trata dos valores usuais, mas sim da representação de um valor qualquer que deixa "resto r"por um dado divisor d, no caso da tabela a seguir $d = 5$. No exemplo a seguir o símbolo $\bar{2}$ está representando qualquer valor que deixa resto 2 na divisão por 5.

$+ \bmod 5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Tabela 2.2: Tabela de adição mod 5

Note que os resultados da adição, utilizando números $\bar{a}$ e $\bar{b}$ da tabela, são diferentes daqueles que encontraríamos utilizando a aritmética dos números inteiros. Por exemplo, na tabela acima, $\bar{1} + \bar{4} = \bar{0}$.

Exemplo 2.1. *Vamos calcular o resto da soma 45 + 34 + 78 + 98 por 5 e verificar a que coluna, na tabela 2.2, pertenceria este resultado.*

Solução. Utilizando as Proposições vistas no Capítulo 1 podemos fazer a soma dos valores aos pares. Somando $45 + 34 = 79$. Na tabela, o número 79 ficaria na coluna , pois o resto na divisão por 5 é 4. Somando $78 + 98 = 176$. Na tabela, o número 176 estaria na coluna , pois o resto na divisão por 5 é 1. Como a soma é $4 + 1 = 5$ o resto é 0 e portanto o valor da soma ficaria na coluna .

□

2.2 Multiplicação Modular

No Capítulo 1 vimos que, se $a \equiv r_1 \ (mod\ d)$ e $b \equiv r_2 (mod\ d)$, então $a \times b \equiv r_1 \times r_2 (mod\ d)$. Assim, o resto da multiplicação de dois valores na divisão por um número d depende apenas da multiplicação de seus restos:

$$a \times b \equiv r_1 \times r_2 \equiv r\ mod\ d.$$

$\times$ mod 5	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tabela 2.3: Tabela de multiplicação mod 5

Para o estudo da multiplicação pode ser construida uma tabela de restos semelhante àquela construida no caso da adição. Nela podem ser encontrados todos os possíveis restos da multiplicação de dois números, na divisão por d, usando apenas a multiplicação de seus restos. A tabela 2.3, de multiplicação módulo 5, apresenta os restos das divisões dos produtos de dois números por 5.

Exemplo 2.2. *Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine o resto da divisão de $a \times b$ por 7.*

Solução. Como vimos anteriormente o resto da divisão dependerá apenas de 2 e 6 pois,

$$a \equiv 6(mod\ 7) \text{ e } b \equiv 2(mod 7)\text{assim}, a \times b \equiv 2 \times 6 \equiv 12 \equiv 5(mod\ 7).$$

Portanto o resto da divisão é 5. □

2.3 Resolução de problemas utilizando Congruência Modular

Embora este tema não faça parte da grade curricular obrigatória das escolas brasileira, muitas provas nacionais de olimpíadas e concursos trazem problemas que sugerem o uso de congruência modular em suas resoluções. A seguir listaremos algumas questões de provas nacionais que abordam este tema.

Exemplo 2.3. *(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. A prova do Colégio Naval naquele ano ocorreu em um domingo, dia 29 de julho de 2007; vamos usar essa data como referência para os candidatos. Contando os dias que faltam para encerrar o ano de 2007, obtemos: $2 + 31 + 30 + 31 + 30 + 31 = 155$ dias, mais os 366 dias de 2008, mais os dias de 2009 até chegar a 17 de setembro que são: $31 + 28 + 31 + 30 + 31 + 30 + 31 + 31 + 17 = 260$ dias; somam um total de 781 dias, que agrupados de

de 7 em 7 dias, a partir de 29 de julho voltam a cair em um domingo. Portanto, podemos resolver o problema por congruência modular. Assim, obtemos $781 \equiv 4(mod 7)$. O que indica que a partir de 29 de julho de 2007 houve 111 semanas completas, que começaram em um domingo e mais 4 dias. Portanto, 17 de setembro de 2009 ocorreu 4 dias após o domingo, portanto ocorreu em uma quinta-feira. □

Exemplo 2.4. *(Colégio Militar de Fortaleza -2011)Dois números inteiros positivos são tais que a divisão do primeiro 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. Tomemos a e b para representar os números citados no problema e vamos indicar seu respectivos restos pela divisão por 7 na forma de congruência:
$a \equiv 6(mod\ 7)$ e $b \equiv 5(mod\ 7)$. Das propriedades das congurências segue que: $a + b = 6 + 5 = 11 \equiv 4(mod\ 7)$. Portanto, somando os dois números e dividindo por 7, o resto é 4. □

Exemplo 2.5. *(XXIV COM-2004)Sejam a, b, c três inteiros positivos tais que $a^2+b^2 = c^2$. Mostre que um deles é múltiplo de 4.*

Solução. Suponha que nenhum deles é divisível por 4. Então estes números são da forma $4k + 1, 4k + 2, 4k + 3$. Elevando cada uma destas expressões ao quadrado obtemos:

$$(4k + 1)^2 = 16k^2 + 8k + 1 \equiv 1(mod\ 8)$$
$$(4k + 2)^2 = 16k^2 + 16k + 4 \equiv 4(mod\ 8)$$
$$(4k + 3)^2 = 16k^2 + 24k + 9 \equiv 1(mod\ 8)$$

Daí, podemos concluir que $a^2, b^2, c^2 \equiv 1, 4(mod\ 8)$. Segue que $a^2 + b^2 \equiv 1 + 1, 1 + 4, 4 + 1, 4 + 4 \equiv 2, 5, 0(mod\ 8)$, o que é um absurdo , pois c_2 não pode assumir nenhum destes valores módulo 8. Logo, um dos números deve ser múltiplo de 4.

□

Exemplo 2.6. *(OBMEP 2^a fase, 2017) Joana retira bolas, sem reposição, de uma caixa com 2017 bolas numeradas de 1 a 2017.*
a) Qual é a quantidade mínima de bolas que ela deve retirar para garantir que pelo menos em uma delas haja um número múltiplo de 3?
b) Qual a quantidade mínima de bolas que ela deve retirar para garantir que existam duas bolas com a soma de seus números igual a um múltiplo de 3?
c) Qual é a quantidade mínima de bolas que ela deve retirar para garantir que existam duas bolas de modo que a soma de seus números seja um múltiplo de 3 e sua diferença seja um múltiplo de 2?

Solução. (a) Podemos separar as bolas em três conjuntos que deixam resto 0, 1 , ou 2, na divisão por 3. Vamos chamar esses conjuntos de A, B e C, respectivamente. Como $2017 = 3\times672+1$, A tem 672 elementos, B tem 673 e C tem 672. Podemos analisar o "pior cenário", isto é, procurar o número máximo de bolas em que nenhuma bola retirada possui número múltiplo de 3. Se pegarmos todas as bolas dos conjuntos B e C, um total de 1345 bolas, não teremos nenhum múltiplo de 3. A próxima bola, portanto necessariamente será do grupo A, que é o grupo dos múltiplos de 3. Assim, se pegarmos 1346 bolas teremos de pegar do grupo A, necessariamente. Portanto, o mínimo de bolas que devem ser retiradas é 1346.

(b) Para que a soma dos números das bolas seja um múltiplo de 3, temos as seguintes possibilidades:

1. duas do grupo A;

2. uma bola do grupo A e uma bola do grupo C.

Qual o número máximo de bolas que podemos pegar de tal forma quer a soma de duas quaisquer não seja um múltiplo de 3? O pior cenário é: pegar uma bola do conjunto A e todas do conjunto B (que tem mais bolas que o grupo C). Então, o total é $1 + 673 = 674$. Se pegarmos 675 bolas, necessariamente a soma de duas delas será um múltiplo de 3. De fato, note que para quaisquer 675 bolas que pegarmos, se duas estiverem no conjunto A, então elas formam um par cuja a soma de seus números é igual a um múltiplo de 3. Se apenas uma estiver no conjunto A ou nenhuma das duas estiver em A, pelo menos 674 bolas estarão em $B \cup C$. Como B tem 673 elementos, temos que ter pelo menos uma do conjunto B e uma do conjunto C e, novamente, a soma dos números nessas bolas será um múltiplo de 3. Portanto, neste caso, a quantidade mínima de bolas é 675.

(c) Temos três conjuntos disjuntos de números inteiros positivos:

$$A_0 = \{x; 1 \leq x \leq 2017, x \equiv 0(mod3)\}$$
$$A_1 = \{x; 1 \leq x \leq 2017, x \equiv 1(mod3)\}$$
$$A_2 = \{x; 1 \leq x \leq 2017, x \equiv 2(mod3)\}$$

O número de elementos de A^1 é 673, já os conjuntos A_0 e A_2 possuem 672 elementos. Começamos com o conjunto com maior número de elementos. Escolhemos todos os ímpares contidos em A_1 e formamos um conjunto B_1 com 337 inteiros (com certeza a soma de quaisquer dois deles não é múltiplo de 3). Escolhemos, a seguir todos os pares contidos em A_2 e formamos um conjunto B_2 com 33 inteiros(com certeza a soma de quaisquer dois

deles não é múltiplo de 3). A soma de um elemento de B_1 com um elemento de B_2 é múltipla de 3, porém , sua diferença não é par. Escolhemos, agora , dois elementos de A_0, um par e um impar e denotamos o conjunto formado por esses elementos por B_0. Temos que a união $B_0 \cup B_1 \cup B_2$ é um conjunto em que quaisquer dois elementos x e y são tais que $x + y$ ou não é múltiplo de 3 ou $x \breve{} y$ não é par e, para qualquer outro elemento a do conjunto diferença $(A_0 \cup A_1 \cup A_2) - (B_O \cup B_1 \cup B_2)$, existe um elemento b de $B_0 \cup B_1 \cup B_2$ tal que:

$$a + b \equiv (mod\ 3) \text{ e } a - b \equiv (mod\ 2)$$

Portanto, a quantidade mínima de bolas que Joana deve retirar é 337 + 336 + 2 + 1 = 676. □

Capítulo 3

Aplicações da Aritmética Modular em nosso cotidiano

O uso da tecnologia tem impactado muito a vida das pessoas. Seu avanço contribuiu para o crescimento de empresas e de muitas facilidades que usufruimos todos os dias. Cada vez mais surgem inovações despertando em quase todo cidadão o desejo de obter ainda mais praticidade.

Apesar de não nos darmos conta, são muitas as aplicações da Aritmética Modular nas inovações tecnológicas que, de alguma forma, estão presentes em nossas vidas. Essas aplicações estão em várias circustâncias em nosso cotidiano pois, todos precisamos fazer compras, seja no supermercado ou pela internet, fazer operações bancárias de forma segura, fazer uso de documentos como RG e CPF para diversos fins, e muito mais.

3.1 Lendo Código de Barras

Vemos nos produtos das prateleiras dos supermercados uma marca de identificação conhecida como código de barras, que na verdade, é uma representação gráfica formada por uma sequência de listras brancas e pretas alternadas, de espessuras variáveis. Há quatro espessuras possíveis para essas listras: finas, médias, grossas ou muito grossas.

O código de barras representa uma sequência de números. A cada número corresponde um espaço de espessura fixa, que corresponde uma sequência de sete dígitos iguais a 1 ou 0. O símbolo 0 é utilizado para indicar uma listra branca fina, o símbolo 00 para uma listra branca média, 000 para uma listra branca grossa e 0000 para uma listra muito grossa. Da maneira análoga, representamos por 1, 11, 111 e 1111, uma listra preta fina, média, grossa ou muito grossa, respectivamente. As sequências de zeros e uns são tranformadas em sequências de dígitos de 1 a 9. Para uma descrição mais detalhada o leitor poderá consultar a referência [7]. Para previnir erros na leitura e decodificação desses símbolos

Figura 3.1: Código de barras
Fonte:https://codigosdebarrabrasil.com.br

foi criado o dígito verificador, que fica localizado no final de cada sequência de algarismos que vem impressa logo abaixo das barras.

Figura 3.2: Produtos com códigos de barra
Fonte:https://www.proteste.org.br/família/nc/noticia/entenda-os-códigos-de-barras

Atualmente, o código de barras é aplicado para acelerar o processo de verificação e controle de produtos em muitas áreas como comércio, indústria, boletos de contas de consumo, boletos bancários, hospitais, correios, ingressos para shows e jogos, transportes, etc. A vantagem do código de barras é que ele pode ser identificado rapidamente e sem erros pelos caixas eletrônicos e aparelhos de leitura óptica. Por exemplo, quando passamos uma mercadoria pelo caixa, o leitor óptico envia ao computador a sequência de barras pretas e brancas impressas no rótulo ou na etiqueta do produto. Um software interpreta qual sequencia de números ela representa, identificando o produto e seu preço. Observe que, quando a leitura óptica falha por algum motivo, o atendente do caixa digita a sequência de algarismos que aparecem abaixo das barras.

O código de barras foi criado nos Estados unidos em 1973 pela empresa Uniform Code Council(UCC) que é também, um conjunto de normas comerciais. Existem vários códigos de barras mas os mais conhecidos são: Universal Produt Code(UPC) e European Article

Number(EAN). O Brasil, assim como os Europeus, adotou em 1983 um código com padrão de 13 dígitos, o EAN-13. Existem códigos de barras com 12, 13 e 14 dígitos.

Os três primeiros dígitos indicam o país de origem do produto ou onde ele foi cadastrado. Por exemplo, no Brasil o registro nacional é 789. Nos produto nacionais são os três primeiros dígitos dos códigos de barras. Os quatro dígitos seguintes identificam a empresa fabricante mas, pode variar de 4 a 7 dígitos. Esse número é fornecido pela EAN, que faz o controle para que não haja números iguais. Os cinco dígitos seguintes representam o código do produto dentro da classificação da própria empresa especificando: tipo, sabor, modelo, cor, tamanho, quantidade, peso, durabilidade, etc. O último algarismo é chamado de dígito de controle. Ele é obtido por meio de operações feitas com os algarismos anteriores, servindo assim para confirmar se a leitura do código foi feita corretamente. Assim, para a sequência de dígitos 7896902211711 do código de barras de um dado produto, temos:

- 789 os 3 primeiros dígitos para produtos produzidos ou cadastrados no Brasil
- 6902 é o código da empresa
- 21171 caracteriza o produto
- 1 é o dígito verificador.

A detecção de erros

Para compreender como funciona o processo de detecção de erros precisamos entender, inicialmente, como se atribui a cada produto, o dígito de verificação. Suponhamos que um determinado produto está identificado pela sequência de dígitos $a_1a_2a\ldots a_{12}a_{13}$. Como os primeiros dígitos da sequência identificam o país de origem, o fabricante e o produto específico, os doze primeiros dígitos da sequência, estão determinados, por um método padrão, a cargo de uma autoridade classificadora em cada país. Denotaremso o décimo terceiro dígito, de verificação, por x.

Vamos representar a sequência de dígitos através de um **vetor de informação** $a = (a_1, a_2, \cdots, a_{12}, x)$.

O sitema EAN-13 utiliza um vetor fixo, chamado **vetor de pesos** dado por:

$$w = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1).$$

Fazendo o porduto entre os dois vetores temos:

$$a \cdot w = (a_1, a_2, \cdots, a_{12}, x) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$$

$$= a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_10 + a_11 + 3a_12 + x.$$

O dígito de verificação x se escolhe de forma tal que a soma acima seja múltiplo de 10, isto é, tal que

$$a \cdot w = 0(mod\ 10)$$

Por exemplo, no código da figura 3.2 os números que indicam o pais de origem, o fabricante e o produto são 789199100082. Vamos ver como foi detectado o dígito de verificação. Chamando este dígito de x e fazendo o produto com o vetor de pesos, temos:

$$7+(3\times 8)+9+(3\times 1)+9+(3\times 9)+1+(3\times 0)+0+(3\times 0)+8+(3\times 2)+x = 94+x$$

Portanto deve-se tomar $x = 6$.

Vejamos agora como funciona a detecção de erros.

O código de barras do guaraná da figura 3.2 é 7891991000826. Suponhamos que por um erro de digitação no quarto dígito, este número é transmitido como $a = 7892991000826$. Ao fazer a verificação de leitura o computador que recebeu a informação faz a operação $a \cdot w$ e obtem :

$$7+(3\times 8)+9+(3\times 2)+9+(3\times 9)+1+(3\times 0)+0+(3\times 0)+8+(3\times 2) = 97$$

Como o resultado não é um múltiplo de 10, o computador avisa que foi cometido algum erro.

3.2 International Standard Book Number (ISBN)

O ISBN(International Standard Book Number) é um sistema universalmente adotado para a classificação de livros. A identificação numericamente de cada livro através desse sistema distingue o pais, a editora e até a edição. No Brasil, a biblioteca Nacional coordena e supervisiona as atividades técnicas da Agência Brasileira ISBN em parceria com a fundação Miguel de Cervantes responsável pela gerência administrativa e pela interface com a Agência internacional do ISBN.

Atendendo a necessidade de tornar o sistema mais eficiente e devido ao crescente aumento das publicações a partir de 1^o de janeiro de 2007, o ISBN passou de 10 para 13 dígitos, com a adoção do prefixo 789, que é o código do Brasil.

Até 2007 a identificação numérica era feita módulo 11 utilizando um vetor de identificação com 10 componentes $w = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$. Por exemplo, um livro cujo código é ISBN 1-4020-0238-6, tinha código final de verificação 6, pois

$$(1, 4, 0, 2, 0, 0, 2, 3, 8, 6) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) =$$
$$= 10 + 36 + 14 + 8 + 9 + 16 + 6 = 99 \equiv 0(mod\ 11)$$

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

O cálculo do dígito de verificação do ISBN-13 é idêntico ao cálculo do EAN-13. Caso haja algum dígito errado, ou troca de dígitos adjacentes, esses erros sempre serão detectados de acordo com o método de verificação de dígitos ISBN, caso contrário o livro terá ISBN inválido.

No sistema ISBN-13 podemos calcular o dígito verificador da seguinte maneira:

1. Multiplica-se os 12 primeiros dígitos mais a_{13} pela sequência $(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$.

2. Calcula-se a soma desse produto, e verifica qual dos possíveis valores do conjunto $a_1 3$ pode assumir para que a soma seja um múltiplo de 10.

Por exemplo, o livro do autor [13] tem o número ISBN 978-85-244-0142-8. O dígito final, de verificação é 8 porque

$$9+(3\times 7)+8+(3\times 8)+5+(3\times 2)+4+(3\times 4)+0+(3\times 1)+4+(3\times 2)+8 = 110 \equiv 0 (mod\ 10)$$

Observe que o cálculo utilizado pelo computador nada mais é que uma aplicação de congruência módulo 10.

3.3 Detecção de erros

No mundo moderno em que vivemos são geniais as vantagens que podemos ter fazendo compras, pagamentos e consultas via internet de forma segura e sem sair de casa. No entanto, a segurança de nossos dados é uma preocupação muito pertinente, pois se os dados não forem muito bem protegidos corremos o risco de ser vítimas de fraudes. Por isso, foram criados os DV (dígitos de verificação), também conhecidos como número-controle. Estes são dígitos incorporados a números para possibilitar a detecção de erros de digitação no ato do processo de digitação. Recurso este muito difundido, presente em códigos de barras, CPF, RG, Números de contas bancárias, entre outras sequências numéricas. Esse(s) digito(s), podem ser mais de um, podendo ser letra(s) ou algarismos variando de 0 a 9. Veremos como calcular o DV, em alguns casos, nas seções seguintes.

Já vimos com funciona a detecção de erros nos exemplos anteriores. Veremos agora um caso em que um erro é cometido mas não é detectado na leitura do código númerico.

O código UPC é muito semalhante aos códigos já citados neste texto. Ele utiliza apenas 12 dígitos (pois usa apenas um dígito para identificar o país de origem do artigo, enquanto o EAN utiliza-se de dois), e o vetor de pesos utilizado pelo UPC tem um dígito a menos:

$$w = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$$

O leitor notará que, se o digitador comete apenas um erro de digitação, trocando um dos dígitos a_i por outro valor, então necessariamente o ponto $a \cdot w$ *não será* congruente a 0 em módulo 10 e assim será possível detectar que o erro foi cometido. Se mais de um erro for cometido na digitação, o fato provavelmente ainda será detectado, mas já não podemos ter certeza, pois ele poderia se compensar mutuamente e a soma poderia ainda continuar sendo um múltiplo de 10.

O leitor pode-se perguntar qual a função do vetor de pesos w. De fato, se a escolha do dígito de verificação x fosse feita simplesmenet de modo que

$$a_1 + a_2 + \cdots + a_{12} + x \equiv (mod\ 10),$$

ainda assim UM erro de digitação seria detectado. Acontece que há um outro erro de digitação muito comum, que consiste em digitar todos os números corretamente, mas trocar a ordem de dois dígitos consecutivos.

Suponha que, ao digitar o número 9 788531 404580 do nossso primeiro exemplo, tenha se cometido esse tipo de erro, e que o número de fato digitado fosse 9788351 404580.Ao efetuar a verificação teríamos:

$$\begin{aligned}(9, 7, 8, 8, 5, 3, 1, 4, 0, 4, 5, 8, 0) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) = \\ = 9 + 21 + 8 + 24 + 3 + 15 + 1 + 12 + 12 + 5 + 24 \\ = 134 \not\equiv 0(mod\ 10)\end{aligned}$$

suponha agora que , ao digitar o número 9 781 402 002380 tenha se sido cometido um erro desse mesmo tipo, e que o número de fato digitado fosse 9 781402 002830. Ao efetuar a verificação teríamos:

$$\begin{aligned}(9, 7, 8, 1, 4, 0, 2, 0, 0, 2, 8, 3, 0) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) = \\ = 9 + 21 + 8 + 3 + 4 + 2 + 6 + 3 + 24 \\ = 80 \equiv 0(mod\ 10)\end{aligned}$$

Este exemplo mostra que o sistema de detecção adotado acima *não tem capacidade de detectar todo erro de transposição* cometido. Realmente um erro de transposição de dois

dígitos consecutivos a_i e a_{i+1} é detectada, neste sistema de codificação (sistema EAN-13) se , e somente se,

$$|a_i - a_{i+1}| \neq 5.$$

Mais ainda, um erro de *transposição não adjacente* do tipo

$$\ldots a_i \ldots a_{i+1} a_{i+2} \ldots \mapsto \ldots a_{i+2} a_{i+1} a_i \ldots$$

não pode ser detectado pelo sistema EAN-13. Mais ainda, um erro de transposição em que dois dígitos não adjacentes a_i e a_j são trocados não pode ser detectado pelo sistema se a diferença $i - j$ é par.

Enunciaremos agora um resultado que descreve a capacidade que determinados sistemas têm para detectar os diveros tipos de erros mais frequentes.

Teorema 3.1. *Seja m um inteiro positivo e $w = (w_1, \ldots, w_n)$ um vetor de pesos. Suponhamos que um vetor de identificação $a = (a_1, \ldots, a_n)$ (onde assumimos que $0 \leq i \leq n$) satisfaz a condição*

$$a \cdot w = a_1 w_1 + \cdots + a_n w_n \equiv c (mod\ m).$$

Então:

1. *Todo erro consistente numa única alteração na posição i-ésima será detectado se, e somente se, $mdc(m, w) = 1$*

2. *Todo erro de transposição da forma*

$$\ldots a_i \ldots a_j \ldots \mapsto \ldots a_j \ldots a_i \ldots$$

será detectado se, e somente se, $mdc(w_i - w_j, m) = 1$.

A demonstração do resultado acima pode ser encontrado em [7].

De acordo com este resultado fica claro que a melhor forma de ter certeza de que um sistema de codificação será capaz de detectar todos os *erros únicos* (digitação de símbolo errado) e todos os *erros de transposição* é tomar, para o valor do módulo m, um número primo. De fato existem vários sistemas em uso que procedem desta forma.

3.4 Cadastro de Pessoa Física(CPF)

O CPF ou Cadastro de Pessoa Física é um documento brasileiro emitido pela secretaria da Receita Federal do Ministério da Fazenda. Seu número é composto por 11 dígitos, sendo

os dois últimos os dígitos verificadores, que atestam se o número do CPF é válido. O CPF tem a seguinte configuração:

$$9 \text{ dígitos base} + 2 \text{ DV} = \text{XXX.XXX.XXX-XX}$$

Os nove primeiros dígitos são a base do cálculo para o décimo e décimo primeiro dígitos, que são chamados de dígitos verificadores. O nono dígito define a Região Fiscal onde o seu CPF foi emitido.

A Tabela 3.1 identifica o número de cada região fiscal.

NÚMERO	REGIÃO
0	RS
1	DF,GO,MS,MT e TO
2	AC,AM,AP,PA,RO e RR
3	CE,MA e PI
4	AL,PB,PE e RN
5	BA e SE
6	MG
7	ES e RJ
8	SP
9	PR e SC

Tabela 3.1: Tabela das Regiões Fiscais
Fonte:idg.receita fazenda.gov.br

Como calcular os dígitos verificadores do CPF?

Tomemos como exemplo os nove primeiros dígitos de um CPF fictício de número 707048354.

O DV será o resto da divisão por 11 do somatório da multiplicação de cada um desses nove algarismos, que são o número base para o cálculo, respectivamente pela sequência: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9.

Quando ocorre do resto ser 10 será considerado apenas o 0. Para alguns bancos, quando o resto é 10 se considera o dígito X.

Vejamos como calcular o primeiro dígito verificador de um CPF:

1. Multiplica-se o número base do CPF pela sequência crescente dos nove primeiros dígitos, a começar pelo 1:

$$(7, 0, 7, 0, 4, 8, 3, 5, 4) \times (1, 2, 3, 4, 5, 6, 7, 8, 9) = (7, 0, 21, 0, 20, 48, 21, 40, 36)$$

2. Calcula-se a soma desse produto:

$$7 + 0 + 21 + 0 + 20 + 48 + 21 + 40 + 36 = 193$$

3. Calcula-se o resto da divisão da soma obtida por 11. Como: $193 = 17 \times 11 + 6$, o resto é 6. Portanto, 6 é o primeiro algarismo do DV.

Vejamos como calcular o segundo dígito:

1. Multiplica-se os nove números do CPF mais o primeiro digito verificador obtido pela sequência crescente dos dez primeiros dígitos, a começar de 0.

$$(7, 0, 7, 0, 4, 8, 3, 5, 4, 6) \times (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) = (0, 0, 14, 0, 16, 40, 18, 35, 32, 54)$$

2. Calcula–se a soma desse produto:

$$0 + 0 + 0 + 14 + 0 + 16 + 40 + 18 + 35 + 32 + 54 = 209$$

3. Calcula-se o resto da divisão da soma obtida por 11. Como $209 : 11 = 19$ é uma divisão exata, ou seja, deixa resto 0. Concluimos que 0 é o segundo algarismo do DV e a sequência completa dos 11 dígitos do nosso CPF fictício é

$$707048354 - 60$$

Capítulo 4

Considerações finais

Apesar das Congruências Modulares não fazerem parte do currículo do Ensino Básico a proposta de introduzir este conteúdo nessa fase escolar seria muito pertinente pois poderia contribuir e incentivar a aprendizagem dos alunos. Acreditamos que embora o nosso público alvo seja muito jovem, isto é, alunos a partir do 6^o ano do ensino fundamental, esta teoria é de fácil compreensão, por isso, poderia ser empregada, tanto para a aquisição de novos conhecimentos como metodologia de aprimoramento de conceitos já estudados. Visto que, para aprender congruências modulares basta ter conhecimento sobre os conceitos de divisibilidade acreditamos ainda que a contribuição do ensino da Aritmética Modular é valido pelos benefícios que esta poderia proporcionar na aquisição das competências e habilidades necessárias, tanto para o âmbito escolar, como para o desempenho de atividades cotidianas dos alunos, como calcular, refletir e comparar, o que favoreceria, em muito, a sua tomada de decisão.

Congruências Modulares englobam teorias fundamentais da aritmética que são conhecimentos indispensáveis à aprendizagem da matemática, como por exemplo, propriedades e operações com números inteiros, que boa parte do alunado tem dificuldade em compreender na forma como é ensinada atualmente.

A metodologia apresentada tem como objetivo oferecer subsídios necessários para que o indivíduo possa avançar adquirindo conhecimentos justificados com teorias que esclareçam os fundamentos empregados pela matemática que é ensinada nas escolas de forma clara e objetiva. O emprego das congruências modulares, vêm favorecer a aproximação do aluno com a matemática, no sentido que lhe dá aplicabilidade utilizando cálculos simples e acessíveis. Além disso, a atualidade do uso de congruências no campo tecnológico, como por exemplo, no cálculo de dígitos verificadores como CPF, CNPJ, o sistema de identificação de livros ISBN, entre outros, vêm aproximar a matemática ensinada nas escolas da matemática envolvida na obtenção de recursos tecnológicos.

São muitas as utilidades que esta teoria proporciona, como o conhecimento da teoria

que envolve os códigos de barras com a qual o aluno poderia avaliar o quanto a matemática contribui para o desenvolvimento da tecnologia e verificar como é fácil identificar as informações que o mesmo traz, como por exemplo, saber se um produto é fabricado no Brasil, se dois produtos diferentes são fabricados pela mesma empresa e outras informações que o código de barras trás.

A partir da teoria das congruências, muitas atividades interessantes e motivadoras poderiam ser propostas para alunos de todas as faixas etárias, uma delas é a possibilidade de descobrir datas passadas e futuras numa contextualização de eventos. E assim, mostrar a eles que é possível, por exemplo, calcular o dia da semana em que nasceram. Esse fato iria motivá-los a compreender melhor a teoria, bem como, possibilitará ao professor fazer futuras generalizações para aprofundar os conhecimentos adqueridos.

Portanto, acreditamos que a Teoria da Aritmética Modular, poderia contribuir de forma significativa para o desenvolvimento do aluno e que a metodologia que propomos associando conceitos a exemplos de como eles pode ser úteis na vida das pessoas, atendem a atual tendência do ensino de matemática, de primar pelo raciocínio e contextualização em lugar de decoração e simples aplicação de conceitos matemáticos em exercícios de fixação. Assim, apesar de a Teoria das Congruências Modulares não fazerem parte do currículo do alunado do ensino básico, esta poderia ser introduzida a partir do 6^o ano do Ensino Fundamental por professores que buscam estratégias para favorecer o processo ensino aprendizagem.

Referências

[1] BRASIL. Secretaria de Educação Fundamental. Parâmetros Curriculares Nacionais: Matemática. Brasília: MEC/SEF, 1998.

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

[3] CRUZ, Priscila. O brasileiro quer educação para já. Estadão de São Paulo, 10 março 2018. Disponível em: opinião.estadao.com.br

[4] COUTINHO, S. C. Criptografia. Apostila do PIC. OBMEP. IMPA, 2014.

[5] DUTENHEFNER, Francisco; CADAR, Luciana. Encontros de Aritmética. Apostila do PIC. OBMEP. IMPA, 2015.

[6] DUTENHEFNER, F. Dutenhefner; L. CADAR. Encontros de Aritmética. PIC. SBM. IMPA.2015

[7] MILIES, Francisco César Polcino Milies. A Matemática dos Códigos de Barras. PIC. OBMEP.2009. Disponível em: obmep.org.br/docs/apostila6.pdf

[8] HEFEZ, A. Elementos de Aritmética, 2ª edição, PIC. SBM. IMPA. 2005.

[9] JURKIEWICZ, Samuel. Divisibilidade e números inteiros,Apostila do PIC, OBMEP. IMPA 2017.

[10] LIMA, E. L. Sobre o ensino da matemática. Revista do Professor de Mátemática. Rio de Janeiro. Sociedade Brasileira de Matemática. Volume 28, p.1-5, Maio/Agosto 1995.

[11] MARCONI, M. A; LAKATOS, E.M. Metodologia do Trabalho Cientifico. 7 edição. São Paulo: Atlas, 2007.

[12] MARTINI, R, Criptografia e Cidadania Digital. Rio de Janeiro, Ciência Moderna, 2001.

[13] SANTOS, José Plínio de Oliveira, Teoria dos Números. 3ª edição. Rio de Janeiro, IMPA, 2009.