UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL-PROFMAT

JOÃO VICTOR LIMA FERNANDES

ENSINO DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA E POSSÍVEIS APLICAÇÕES

JUAZEIRO DO NORTE - CEARÁ

2018

JOÃO VICTOR LIMA FERNANDES

ENSINO DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA E POSSÍVEIS APLICAÇÕES

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Francisco De Assis Benjamim Filho

JUAZEIRO DO NORTE - CEARÁ

2018

Dados internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

F363e Fernandes, João Victor Lima

Ensino de aritmética modular na educação básica e possíveis aplicações. / João Victor Lima Fernandes. – Juazeiro do Norte, 2018.

47 f.; il. color.

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia, Programa de Pós-graduação em Matemática em Rede Nacional, 2018.

Orientação: Prof. Dr. Francisco de Assis Benjamim Filho.

1. Aritmética modular (Ensino). 2. Educação básica (Métodos de ensino). 3. Avaliação da aprendizagem. I. Título

CDD 372.72

Bibliotecária: Valeska Paulino Nogueira – CRB 3/1198

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Ensino de Aritmética Modular na Educação Básica e Possíveis Aplicações

João Victor Lima Fernandes

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática

Aprovada em 31 de outubro de 2018.

Banca Examinadora

Francisco de Assis Benjamim Filho.

Prof. Dr. Francisco de Assis Benjamim Filho - UFCA

Orientador

Francisco Pereira Chaves

Prof. Dr. Francisco Pereira Chaves - UFCA

Maria Silvana Alcântara Costa

Profa. Dra. Maria Silvana Alcântara Costa - UFCA

Dedico este trabalho a todos que contribuíram com a sua realização.

AGRADECIMENTOS

À CAPES, pelo apoio financeiro;

Aos meus pais, Eugenio Fernandes Fonseca e Lucia Maria Lima Fernandes, pelo incentivo, criação e educação dada e toda ajuda necessária para o término dessa etapa;

À minha eterna namorada, amiga e companheira, Edvânia Castro Vieira, pelo apoio, compreensão, paciência e auxílio para eu chegar até aqui; Aos amigos e familiares que me apoiaram e compreenderam minha ausência para que eu pudesse alcançar esse objetivo;

Ao professor orientador Dr. Francisco de Assis Benjamim Filho, pela paciência e toda colaboração para que este trabalho fosse concluído;

À coordenadora, professora Dra. Maria Silvana Alcântara Costa, pelas sábias palavras, incentivo e apoio durante todo o curso;

Aos professores das disciplinas do programa, que lecionaram com maestria e ombridade;

Aos professores participantes da banca examinadora Francisco Pereira Chaves e Maria Silvana Alcântara Costa pelo tempo, pelas valiosas colaborações e sugestões.

Aos colegas da turma de mestrado, pelas ajudas e apoio;

Aos motoristas da empresa de ônibus Guanabara que me levaram e buscaram por todo esse caminho nessa jornada;

Mesmo o pó quando reunido torna-se uma montanha. (Provérbio japonês)

RESUMO

Este trabalho possui como principais finalidades apresentar a aritmética modular, um conteúdo comumente visto no ensino superior, e mostrar por meio de exemplos de aplicações, que este tópico deveria ser ensinado na educação básica. Especificamente, veremos um pouco da história da aritmética modular e a teoria necessária para a compreensão das ideias básicas do assunto. Mostraremos alguns sites que podem auxiliar o professor na avaliação do aprendizado dos alunos após o estudo de aritmética modular e problemas de exames de admissão e olimpíadas que podem ser resolvidos usando este conteúdo. Em seguida, veremos alguns livros do Ensino Básico que abordam critérios de divisibilidade bem como tópicos relacionados. A presença de tais assuntos em livros desse nível pode ser usada como motivação para a introdução de conceitos mais gerais de aritmética modular. Listaremos uma série de aplicações da teoria desenvolvida neste trabalho. Estudaremos como aplicá-la para entender a criação dos números de ISBN e CPF e a razão pela qual a tradicional prova dos noves caiu em desuso. Veremos ainda os critérios de divisibilidade por 3, 9, 10, 11 e como determinar o resto na divisão de polinômios usando aritmética modular. Mostraremos ainda aplicações de equações diofantinas e um jogo de dominó para a verificação do aprendizado dos conceitos de aritmética modular. Ao final, esperamos que este trabalho contribua com o ensino de aritmética modular na Educação Básica.

Palavras-chave: Aritmética Modular. Educação Básica. Ensino.

ABSTRACT

The main purposes of this work is to present the modular arithmetic, content commonly seen in higher education, and show by way of examples of applications that this topic should be taught in basic education. Specifically, we will look at some of the history of modular arithmetic and the theory needed to understand the basic ideas of the subject. We will show you some sites that can help teacher evaluation of student learning after modular arithmetic study and problems of admission exams and olympics that can be solved using this content. Next, we will look at some books of Basic Education that address divisibility criteria as well as related topics. The presence of such subjects in books of this level can be used as a motivation for the introduction of more general concepts of modular arithmetic. We will list a number of applications of the theory developed in this work. We will study how to apply it to understand the creation of ISBN and CPF numbers and the reason why the traditional nines test has fallen into disuse. We will see also divisibility criteria by 3, 9, 10, 11 and how to determine the remainder in the division of polynomials using modular arithmetic. We will also show applications of diophantine equations and a domino game to verify the learning of concepts of modular arithmetic. In the end, we hope that this work contributes to the teaching of modular arithmetic in Basic Education.
Keywords: Modular Arithmetic. Basic education. Teaching.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CPF	Cadastro de Pessoa Física
ISBN	International Standard Book Number
PCN	Parâmetro Curricular Nacional
a.C.	Antes de Cristo
MMC	Mínimo Múltiplo Comum
MDC	Máximo Divisor Comum
PCN+	Parâmetro Curricular Nacional +
Enem	Exame Nacional do Ensino Médio
Etc.	Et cetera
mod	Módulo
OBM	Olimpíada Brasileira de Matemática
RG	Registro Geral
CNPJ	Cadastro Nacional de Pessoa Jurídica
EsPCEx	Escola Preparatória de Cadetes do Exército

LISTA DE SÍMBOLOS

$\in$	Pertence
$\mathbb{Z}$	Inteiros
$\leq$	Menor ou igual
$<$	Menor
$\|a\|$	módulo de a
$\|$	Divide
$\neq$	Diferente
$\nmid$	Não divide
$\mathbb{N}$	Naturais
$>$	Maior
$\equiv$	Congruente
$:=$	Definido por
$\not\equiv$	Incongruente
(c,m)	MDC de c e m
!	Fatorial
$\left[\frac{z}{x}\right]$	Parte inteira da divisão $\frac{z}{x}$

SUMÁRIO

1 INTRODUÇÃO

Ao estudar Aritmética Modular na graduação e no mestrado, me encantei com o tema pois é instigante, facilita a resolução de vários tipos de problemas, simplifica cálculos e possui interessantes aplicações. Me perguntei então o motivo de não ser estudada no Ensino Básico, visto que os pré-requisitos necessários são mínimos, entre eles: MMC, MDC, divisão euclidiana e números primos, ou seja, conteúdos estudados no Ensino Fundamental. O assunto é bem amplo, então nos restringimos às partes que podem ser vistas após o estudo dos conteúdos mencionados acima e após os critérios de divisibilidade de alguns números naturais.

Será presentada a importância do estudo da Aritmética Modular para o professor do Ensino Básico. Além disso, desejamos abordar os principais teoremas do conteúdo, discutir autores que tratam do tema, resolver algumas questões de olimpíadas com o conteúdo e indicar aplicações e sites sobre o assunto.

Foi feita uma pesquisa bibliográfica em livros e dissertações que também tratam do tema para que, ao compará-los, pudesse chegar numa conclusão.

1.1 História da Aritmética Modular

Segundo Hefez (2015), acredita-se que Tales de Mileto tenha introduzido na Grécia o estudo da Matemática que havia aprendido com egípcios. Em seguida Pitágoras de Samos difundiu-a através da escola pitagórica e seus membros. Com todo o desenvolvimento da Matemática, em torno de 300 a.C., surgiu um tratado com 13 livros em Alexandria, *Os Elementos* de Euclides cuja importância estende-se até os dias atuais pois reunia a maior parte do conhecimento matemático que se tinha na época. Eram 10 livros de Geometria e 3 de Aritmética. Nele, há conceitos sobre MMC, MDC, números primos, divisão euclidiana, etc.

Cerca de 500 anos depois, Diofanto de Alexandria em seu livro *Arithmetica* (13 volumes) voltou a impulsionar o estudo de Aritmética o que influenciou Pierre de Fermat mais de 1300 anos depois através de problemas como encontrar soluções racionais ou inteiras da equação $x^2 + y^2 = z^2$. Entre esse período merece menção Eratóstenes por seus trabalhos relacionados aos números primos e por ter desenvolvido seu famoso Crivo.

Fermat contribuiu imensamente para o desenvolvimento da Teoria dos Números através da descoberta de vários teoremas e ficou marcado pelo Último Teorema de Fermat, que diz ser impossível um cubo ser igual a soma de dois cubos, uma biquadrada ser igual a soma de duas biquadradas ou qualquer outra potência superior. Explicitamente, para $n \geq 3$, a equação

$$x^n + y^n = z^n,$$

não tem soluções inteiras positivas.

Leonhard Euler (1707-1783) provou os resultados de Fermat (menos O Último Teorema), e é considerado o matemático mais importante do século XVII, possui trabalhos significativos sobre os mais diversos assuntos, como funções, números complexos, cálculo diferencial e integral, teoria dos números, acústica, música, etc.

Carl Friederich Gauss (1777-1855), um dos matemáticos mais importantes da história da Matemática, autor do livro *Disquisitiones Arithmeticae* em 1801, introduziu a noção de congruência, inclusive com a notação usada até hoje, desenvolveu a teoria dos resíduos quadráticos, demonstrou a Lei da Reciprocidade Quadrática, etc. Sendo portanto fundamental para a aritmética modular.

2 ENSINO DE ARITMÉTICA MODULAR

Este capítulo está dividido em duas partes, a primeira relacionada à aritmética modular no Ensino Básico e a outra, no Ensino Superior. A primeira não trata do conteúdo em si nem de como ele é abordado, pois ele não é estudado nessa etapa, pelo menos não com a leve abrangência que sugeriremos aqui. Comentaremos sobre autores que defendem que esse tópico seja visto pelo alunos apresentando seus argumentos e metodologias para que seja posto em prática esse estudo. Na segunda parte é dada ênfase ao estudo do conteúdo no Ensino Superior.

2.1 Aritmética Modular no Ensino Básico

Os Parâmetros Curriculares Nacionais, PCN (1997), destacam que a Matemática deve desenvolver o raciocínio e a imaginação do aluno enquanto os PCN+ (2006), afirmam que o Enem possui cinco competências gerais, entre elas: dominar diferentes linguagens, representações matemáticas, compreender processos, sejam eles tecnológicos, etc. Seria interessante que os alunos dominassem a linguagem da aritmética modular e que compreendessem os procedimentos existentes.

Na pesquisa biliográfica que fizemos, não foram encontrados em livros do ensino básico o conteúdo de aritmética modular.

Alguns autores sugerem o estudo no Ensino Fundamental e outros no Ensino Médio. Para Ferreira (2018), "Devido à importância do estudo e aplicabilidade das congruências modulares que estimulam o desenvolvimento de habilidades essenciais para a formação do aluno, propomos o ensino de Congruências Modulares a partir do 6º ano do Ensino Fundamental.". Sá (2018), diz que é um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental, que é gerador de excelentes oportunidades de contextualização no processo de ensino/aprendizagem de matemática. Souza (2015), defende que aritmética modular seja introduzida na grade curricular das séries finais do Ensino Fundamental. Sant'Anna (2013), afirma que é uma ferramenta valiosa de ensino para as séries finais do Ensino Fundamental. Pinheiro (2018) apresenta uma proposta de se trabalhar Aritmética Modular com os alunos do Ensino Fundamental II.

Freitas (2015) propõe o estudo de congruências no Ensino Médio. Nessa mesma direção, Pinto et al. (2017) acreditam que "esse objeto de estudo quando aplicado nesse nível de ensino pode levar aos educandos habilidades que os permitem criar conjecturas, deixando-os confortáveis para fazer abstrações, provocando argumentações de diferentes teor de escrita ou fala".

Mattos et. al (2006) afirmam que "o estudo de assuntos inerentes à teoria dos números favorece o desenvolvimento de ideias fundamentais da matemática, tais como: conjecturas, argumentações e demonstrações, além de ajudar os estudantes no entendimento conceitual da aritmética e da álgebra".

Em outros países também ocorre esse questionamento sobre o estudo e a importância da Aritmética Modular no Ensino Básico, como podemos observar no seguite trecho:

> No entanto, apesar do potencial que a Aritmética Modular tem como uma ferramenta pedagógica, com uma ampla variedade de aplicações contextualizadas e aplicáveis no ambiente escolar e depois de rever alguns textos destinados ao ensino básico e secundário, pode-se ver como a aritmética modular não é abordada nesses casos e a maior aproximação que se tem é quando nos primeiros anos do ensino fundamental ensina-se a fazer medições de tempo (fenômeno cíclico e portanto associado à aritmética modular)"(Bello, (2011), p.68 tradução própria).[1].

2.2 Aritmética Modular no Ensino Superior

No Ensino Superior o estudo de Aritmética Modular está presente em disciplinas de Teoria dos Números ou Matemática Básica. Vejamos primeiro como realizar a divisão euclidiana.

2.2.1 Algoritmo de Euclides

Veremos a seguir a noção de divisibilidade bem como suas propriedades e o algoritmo da divisão de Euclides.

Definição 2.1. *(Divisibilidade) Dados inteiros a e b, dizemos que a divide b e indicamos por $a \mid b$, se existe um inteiro c tal que $b = ac$. Caso contrário, dizemos que a não divide b e indicamos por $a \nmid b$.*

Antes de passarmos às propriedades da divisibilidade, definamos o módulo de um número.

Definição 2.2. *Seja a um número inteiro. O módulo de a, denotado por $|a|$, é definido por* $|a| = \begin{cases} a, & se\ a \geq 0 \\ -a, & se\ a < 0. \end{cases}$

Proposição 2.1. *A divisão tem as seguintes propriedades:*

1. *$m \mid m$ e $1 \mid m$;*
2. *Se $d \mid m$ então $ad \mid am$;*
3. *Se $ad \mid am$ e $a \neq 0$, então $d \mid m$;*
4. *$m \mid 0$;*
5. *Se $d \mid m$ e $m \neq 0$, então $|d| \leq |m|$;*
6. *Se $d \mid m$ e $m \mid d$, então $d = \pm m$;*

[1]Sin embargo, y a pesar del potencial que tiene la Aritmética Modular como una herramienta pedagógica, con una gran variedad de aplicaciones contextualizadas y aplicables en el ámbito escolar, y después de revisar algunos textos diseñados para la educación básica y media, se puede ver cómo la aritmética modular no es abordada en estas instancias y la mayor aproximación que se presenta es cuando en los primeros cursos de la básica primaria se enseña a hacer mediciones de tiempo (fenómeno cíclico y por tanto asociado a la aritmética modular).

7. *Se* $d \mid m$ *e* $d \neq 0$ *então* $\frac{m}{d} \mid m$*;*
8. *Se* $d \mid a$ *e* $d \mid b$ *então* $d \mid (a+b)$*.*

Demonstração. Todas as propriedades decorrem quase imediatamente da definição.

1. Como $m = 1 \cdot m$ então $m \mid m$ e $1 \mid m$.
2. Se $d \mid m$, então $m = d \cdot c$, para algum $c \in \mathbb{Z}$, logo $am = cad$, donde $ad \mid am$.
3. Se $ad \mid am$, então $ad \cdot k = am$, para algum $k \in \mathbb{Z}$, dividindo ambos os membros por a, obtemos: $d \cdot k = m$, ou seja, $d \mid m$.
4. Como $m \cdot 0 = 0$ temos que $m \mid 0$.
5. Se $d \mid m$, então $d \cdot k = m$ para algum $k \in \mathbb{Z}$, o que, pela propriedade do módulo, implica $|d| \cdot |k| = |m|$. Como $m \neq 0$, temos $k \neq 0$ e $|k| \geq 1$, daí $|d| \leq |m|$.
6. Se $d \mid m$ e $m \mid d$, então $d \cdot k = m$ e $m \cdot q = d$, com $k, q \in \mathbb{Z}$. Ou seja, $mq \cdot k = m$. Dividindo ambos os membros por m, obtemos $q \cdot k = 1$, logo $q = \pm 1$. Portanto $d = \pm m$.
7. Se $d \mid m$, então $m = a \cdot d$ e portanto $\frac{m}{d}$ é um inteiro. Como $\frac{m}{d} \cdot d = m$, segue da definição que $\frac{m}{d} \mid m$.
8. Se $d \mid a$ e $d \mid b$, então existem r e s tais que $a = rd$ e $b = sd$. Como $a + b = (r+s)d$, temos que $d \mid (a+b)$.

□

Mesmo quando a não divide b, pode-se estabelecer uma relação entre eles. Temos então o seguinte resultado cuja prova pode ser encontrada em Hefez (2005).

Teorema 2.1. *(Algoritmo da divisão de Euclides) Dados* $x, y \in \mathbb{Z}$*,* $x \neq 0$*. Existem únicos inteiros* a*,* b *tais que* $y = a \cdot x + b$*, onde* $0 \leq b < |a|$*, chamamos* a *de quociente,* b *de resto,* y *de dividendo e* x *de divisor.*

Exemplo 2.1. *Como* $7 = 3 \cdot 2 + 1$*, o quociente e o resto da divisão de* 7 *por* 2 *são iguais a* 3 *e* 1 *respectivamente.*

Vários conceitos estão diretamente relacionados com a divisão de Euclides, como: Máximo Divisor Comum (MDC) e números primos que passamos a definir.

2.2.2 Números Primos

Definição 2.3. *Um natural* n $(n > 1)$ *é dito primo se seus únicos divisores forem* 1 *e* n*. Se* n *não é primo, dizemos que é composto.*

Veremos agora um resultado que desempenha um papel crucial neste trabalho. Ele diz basicamente que os números primos são os ingredientes necessários para a contrução de todos os demais números.

Teorema 2.2 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que* 1 *é primo ou se escreve como produto de números primos. Além disso, tal representação é única exceto pela ordem dos fatores.*

Demonstração. Faremos a prova por indução. Para $n = 2$ o resultado é válido. Suponhamos que o resultado é válido para todo número natural menor que n, provaremos que vale para n. Se n é primo então não há o que mostrar. Suponhamos que n seja composto, logo pode ser escrito da seguinte maneira: $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Devido à hipótese de indução, existem primos $p_1, ..., p_a$ e $q_1, ..., q_b$ tais que $n_1 = p_1 \cdots p_a$ e $n_2 = q_1 \cdots q_b$. Assim, $n = p_1 \cdots p_a \cdot q_1 \cdots q_b$.

Mostraremos que se escreve de modo único. Suponhamos que $n = p_1 \cdots p_c = q_1 \cdots q_d$, onde cada p_i e q_j é primo. Como $p_1 \mid q_1 \cdots q_d$, temos que $p_1 \mid q_j$ para algum j. Podemos supor, sem perda de generalidade, que $p_1 \mid q_1$, o que acarreta $p_1 = q_1$. Assim $\frac{n}{p_1} = p_2 \cdots p_c = q_2 \cdots q_d$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são iguais, isto é, $c = d$ e, exceto pela ordem dos fatores, $p_1, ..., p_c$ e $q_1, ..., q_d$ são iguais. □

O próximo resultado trata da infinitude dos números primos. Para prová-lo, usaremos o Teorema Fundamental da Aritmética.

Teorema 2.3. *Existem infinitos números primos.*

Demonstração. Suponha que existem apenas um número finito n de primos e sejam $p_1, p_2, ..., p_n$ tais números. Considere $P = (p_1 \cdot p_2 \cdots p_n) + 1$. Note que P não é divisível por nenhum dos p_i's pois a divisão de P por qualquer um deles deixa resto 1. Mas, pelo resultado anterior, P é primo ou composto o que implica a existência de um primo que não está na lista. Absurdo. Logo, existem infinitos primos. □

2.2.3 Mínimo Múltiplo Comum

Definição 2.4. *O mínimo múltiplo comum dos números inteiros positivos $a_1, ..., a_n$, denotado por $[a_1, ..., a_n]$, é o menor número inteiro positivo que é divisível por $a_1, ..., a_n$.*

Exemplo 2.2. *Calcule o MMC de* 8 *e* 12.

Três métodos podem ser considerados:

- **Método 1:** Uma maneira de resolver é listar os múltiplos de 8 e os múltiplos de 12 até encontrar um número que esteja nas duas listas:
  Múltiplos de 8: 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, ...
  Múltiplos de 12: 12, 24, 36, 48, 60, 72, 84, 96, 108, 120, 132, 144, ...
  Comparando, percebemos que o menor múltiplo de ambos é 24.
- **Método 2:** Utilizando a fatoração em números primos de ambos os números e multiplicando-se os primos com os maiores expoentes: $8 = 2^3$, $12 = 2^2 \cdot 3$, multiplicamos 2^3 por 3, obtendo 24.
- **Método 3:** Utilizando a fatoração em números primos como descrito abaixo (acaba sendo o método 2 feito de um modo um pouco diferente).

Tabela 1: MMC de 8 e 12

8	12	2
4	6	2
2	3	2
1	3	3
1	1	24

Fonte: Autor.

Na primeira linha, colocamos os números dos quais calcularemos o MMC, à direita deles, pomos um número primo que divide pelo menos um dos dois, no caso 2 (que divide ambos), os resultados das divisões colocamos abaixo e repetimos o processo até que ambos os quocientes sejam 1. Por fim, multiplicamos os números que estão na última coluna e o resultado será o MMC.

2.2.4 Máximo Divisor Comum

Definição 2.5. *O máximo divisor comum dos números $a_1, ..., a_n$, não todos nulos, denotado por $(a_1, ..., a_n)$, é o maior número inteiro que divide $a_1, ..., a_n$.*

Exemplo 2.3. *Calcule o MDC de* 8 *e* 12.

Analogamente ao que foi feito com o MMC, temos

- **Método 1:** Uma maneira de resolver é listar os divisores positivos de 8 e os divisores positivos de 12 até encontrar um número que esteja nas duas listas:
  Divisores de 8: $1, 2, 4, 8$.
  Divisores de 12: $1, 2, 3, 4, 6, 12$.
  Comparando, percebemos que o maior divisor de ambos é 4.
- **Método 2:** Utilizando a fatoração em números primos de ambos os números e multiplicando-se os primos com menores expoentes que estejam em ambas: $8 = 2^3$, $12 = 2^2 \cdot 3$. Observando que apenas o 2^2 está em ambos concluímos que 4 é o MDC.
- **Método 3:** Utilizando a fatoração em números primos como descrito abaixo (acaba sendo o método 2 feito de um modo um pouco diferente).

Tabela 2: MDC de 8 e 12

8	12	2
4	6	2
2	3	2
1	3	3
1	1	4

Fonte: Autor.

Na primeira linha, colocamos os números dos quais calcularemos o MDC, à direita, pomos um número primo que divide pelo menos um dos dois, no caso 2 (que divide ambos), os resultados das divisões colocamos abaixo e repetimos o processo até que ambos os quocientes sejam 1. Por fim, entre os números da última coluna, selecionamos apenas os que dividiram ambos os números das colunas anteriores, o produto de tais números será o MDC.

2.2.5 Algoritmo de Euclides Estendido

O Algoritmo de Euclides Estendido é um método para calcular o MDC de dois números a e b. Como $(a, b) = (|a|, |b|)$, é suficiente considerarmos $a > 0$ e $b > 0$. Tal método consiste em aplicar repetidas vezes o algoritmo da divisão. Isto é:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b \\ b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= r_3q_4 + r_4, \quad 0 < r_4 < r_3 \end{aligned}$$

Como a sequência $b > r_1 > r_2 > \cdots$ é formada por números não negativos, para algum n, $r_{n+1} = 0$. Assim, teremos

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + r_{n+1}, \quad r_n = 0 \end{aligned}$$

Disponhamos essas informações em uma tabela:

Tabela 3: Algoritmo de Euclides Estendido

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-1}	r_n

Fonte: Alencar Filho, (1981)

Vejamos como utilizá-lo através do exemplo anterior:

Tabela 4: Uso do algoritmo de Euclides Estendido

	1	2	
12	8	4	0

Fonte: Autor.

Coloca-se os dois números um ao lado do outro (o maior, mais à esquerda), divide-se um pelo outro, o resultado coloca-se acima do menor número e o resto à direita dos dois números iniciais. Repete-se o processo com o menor número inicial e o resto

obtido anteriormente, divide-se um pelo outro, o resultado coloca-se acima do menor número e o resto à direita dos dois números utilizados na divisão. Ao encontrar o resto 0, o MDC é o número ao lado dele.

2.2.6 Equações Diofantinas Lineares

Uma equação da forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, onde $a_1, ..., a_n, c$ são números inteiros, é chamada de equação diofantina linear geral. Vários problemas de aritmética podem ser resolvidos através da resolução de equações desse tipo. Temos então o seguinte resultado.

Teorema 2.4. *A equação diofantina*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{1}$$

tem solução inteira se, e somente se $(a_1, ..., a_n) \mid c$.

Para provar o teorema anterior, vejamos alguns lemas.

Lema 2.1. *(Bezout) Dados inteiros* a *e* b*, existem inteiros* x *e* y *tais que*

$$ax + by = (a, b).$$

Assim, se c *é inteiro,* $c \mid a$ *e* $c \mid b$*, então* $c \mid (a, b)$.

Demonstração. Se $a = 0$ e $b = 0$ então consideramos $x = y = 0$. Caso contrário, seja $I(a, b)$ o conjunto de todas as combinações lineares com coeficentes inteiros, isto é, a coleção de todos os números da forma $ax + by$ com x e y inteiros. Note que $I(a, b)$ tem algum elemento positivo pois se a e b são diferentes de zero, basta considerar x e y com sinais opostos aos de a e b respectivamente. Se $a = 0$ e $b \neq 0$ então considere $x = 0$ e y com sinal oposto ao de b. Analogamente se $a \neq 0$ e $b = 0$. Seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$. Tal elemento existe, pelo princípio da boa ordem. Afirmação: d divide todos os elementos de $I(a, b)$. Com efeito, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto da divisão de m por d, isto é, $m = dq + r$ com $0 \leq r < d$. Dessa forma, temos

$$r = m - dq = a(x - qx_0) + b(y - qx_0) \in I(a, b). \tag{2}$$

Mas, como $r < d$ e d foi escolhido como o menor elemento positivo de $I(a, b)$, temos $r = 0$ e, pela expressão 2, $d \mid m$.

Ademais, como $a, b \in I(a, b)$, temos que $d \mid a$ e $d \mid b$, e assim $d \leq (a, b)$. Se $c \mid a$ e $c \mid b$ então $c \mid (ax_0 + by_0)$, ou seja, $c \mid d$. Tomando $c = (a, b)$ obtemos $(a, b) \mid d$ que, juntamente com a desigualdade $d \leq (a, b)$, mostra que $d = (a, b)$. □

Lema 2.2. *Sejam $a, b, c \in \mathbb{Z}$. Então a equação $ax + by = c$ possui solução nos inteiros se, e somente se, $(a, b) \mid c$.*

Demonstração. Suponhamos que a equação $ax + by = c$ tem uma solução, isto é, existe um par de inteiros x_0, y_0 tais que $ax_0 + by_0 = c$. Seja $d = (a, b)$, então existem inteiros r e s tais que $a = dr$ e $b = ds$. Logo, $c = drx_0 + dsy_0 = d(rx_0 + sy_0)$. Como $rx_0 + sy_0 \in \mathbb{Z}$, segue-se que $d \mid c$.

Reciprocamente, seja $d = (a, b)$ e suponhamos que $d \mid c$, isto é, $c = dt$, $t \in \mathbb{Z}$. Pelo Lema de Bezout, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$ o que implica: $c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$, isto é, o par de inteiros: $X = tx_0 = (c/d)x_0$ e $Y = ty_0 = (c/d)y_0$ é uma solução da equação $ax + by = c$. □

Passemos agora à demonstração do Teorema 2.4.

Demonstração. Seja $d = (a_1, ..., a_n)$ e suponha inicialmente que a equação (2) tem solução, isto é, existem $x_1, ..., x_n$ tais que $a_1x_1 + \cdots + a_nx_n = c$. Mostraremos que $d \mid c$. De fato, como d divide cada a_i, $i = 1, ..., n$, pela Propriedade 8 da Proposição 2.1, divide toda combinação linear de $a_1, ..., a_n$. Em particular, d divide $a_1x_1 + \cdots a_nx_n = c$.

Reciprocamente, suponha que $(a_1, ..., a_n) \mid c$ e mostremos que a equação tem solução. A prova será feita usando indução. O caso $n = 2$ é o Lema 2.1. Suponha que o resultado é válido para $2, ..., n - 1$ e provemos que vale para n.

Como $(a_1, ..., a_n) = (a_1, (a_2, a_3, ..., a_n))$, pelo Lema de Bezout, existem números inteiros x e y tais que $(a_1, ..., a_n) = a_1x + (a_2, a_3, ..., a_n)y$. Mas, pela hipótese de indução, existem inteiros $x_2, ..., x_n$ tais que $(a_2, a_3, ..., a_n) = a_2x_2 + a_3x_3 + \cdots + a_nx_n$. O que nos dá,

$$(a_1, ..., a_n) = a_1x + \cdots + a_2(x_2y) + \cdots + a_n(x_ny)$$

Pelo princípio de indução finita, o resultado vale para todo $n \geq 2$ finalizando a demonstração. □

Vimos acima que a equação (2) tem solução quando $d \mid c$. Analisaremos como obter explicitamente tais soluções no caso $n = 2$. Antes, vejamos o seguinte lema.

Lema 2.3. *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração. Como $(a, b) = 1$, pelo Lema 2.1, existem inteiros p e q tais que $pa+qb = 1$. Multiplicando ambos os lados por c, temos $p(ac) + q(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$, pela Propriedade 8 da Proposição 2.1, $a \mid c$. □

No próximo resultado, seguiremos a abordagem de Alencar Filho (1981).

Teorema 2.5. *Se $d \mid c$, onde $d = (a, b)$, e se o par de inteiros x_0 e y_0 é uma solução particular da equação diofantina linear $ax + by = c$ então todas as demais soluções desta equação são dadas pelas fórmulas*

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t, \ t \in \mathbb{Z}. \tag{3}$$

Demonstração. Considere o par ordenado (x_0, y_0), uma solução da equação $ax + by = c$ e seja (x_1, y_1) uma outra solução qualquer desta equação. Então,

$$ax_0 + by_0 = c = ax_1 + by_1 \tag{4}$$

e, portanto:

$$a(x_1 - x_0) = b(y_0 - y_1). \tag{5}$$

Como $d = (a, b)$, existem inteiros r e s tais que $a = dr$ e $b = ds$ com r e s primos entre si, isto é $(r, s) = 1$. Substituindo tais valores de a e b na igualdade anterior e cancelando o fator com d, obtemos

$$r(x_1 - x_0) = s(y_0 - y_1). \tag{6}$$

Assim, como $r \mid s(y_0 - y_1)$ e como $(r, s) = 1$, pelo Lema 2.3, temos que $r \mid (y_0 - y_1)$, isto é:

$$y_0 - y_1 = rt \quad e \quad x_1 - x_0 = st,\ t \in \mathbb{Z}. \tag{7}$$

Temos então as fórmulas

$$\begin{aligned} x_1 &= x_0 + st = x_0 + (b/d)t, \\ y_1 &= y_0 - rt = y_0 - (a/d)t. \end{aligned}$$

Tais valores de x_1 e y_1 satisfazem realmente a equação $ax + by = c$, qualquer que seja $t \in \mathbb{Z}$, temos

$$\begin{aligned} ax_1 + by_1 &= a[x_0 + (b/d)t] + b[y_0 - (a/d)t] \\ &= ax_0 + by_0 + (ab/d - ab/d)t \\ &= c + 0 \cdot t \\ &= c. \end{aligned}$$

□

Descobriremos agora uma solução de uma equação diofantina linear utilizando o algoritmo estendido de Euclides combinado com o teorema anterior.

Exemplo 2.4. *Encontre as soluções de* $90x + 28y = 22$.

A equação possui solução pois $2 = (90, 28)$ divide 22. Agora dividiremos a equação por 2, obtendo: $45x + 14y = 11$. Utilizando o algoritmo estendido de Euclides:

$$\begin{aligned} 45 &= 14 \cdot 3 + 3 \\ 14 &= 3 \cdot 4 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

Substituindo do final para o início, obtemos:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 1 &= 3 - (14 - 3 \cdot 4) \cdot 1 \\ 1 &= 3 - 14 + 3 \cdot 4 \\ 1 &= 5 \cdot 3 - 14 \\ 1 &= 5 \cdot (45 - 14 \cdot 3) - 14 \\ 1 &= 5 \cdot 45 - 15 \cdot 14 - 14 \\ 1 &= 5 \cdot 45 - 16 \cdot 14 \end{aligned}$$

Multilicando a última equação por 11, obtemos $11 = 55 \cdot 45 + (-176) \cdot 14$. Portanto $(x, y) = (55, -176)$ é uma solução.

O resultado acima diz que uma solução particular é $(x_0, y_0) = (55, -176)$. As outras soluções são encontradas através das fórmulas: $x = x_0 + tb$ e $y = y_0 - ta$, $t \in \mathbb{Z}$. Ou seja, $x = 55 + 14t$ e $y = -176 - 45t$, $t \in \mathbb{Z}$. Por exemplo, para $t = -4$, obtemos a outra solução $(x, y) = (-1, 4)$.

2.3 Aritmética dos Restos

Definição 2.6. *Sejam $a, b \in \mathbb{Z}$ e m um inteiro positivo. Dizemos que a é congruente a b módulo m se $m \mid (a - b)$ e denotamos por $a \equiv b \ (mod\ m)$. Quando $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b \ (mod\ m)$.*

Exemplo 2.5. $7 \equiv 1 \ (mod\ 3)$*, pois* $3 \mid (7 - 1) = 6$*.*

Exemplo 2.6. $8 \not\equiv 1 \ (mod\ 3)$*, pois* $3 \nmid (8 - 1) = 7$*.*

Como o resto da divisão de qualquer número por 1 é sempre 0, todos os números são congruentes entre si módulo 1. Portanto é suficiente considerar $m > 1$. A proposição seguinte caracteriza a relação de congruência.

Proposição 2.2. *Se $a, b, m \in \mathbb{Z}$ então $a \equiv b \ (mod\ m)$ se, e somente se, $a = b + qm$ para algum inteiro q.*

Demonstração. De fato, $a \equiv b \ (mod\ m)$ se, e somente se, $m \mid (b - a)$, isto é, se e somente se, existe $q \in \mathbb{Z}$ tal que $a - b = mq$. □

Proposição 2.3. *Sejam $a, b, c, d, m \in \mathbb{Z}$, temos:*

1. *Se $a \equiv c \ (mod\ m)$ e $b \equiv d \ (mod\ m)$, então $a + b \equiv (c + d) \ (mod\ m)$.*
2. *Se $a \equiv c \ (mod\ m)$ e $b \equiv d \ (mod\ m)$, então $a \cdot b \equiv c \cdot d \ (mod\ m)$.*

Demonstração. A demonstração decorre da definição de congruência e da Proposição 2.2.

1. Se $a \equiv c \ (mod\ m)$ e $b \equiv d \ (mod\ m)$, então existem inteiros k e q tais que $a - c = mk$ e $b - d = m \cdot q$. Somando as equações anteriores temos, $a - c + b - d = m \cdot k + m \cdot q$, o que nos dá, $a + b = c + d + m(k + q)$, ou seja, $a + b \equiv c + d \ (mod\ m)$.

2. Se $a \equiv c\ (mod\ m)$, então $a - c = m \cdot q$ e se $b \equiv d\ (mod\ m)$, então $b - d = m \cdot k$. Ou seja, $m \mid (a - c)$ e $m \mid (b - d)$. Note que

$$\begin{aligned} ab - cd &= b(a - c) + c(b - d) \\ &= bmq + cmk \\ &= m(bq + ck) \end{aligned}$$

Logo, $m \mid (ad - bc)$ como queríamos.

□

Aplicações sucessivas do item 2, da Proposição 2.3, nos dão o seguinte resultado.

Proposição 2.4. *Sejam $a, b, m \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $a \equiv b\ (mod\ m)$ então $a^n \equiv b^n\ (mod\ m)$.*

Demonstração. Faremos a prova por indução. O caso $n = 1$ foi provado acima. Suponha que $a^n \equiv b^n\ (mod\ m)$ para um certo n. Multiplicando membro a membro por $a \equiv b\ (mod\ m)$ obtemos $a^{n+1} \equiv b^{n+1}\ (mod\ m)$, o que prova o resultado. □

A proposição seguinte mostra que a relação de congruência é uma relação de equivalência.

Proposição 2.5. *Sejam $a, b, c \in \mathbb{Z}$ e m um inteiro positivo. Temos que:*

1. *$b \equiv b\ (mod\ m)$;*
2. *Se $a \equiv c\ (mod\ m)$, então $c \equiv a\ (mod\ m)$;*
3. *Se $a \equiv c\ (mod\ m)$ e $c \equiv b\ (mod\ m)$, então $a \equiv b\ (mod\ m)$.*

Demonstração. 1. Como $m \mid 0$ e $0 = b - b$, obtemos a primeira propriedade.

2. Se $a \equiv c\ (mod\ m)$, então existe $k \in \mathbb{Z}$ tal que $m \cdot k = (a - c)$ o que equivale a $-m \cdot k = (c - a)$. Daí, $m \mid (c - a)$ e $c \equiv a (mod\ m)$.
3. Se $a \equiv c\ (mod\ m)$ e $c \equiv b\ (mod\ m)$ então existem $k, q \in \mathbb{Z}$ tais que $m \cdot k = a - c$ e $m \cdot q = c - b$. Subtraindo membro a membro, obtemos: $m \cdot k - m \cdot q = (a - c) - (c - b) = a - b$. Concluindo que $m \mid (a - b)$, logo $a \equiv b\ (mod\ m)$.

□

No conjunto dos números reais, uma solução da equação $aX = 1$ é chamada de inverso de a. No contexto da aritmética modular, uma solução da equação de congruência $aX \equiv 1\ (mod\ m)$ é chamada de inverso de a módulo m. Veremos quando um número a tem um inverso módulo m. Antes porém, vejamos o seguinte resultado que diz em quais circunstâncias vale a lei do corte para congruências.

Lema 2.4. *Se a, b, c e m são inteiros com $c \neq 0$, e $ac \equiv bc\ (mod\ m)$ então $a \equiv b\ (mod\ \frac{m}{d})$ onde $d = (c, m)$.*

Demonstração. Como $ac \equiv bc\ (mod\ m)$, existe um número inteiro k tal que $ac - bc = km$. Dividindo os dois lados por d, obtemos $(c/d)(a - b) = k(m/d)$. Logo $(m/d) \mid (c/d)(a - b)$ e,

como $(m/d, c/d) = 1$, pelo Lema 2.3, $(m/d) \mid (a-b)$ o que implica $a \equiv b \ (mod\ m/d)$. □

Estamos agora em condições de provar o Teorema de Euler.

Teorema 2.6. *(Teorema de Euler) Sejam $a, m \in \mathbb{Z}$, $m > 1$. A congruência $aX \equiv 1 \ (mod\ m)$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ for solução, então x_1 é solução da congruência se, e somente se, $x_1 \equiv x_0 \ (mod\ m)$.*

Demonstração. Pela Proposição 2.2, temos que x_0 é uma solução da congruência se, e somente se, $ax_0 - 1 = m \cdot k$, para algum $k \in \mathbb{Z}$, ou seja, a equação diofantina $aX + mY = 1$ possui solução inteira. Pelo Teorema 2.4, isso ocorre se, e somente se, $(a, m) = 1$.

Se x_1 e x_0 são soluções de $aX \equiv 1 \ (mod\ m)$, então $ax_0 \equiv 1 \ (mod\ m)$ e $ax_1 \equiv 1 \ (mod\ m)$. Pela Propriedade 3 da Proposição 2.5 temos $ax_1 \equiv ax_0 \ (mod\ m)$. Pelo Lema 2.4, como $(a, m) = 1$, obtemos $x_1 \equiv x_0 (mod\ m)$.

Reciprocamente, suponha que $x_1 \equiv x_0 \ (mod\ m)$ e que $ax_0 \equiv 1 \ (mod\ m)$. Assim, obtemos $ax_1 \equiv ax_0 \ (mod\ m)$ e, novamente pela Propriedade 3 da Proposição 2.5, $ax_1 \equiv 1 \ (mod\ m)$. Concluindo a demonstração do teorema. □

Enunciamos agora os Teoremas de Fermat e Wilson. Eles serão usados no jogo de dominó proposto no Capítulo 4 e num problema do capítulo 3. A demonstração desses resultados bem como do Teorema de Zeller que virá na sequência podem ser encontradas em Hefez (2015).

Teorema 2.7. *(Pequeno Teorema de Fermat) Se p é primo e $p \nmid a$ então*

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

Corolário 2.1. *Se p é primo e a é um número inteiro positivo, então $a^p \equiv a \ (mod\ p)$.*

Teorema 2.8. *(Wilson) Se p é um número primo, então*

$$(p-1)! \equiv -1 \ (mod\ p).$$

O Teorema de Zeller é um método utilizado para determinar em qual dia da semana uma data ocorreu. Expliquemos a notação usada em tal resultado. As letras d, m e A denotam o dia, o mês e o ano de uma data, respectivamente. Os dias da semana são representados por: domingo = 1, segunda = 2 e assim sucessivamente. Quanto aos meses, temos: Março = 1, Abril = 2, Maio = 3, e assim por diante, até Janeiro = 11 e Fevereiro = 12. Se a data for nos meses de Janeiro ou Fevereiro, deve ser considerado o ano anterior, por exemplo, em 5 de Janeiro de 2018, $d = 5$, $m = 11$ e $A = 2017$. A notação $[x]$ representará o maior número inteiro que não supera x. Assim, por exemplo, $[2, 1] = 2$, $[2, 9] = 2$, $[\pi] = 3$ e $[e] = 2$.

Teorema 2.9. *(Teorema de Zeller)*

$$s(d,m,A) = d + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] (mod\ 7)$$

O Teorema de Zeller é tratado também por Lage (2018). No referido trabaho são feitas atividades com alunos do Ensino Fundamental (oitavo e nono ano) da rede privada e do Ensino Médio (primeiro ano) da rede estadual.

Exemplo 2.7. *Em que dia da semana foi* 7 *de setembro de* 2017*?*
Pelo Teorema de Zeller,

$$\begin{aligned} s(7,7,2017) &= 7 + 1 + \left[\frac{13.7-1}{5}\right] + 2017 + \left[\frac{2017}{4}\right] - \left[\frac{2017}{100}\right] + \left[\frac{2017}{400}\right] (mod\ 7) \\ &= 8 + 18 + 2017 + 504 - 20 + 5\ (mod\ 7) \\ &= 2532\ (mod\ 7) \\ &= 5\ (mod\ 7) \end{aligned}$$

Ou seja, quinta-feira.

3 OLIMPÍADAS E INTERNET

Neste capítulo, voltamos nossa atenção para o uso da aritmética modular para resolver problemas de olimpíadas e testes de admissão bem como para o uso de sites que podem auxiliar o professsor no ensino desse tópico.

3.1 Aritmética Modular em Olimpíadas/Exames de Admissão

Veremos agora alguns problemas de olimpíadas ou de exames de admissão que podem ser resolvidos usando aritmética modular.

Exemplo 3.1. *(Colégio Naval - 2007) Qual será o dia da semana na data 17 de setembro de 2009?*

Solução: Utilizando o Teorema de Zeller com $d = 17$, $m = 7$ e $A = 2009$, obtemos

$$\begin{aligned} s(17,7,2009) &= 17 + 1 + \left[\frac{13\cdot 7 - 1}{5}\right] + 2009 + \left[\frac{2009}{4}\right] - \left[\frac{2009}{100}\right] + \left[\frac{2009}{400}\right] \ (mod\ 7) \\ & \quad 18 + 18 + 2009 + 502 - 20 + 5 \ (mod\ 7) \\ &= 2532 \ (mod\ 7) \\ &= 5 \ (mod\ 7) \end{aligned}$$

Ou seja, quinta-feira.

Exemplo 3.2. *(XXXIV Olimpíada Cearense de Matemática) Faça os seguintes itens:*

1. *Prove que existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2013$.*
2. *Prove que não existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2014$.*

Fazendo $z = 2x$, obtemos $y^4 - x^4 = 671$ ou, ainda, $(y^2 - x^2)\cdot(y^2 + x^2) = 11\cdot 61$. Portanto, $y^2 - x^2 = 11$ e $y^2 + x^2 = 61$, de forma que $x = 5$, $y = 6$ e $z = 10$.

Para solucionar o segundo item, suponha que existe uma solução. Como $a^4 \equiv 0$ ou $1\ (mod\ 8)$, temos $13x^4 + 3y^4 - z^4 \equiv 0, 2, 4, 5$ ou $7\ (mod\ 8)$. Mas, como $2014 \equiv 6\ (mod\ 8)$, chegamos a uma contradição.

Exemplo 3.3. *(OBM 2012) Para homenagear a Copa do Mundo e as Olimpíadas no Brasil, Esmeralda, a prefeita da cidade Gugulândia, decidiu que seria feriado em sua cidade no dia x do mês de número y, onde x é o último algarismo do número 2016^{2014} e y é o resto de 2014^{2016} na divisão por 11. Assim, esse feriado será no dia:*

Para calcular x, notamos que $2016 \equiv 6\ (mod\ 10)$ e $6^n \equiv 6\ (mod\ 10)$, para todo natural n. Então, pela propriedade 3 da proposição 2.5, temos $2016^{2014} \equiv 6\ (mod\ 10)$, ou seja, dia 6. Analogamente, para calcularmos y, percebemos que $2014 \equiv 1\ (mod\ 11)$ e $1^{2016} \equiv 1\ (mod\ 11)$, então $2014^{2016} \equiv 1\ (mod\ 11)$, ou seja, mês 1.

Exemplo 3.4. *(IME 2000) Prove que os inteiros k e k^5 têm o mesmo algarismo das unidades.*

Dois números têm o mesmo último dígito se, e somente se, a diferença entre eles é múltiplo

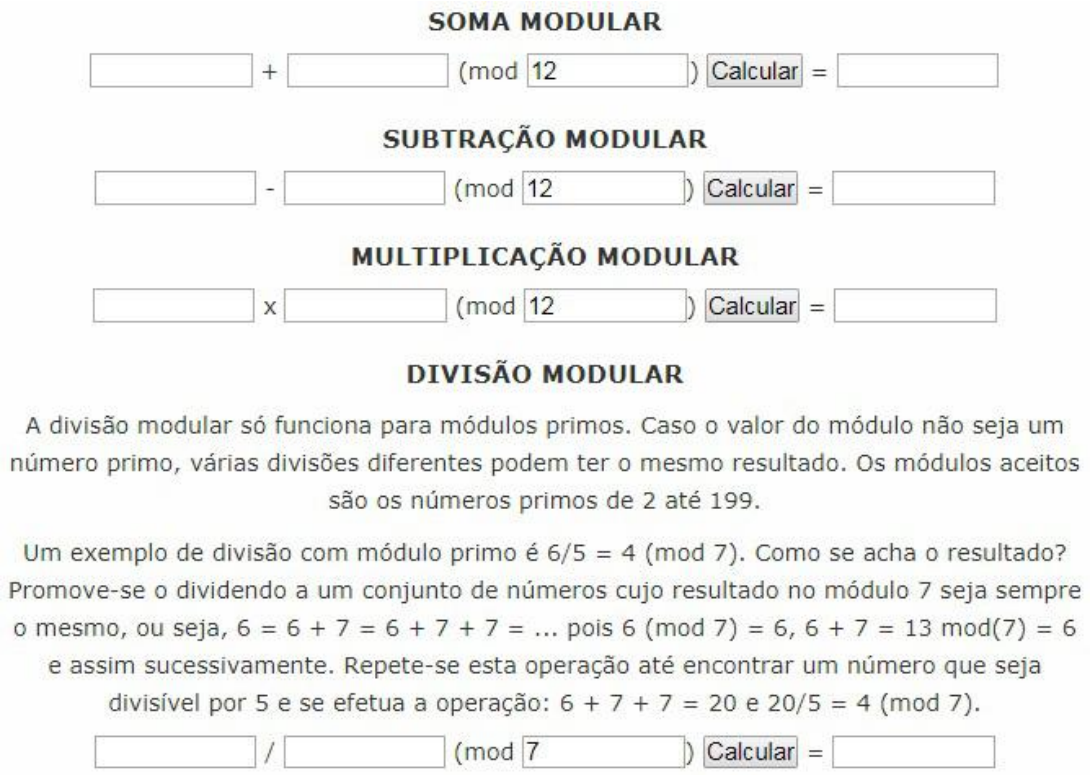
de 10. Para mostrar que um número é multiplo de 10 basta mostrar que ele é múltiplo de 2 e de 5. Como $D := k^5 - k = (k-1)k(k+1)(k^2+1)$ e k, $k+1$ são consecutivos, D é múltiplo de 2. Se k for múltiplo de 5, não há mais o que fazer. Caso contrário, notamos que, como 5 é primo e $k \in \mathbb{Z}$, pelo corolário do Pequeno Teorema de Fermat, $k^5 \equiv k \ (mod\ 5)$, ou seja, k^5 é múltiplo de 5.

3.2 Aritmética Modular com o Uso de Sites

Nesta seção, sugerimos alguns sites que podem ser usados para auxiliar o professor em sala de aula. Eles poderiam ser utilizados ao final da explicação de todo o conteúdo ou, de preferência, no decorrer das aulas.

O site *numaboa* possui uma ferramenta interessante pois permite a realização de operações modulares escolhendo-se o módulo e os valores, como pode ser observado na imagem abaixo.

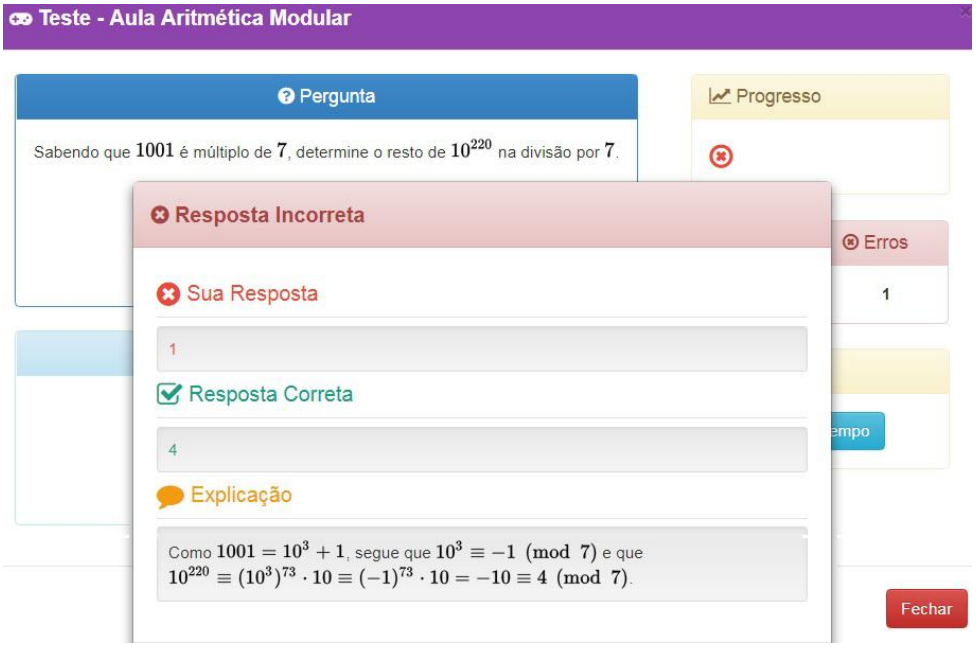
Figura 1: Operações com Aritmética Modular.



Fonte: [1]

POTI-(Polos Olímpicos de Treinamento Intensivo) é outra ferramenta interessante pois além de abordar o conteúdo, apresenta video-aulas com exemplos e propõe diferentes questões sobre Aritmética Modular exigindo que o aluno raciocine e lembre das definições, propriedades e teoremas, podendo ser apresentado depois que o aluno estudar todo o conteúdo.

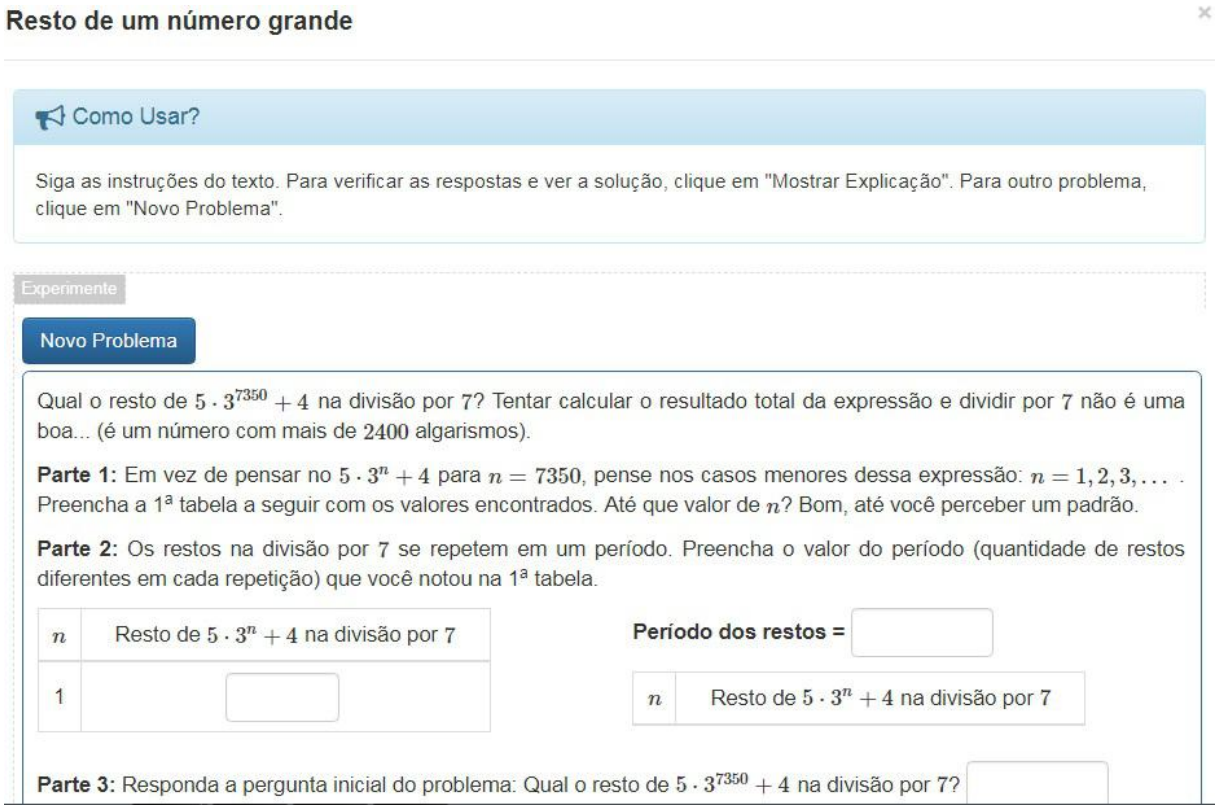
Figura 2: Exemplo de questão que pode ser exercitada pelo aluno no site.



Fonte: [24]

No *Portal do Saber* há explicações dos conteúdos, vídeo-aulas e é possível resolver algumas questões sobre como encontrar o resto de uma divisão, entre outros assuntos. Este site é um pouco diferente do site anterior que trazia questões aleatórias sobre Aritmética Modular. No Portal do Saber há um direcionamento específico.

Figura 3: Questão sobre resto de divisão de número grande.



Fonte: [23]

4 APLICAÇÕES NO COTIDIANO E NO ENSINO

Neste capítulo, estudaremos alguns tópicos que podem ser compreendidos com o uso de técnicas de aritmética modular. Abordaremos os critérios de divisibilidade por 3, 9, 10 e 11. Veremos como são determinados alguns dígitos na criação de CPF e ISBN, a razão para a falha da prova dos noves em algumas situações, aplicações de equações diofantinas além de um jogo de dominó, adaptável para outras situações, para verificar o aprendizado do assunto. Começamos apresentando livros que trazem critérios de divisibilidade.

4.1 Divisibilidade em Livros do Ensino Básico

Chamamos atenção para o fato de alguns livros do 6º ano do Ensino Fundamental apresentarem critérios de divisibilidade como, por exemplo, Bianchini (2015) e Andrini e Vasconcelos (2012) os quais, entre outros, trazem critérios de divisibilidade por 3, 9 e 10. O critério de divisibilidade por 11 não aparece nos livros citados mas o apresentaremos pois o usaremos para mostrar uma aplicação no estudo de CPF.

4.1.1 Critérios de Divilibilidade

Existem métodos simples para verificar se um número pode ser dividido por outro. Os critérios de divisibilidade estão presentes em livros didáticos do Ensino Fundamental, mas sem a devida explicação do motivo de funcionarem. Selecionamos os critérios de divisibilidade por 3, 9, 10 e 11. A abordagem que faremos é baseada em Santos (2006).

Começaremos com os critérios de divisibilidade por 3 e por 9.

Teorema 4.1 (Critério de divisibilidade por 3, 9)**.** *Um inteiro com representação decimal* $P = a_n a_{n-1}...a_0$ *é divisível por* 3*, (resp. por* 9*) se, e somente se* $S_P = a_n + a_{n-1} + \cdots + a_0$ *for divisível por* 3*, (resp. por* 9*).*

Demonstração. Note que

$$P = a_n a_{n-1}...a_0 = a_0 + a_1 \cdot 10 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n.$$

Fazendo as substituições: $10 = 9 + 1$, $100 = 99 + 1$, $10^{n-1} = \overbrace{99...9}^{n-1\ termos} +1,...,10^n =$

$\overbrace{99...9}^{n\ termos}+1$, obtemos

$$\begin{aligned} P &= a_0 + a_1(9+1) + \cdots + a_{n-1}\overbrace{(9...9+1)}^{n-1\ termos\ 9} + a_n\overbrace{(9...9+1)}^{n\ termos\ 9} \\ &= a_0 + a_1 \cdot 9 + a_1 + \cdots + \overbrace{a_{n-1} \cdot 9...9}^{n-1\ termos\ 9} + a_{n-1} + \overbrace{a_n \cdot 9...9}^{n\ termos\ 9} + a_n \\ &= a_0 + a_1 + \cdots + a_{n-1} + a_n + 9 \cdot k \\ &= S_P + 9 \cdot k, \end{aligned}$$

onde $k = a_1 + 11 \cdot a_2 + \cdots + \overbrace{11...1}^{n\ termos} \cdot a_n$. Donde conluímos que P é divisível por 3, (resp. por 9) se, e somente se, $S_P = a_n + a_{n-1} + \cdots + a_1 + a_0$ for divisível por 3, (resp. por 9). □

Exemplo 4.1. *(EsPCEx) No número $y = 34n27$, qual é o valor possível para o algarismo n para que y seja divisível por 9?*
A soma dos algarismos de y é $S_y = 3+4+n+2+7 = 16+n$. O critério de divisibilidade por 9 diz que y é divisível por 9 se, e somente se, S_y for divisível por 9. Como os possíveis valores para o algarismo n são $0, 1, ..., 9$, o único valor de n que torna S_y divisível por 9 é $n = 2$.

Inspirados no exemplo acima, propomos os seguintes exercícios:

Exercício 4.1. *No número $x = 34m2732n31$, quais são os valores possíveis para os algarismos m e n para que x seja divisível por 9?*

Exercício 4.2. *No número $x = 34m2732n31$, quais são os valores possíveis para os algarismos m e n para que y seja divisível por 3?*

A Aritmética Modular tem uma série de aplicações em nosso cotidiano. Veremos algumas delas que por si só já motivariam o ensino dessa disciplina em turmas da Educação Básica. Uma dessas aplicações é a possibilidade de determinar dígitos de certos números como, por exemplo, os números de CPF e de ISBN. Tais números têm dígitos especiais chamados dígitos verificadores ou de controle.

Veremos a seguir os critérios de divisibilidade por 10 e por 11, os quais serão usados para estudar a confecção de CPF e ISBN, respectivamente.

Teorema 4.2 (Critério de divisibilidade por 10)**.** *Um número $P = a_n a_{n-1}...a_2 a_1 a_0$ é divisível por 10 se, e somente se, $a_0 = 0$.*

Demonstração. De fato, temos que

$$\begin{aligned} P &= a_n a_{n-1}...a_2 a_1 0 + a_0 \\ &= a_n a_{n-1}...a_2 a_1 \cdot 10 + a_0. \end{aligned}$$

Portanto, P é divisível por 10 se, e somente se, a_0 for igual a zero. □

A prova do resultado anterior mostra ainda que o resto da divisão de um número P por 10 é igual ao dígito das unidades de P.

Antes de analisarmos o critério de divisibilidade por 11, vejamos o seguinte resultado.

Lema 4.1. *As seguintes afirmações são verdadeiras:*

1. *Todo número da forma* $99...99$ *onde o número de algarismos* 9 *é par, é divisivel por* 11*.*
2. *Todo número da forma* $100...001$ *onde o número de algarismos* 0 *é par, é divisível por* 11*.*

Demonstração. Para provarmos 1., notemos que

$$\begin{aligned}
9999 &= 9900 + 99 = 11 \cdot 909,\\
999999 &= 999900 + 99 = 11 \cdot 90909,\\
99999999 &= 99999900 + 99 = 11 \cdot 9090909,\\
9999999999 &= 9999999900 + 99 = 11 \cdot 909090909,\\
\cdots\cdots\cdots\cdots &\cdots \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\overbrace{99999\cdots99999}^{2n\ termos} &= \overbrace{99999\cdots99999}^{2n-2\ termos}00 + 99 = 11 \cdot \overbrace{9090\cdots9090}^{n-1\ termos\ 90}9.
\end{aligned}$$

Quanto à prova de 2., percebamos que

$$\begin{aligned}
1001 &= 990 + 11 = 11 \cdot 91,\\
100001 &= 99990 + 11 = 11 \cdot 9091,\\
10000001 &= 9999990 + 11 = 11 \cdot 909091,\\
1000000001 &= 999999990 + 11 = 11 \cdot 90909091,\\
\cdots\cdots\cdots\cdots &\cdots \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
1\overbrace{0000\cdots0000}^{2n\ termos}1 &= \overbrace{99999\cdots99999}^{2n\ termos}0 + 99 = 11 \cdot \overbrace{9090\cdots9090}^{n-1\ termos\ 90}91,
\end{aligned}$$

como queríamos. □

Teorema 4.3 (Critério de divisibilidade por 11)**.** *Os seguintes fatos são verdadeiros:*

1. *O inteiro* $P = a_{2n}a_{2n-1}...a_3a_2a_1a_0$ *é divisível por* 11 *se, e somente se,*

$$S_P := a_0 - a_1 + a_2 - a_3 - \cdots - a_{2n-1} + a_{2n}$$

   é divisível por 11*.*

2. *O inteiro* $P = a_{2n-1}a_{2n-2}...a_3a_2a_1a_0$ *é divisível por* 11 *se, e somente se,*

$$S_P := a_0 - a_1 + a_2 - a_3 + \cdots + a_{2n-2} - a_{2n-1}$$

   é divisível por 11*.*

Isto é, um número P é divisível por 11 *se, e somente se, a soma alternada dos algarismos de P for divisível por* 11.

Demonstração. Para provar 1, usaremos as substituições $10 = 11 - 1$, $10^2 = 99 + 1$, $10^3 = 1001 - 1$,...,$10^{2n-1} = \overbrace{100..001}^{2n-2 \text{ termos } 0} - 1$, $10^{2n} = \overbrace{99..99}^{2n \text{ termos}} + 1$, temos que,

$$\begin{aligned}
P &= a_{2n}a_{2n-1}...a_3a_2a_1a_0 \\
&= a_{2n}10^{2n} + a_{2n-1} \cdot 10^{2n-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\
&= a_{2n}(\overbrace{99...99}^{2n \text{ termos}} + 1) + a_{2n-1}(\overbrace{100...001}^{2n-2 \text{ termos } 0} - 1) + \cdots + a_3(1001 - 1) \\
&\quad + a_2(99 + 1) + a_1(11 - 1) + a_0 \\
&= \overbrace{99...99a_{2n} + 100..001a_{2n-1} + \cdots + 1001a_3 + 99a_2 + 11a_1}^{I} \\
&\quad + \overbrace{a_{2n} - a_{2n-1} - \cdots - a_3 + a_2 - a_1 + a_0}^{S_P}.
\end{aligned}$$

Pelo Lema 4.1, o termo I acima é divisível por 11. Assim, P é divisível por 11 se, e somente se, S_P for divisível por 11. O caso 2, em que P tem uma quantidade par de algarismos, é provado de modo similar. □

Vejamos um exemplo:

Exemplo 4.2. *O número* 5432 *não é divisível por* 11 *uma vez que* $2-3+4-5 = -2$ *que não é divisível por* 11 *mas, o número* 9482 *é divisível por* 11 *pois* $2 - 8 + 4 - 9 = -11$*, que é divisível por* 11.

4.2 CPF

O Cadastro de Pessoa Física (CPF) é um conjunto de 11 números que serve para identificação de uma pessoa. Os dois últimos números são dígitos verificadores (ou de controle) e são calculados assim: multiplica-se o primeiro número por 1, o segundo por 2, o terceiro por 3, até o nono que deve ser multiplicado por 9. Soma-se os resultados obtidos e calcula-se o resto da divisão por 11, tal resto será o primeiro dígito de controle, exceto se tal resto for 10, situação em que o dígito será 0. Para o segundo dígito de controle multiplica-se o segundo número por 1, o terceiro por 2, o quarto por 3 até o décimo número que deve ser multiplicado por 9, soma-se os resultados obtidos e divide-se por 11, o segundo dígito de controle é o resto dessa divisão. Como antes, se tal resto for 10, o dígito verificador será 0.

Exemplo 4.3. *Quais os últimos dígitos de uma pessoa com CPF:* $043.864.653 - XX$*?*
Temos,

$$0 \cdot 1 + 4 \cdot 2 + 3 \cdot 3 + 8 \cdot 4 + 6 \cdot 5 + 4 \cdot 6 + 6 \cdot 7 + 5 \cdot 8 + 3 \cdot 9 = 212,$$

que dividido por 11 deixa resto 3, logo o primeiro dígito de controle é 3. Para a determinação do segundo dígito, calculamos

$$4 \cdot 1 + 3 \cdot 2 + 8 \cdot 3 + 6 \cdot 4 + 4 \cdot 5 + 6 \cdot 6 + 5 \cdot 7 + 3 \cdot 8 + 3 \cdot 9 = 200,$$

que dividido por 11 deixa resto 2. Logo, o CPF dessa pessoa é: $043.864.653 - 32$.

4.3 ISBN

International Standard Book Number (ISBN), é um sistema que serve para catalogação de livros, trabalhos de final de curso, mapas de guia de turismo, etc. Identifica-se o país, o autor, o título, editora, facilitando inclusive a comercialização. Atualmente possui 13 dígitos e apenas o último é de controle. Para calculá-lo, deve-se multiplicar o primeiro número por 1, o segundo por 3, o terceiro por 1, o quarto por 3 e assim sucessivamente até o décimo segundo número, que deve ser multiplicado por 3, soma-se os resultados obtidos e divide-se o resultado por 10, o dígito de controle é a diferença entre 10 e o resto dessa divisão.

Exemplo 4.4. *Qual o dígito de controle do ISBN* $978 - 85 - 426 - 1146-?$
Devemos calcular o resto da divisão do número

$$9 \cdot 1 + 7 \cdot 3 + 8 \cdot 1 + 8 \cdot 3 + 5 \cdot 1 + 4 \cdot 3 + 2 \cdot 1 + 6 \cdot 3 + 1 \cdot 1 + 1 \cdot 3 + 4 \cdot 1 + 6 \cdot 3 = 125$$

por 10, isto é, 5. Portanto, o dígito de controle é igual a $10 - 5 = 5$.

Vale ressaltar que os dígitos de controle ajudam na detecção de erros mas não de todos os tipos. Por exemplo, se uma pessoa digitasse para o ISBN anterior $978 - 85 - 484 - 1146 - 5$, ou seja, trocasse 26 por 84 não seria detectado o erro. Quanto maior a quantidade de dígitos de controle, maior a chance de encontrar erros. Os dígitos de controle detectam mais facilmente trocas de posições de números, que é o que ocorre com mais facilidade.

4.4 Prova dos Noves

Nesta seção abordaremos a prova dos noves, um procedimento antigo que por muito tempo foi usado para verificar se uma das quatro operações: adição, subtração, multiplicação ou divisão, havia sido feita corretamente. No livro "Elementos de Arithmetica" de João José Luiz Viana, publicado em 1906 já pode ser encontrada a prova dos noves para cada uma das quatro operações. Apenas para ilustrar, apresentaremos a seguir, a prova dos noves presente em tal livro para a multiplicação.

Relembremos que em uma multiplicação, o primeiro número chama-se multiplicando; o segundo, chama-se multiplicador; e o terceiro, produto.

Teorema 4.4 (Prova dos noves para a multiplicação, [31])**.** *Tiram-se os noves ao multi-*

plicando e ao multiplicador; multipicam-se os dois restos, e tiram-se os noves ao resultado; tirando depois os noves do produto, os dois restos devem ser iguais.

Demonstração. Sejam A o multiplicando e B o multiplicador, AB será o produto. Pelo algoritmo da divisão, podemos escrever o multiplicando e o multiplicador, respectivamente como $A = 9Q + R$ e $B = 9Q' + R'$, onde $0 \leq R < 9$ e $0 \leq R' < 9$.

Multiplicado membro a membro tais expressões para A e B, obtemos

$$\begin{aligned} AB &= 9^2QQ' + 9Q'R + 9QR' + RR' \\ &= 9(9QQ' + Q'R + QR') + RR'. \end{aligned}$$

Logo, o resto da divisão do produto AB por 9 é igual ao resto da divisão por 9 do produto RR' dos restos que se obtém tirando os 9 do multiplicando e do multiplicador. □

Podemos aplicar a Aritmética Modular para entender porque a prova dos noves indica apenas eventualmente erros mas nunca acertos. Analisando a regra descrita no Teorema 4.4, percebemos que devem ser calculados os noves fora do multiplicando e do multiplicador e que deve ser calculado o noves fora do produto dos resultados. Este, por sua vez, deve ser igual ao noves fora do produto. Como calcular noves fora de um número p significa calcular q, com $0 \leq q < 9$, tal que $p \equiv q \ (mod\ 9)$, isso quer dizer que se a diferença entre os dois números finais acima for múltiplo de 9 então a prova dos noves indicará que a conta está certa mesmo que possa não estar. Em outras palavras, a validez da prova dos noves em uma multiplicação é necessária mas não é suficiente para que a operação esteja correta.

Veremos a seguir três exemplos: o primeiro com resposta correta, o segundo com resposta incorreta cujo erro é detectado pela prova dos noves e, finalmente, o terceiro com um erro que não é detectado.

Exemplo 4.5. *Verifique através da prova dos noves se a multiplicação* $78 \cdot 45 = 3510$ *está errada.*

Ao somarmos os algarismos de 78 encontramos 15, que tirando 9, obtemos 6. Fazendo o mesmo para 45 encontramos 0. Multiplicando ambas as respostas obtemos 0. Para conferir, somamos os algarismos de 3510, tiramos 9 e obtemos 0. Como obtivemos o mesmo valor, a resposta pode estar correta embora não possamos ter certeza disso. Porém, se com a prova dos noves não tivéssemos obtido o mesmo resto, então a multiplicação estaria errada. O próximo exemplo ilustra isso.

Exemplo 4.6. *Verifique através da prova dos noves se a multiplicação* $78 \cdot 45 = 3511$ *está errada.*

Como vimos no exemplo 4.5 acima, o noves fora do produto dos noves fora do multiplicando e do multiplicador é 0. Porém agora, o noves fora do produto é igual a 1. Neste caso, podemos assegurar que a operação está errada pois a prova dos noves não foi satisfeita.

Exemplo 4.7. *Um estudante realizou a seguinte operação* $17 \cdot 3 = 42$. *Verifique através da prova dos nove se ele errou.*
Ao somarmos os algarismos de 17, encontramos 8 que, multiplicado por 3, resulta 24, que ao retirarmos 9 duas vezes, obtemos 6. Ao somarmos os algarismos de 42, encontramos 6, como obtivemos o mesmo valor, a resposta pode estar correta.

Como sabemos, $17 \cdot 3 = 51$ e, portanto, a resposta acima não está correta. Acontece que foi encontrado $42 = 51 - 9$ como resposta, valor que deixa resto igual ao deixado por 24 ao ser dividido por 9 induzindo-nos a acreditar que a conta está correta, quando, na verdade, não está.

Talvez por causa de exemplos como o 4.7, a prova dos noves praticamente não seja mais ensinada em salas de aula. A esse respeito, Freitas et al. (2016), escreveram

> a prova dos nove remotamente ainda é usada nos dias atuais, seja por algum comerciante local ou por alguns professores do Ensino Fundamental em momentos de Extensão, fato observado na extensão ocorrida no Dia Nacional da Matemática no Colégio de Aplicação Cap/UFAC (2012). (Freitas et. al 2016, p. 10).

De qualquer modo, a prova dos noves é um método prático que serve para verificação da resposta, tornando-a mais confiável. Sugerimos que no lugar de deixar a prova dos noves renegada ao esquecimento, os professores da educação básica a ensinem aos alunos deixando claro que ela serve para detectar certos tipos de erros (mas não todos) e enfatizem que ela não serve para garantir que uma operação está correta. Uma abordagem detalhada da prova dos noves para as quatro operações pode ser encontrada em Ferreira (2017).

4.5 Polinômios

Aritmética Modular pode ser usada para calcular o resto da divisão de polinômios, conteúdo estudado no Ensino Médio usando outras técnicas. Vejamos um exemplo desse fato.

Exemplo 4.8. *(IME) Prove que* $P(x) = x^{999} + x^{888} + x^{777} + ... + x^{111} + 1$ *é divisível pelo polinômio* $D(x) = x^9 + x^8 + x^7 + \cdots + x + 1$.
Como $x^{10} - 1 = (x-1)(x^9 + x^8 + \cdots + x + 1)$, usando a notação de congruência temos que $x^{10} - 1 \equiv 0 \ (mod\ x^9 + x^8 + \cdots + x + 1)$, ou $x^{10} \equiv 1 \ (mod\ x^9 + x^8 + \cdots + x + 1)$. Assim, todas as potências de x^{10} de $P(x)$ podem ser substituídas pelo número 1, daí:

$$\begin{aligned} P(x) &= x^{999} + x^{888} + x^{777} + \cdots + x^{111} + 1 \\ &= x^9 \cdot (x^{10})^{99} + x^8 (x^{10})^{88} + \cdots + x(x^{10})^{11} + 1 \\ &\equiv x^9 + x^8 + x^7 + \cdots + x + 1 \ (mod\ x^9 + x^8 + x^7 + \cdots + x + 1) \\ &\equiv 0 \ (mod\ x^9 + x^8 + x^7 + \cdots + x + 1). \end{aligned}$$

Logo, $P(x)$ é divisível por $D(x)$.

4.6 Aplicações de Equações Diofantinas

Veremos a seguir algumas aplicações de Equações Diofantinas.

Aplicação 1: (Caixas Eletrônicos) Ao usar um caixa eletrônico você já se perguntou como ele consegue decidir se a quantia pedida poderá ser retirada?

Por exemplo, se um caixa eletrônico só possui notas de 20 e 50 reais, então não é possível retirar 115 reais. De fato, três notas de 50 ou 6 notas de 20 totalizam 150 e 120 respectivamente, valores superiores a 115. Analogamente, duas notas de 50 ou 5 notas de 20 resultam no valor comum 100. Além disso, é simples perceber que a soma de qualquer quantidade de notas de 20 com qualquer quantidade de notas de 50 será sempre menor ou maior do que 115 reais.

Se nesse mesmo caixa eletrônico alguém tentasse sacar 510 reais e não fosse permitida a transação o que poderia ter ocorrido, visto que $3 \cdot 20 + 9 \cdot 50 = 510$ e assim, deveria ser possível retirar 510 reais? Acontece que o caixa pode não ter a quantidade de notas suficiente para realizar a transação.

Nos dois casos acima, apareceria a mensagem "Quantia não pode ser paga. Digite outro valor."

Os softwares dos caixas eletrônicos possuem um sistema de contagem de notas e, provavelmente, um sistema que resolve equações diofantinas lineares para que possa, de forma rápida, mostrar uma mensagem na tela quando uma pessoa tenta realizar uma operação e não é permitido por conta de não existir solução para a equação ou devido à quantidade de notas disponíveis no interior do caixa.

Nas situações acima, devem ser resolvidas as equações diofantinas lineares $20x + 50y = 115$ e $20x + 50y = 510$. A primeira não tem solução pois $(20, 50) = 10$ que não divide 115 enquanto no segundo caso, embora 10 divida 510, a quantidade de cédulas disponível no caixa devia não ser suficiente.

Como, no Brasil, existem cédulas disponíveis de 2, 5, 10, 20, 50 e 100 reais, ao solicitar uma quantia p em um caixa que contivesse cédulas de cada um desses valores, o caixa deveria resolver a equação diofantina

$$2\alpha + 5\beta + 10\gamma + 20\delta + 50\varphi + 100\psi = p.$$

Como $(2, 5, 10, 20, 50, 100) = 1$, qualquer valor deveria poder ser pago. Mas não é bem assim! Por exemplo, o valor $p = 3$ não pode ser pago pois, embora a equação tenha solução ($\alpha = -1$, $\beta = 1$, $\gamma = \delta = \varphi = \psi = 0$ é uma delas), alguma das entradas do vetor das variáveis $(\alpha, \beta, \gamma, \delta, \varphi, \psi)$ tem que ser negativa, o que inviabiliza o pagamento.

Aplicação 2: (Indo à Festa) Em um clube, o ingresso custa 18 reais para cada homem e 12 reais para cada mulher. Sabendo que em uma noite foram arrecadados 2652 reais,

qual é o maior número de mulheres que pode ter entrado sabendo que havia homens e mulheres na festa? Em outra noite, mantidos os valores dos ingressos, é possível arrecadar 1450 reais?

Sejam H o número de homens e M o número de mulheres que entraram na festa. Podemos transformar o problema na tarefa de resolver a equação diofantina

$$18H + 12M = 2652, \tag{8}$$

que pode ser resolvida como fizemos no Exemplo 2.4. A equação possui solução pois $6 = (18, 12)$ divide 2652. Utilizando o algoritmo estendido de Euclides, obtemos:

$$\begin{aligned} 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Escrevendo a primeira das equações acima como $6 = 18 - 12$ e multiplicando por $442 = 2652/6$, obtemos

$$2652 = 442 \cdot 18 - 442 \cdot 12, \tag{9}$$

o que significa que $(H_0, M_0) = (442, -442)$ é uma solução da equação 8. Pelo Teorema 2.5, todas as soluções de 8 podem ser encontradas por meio das fórmulas $H = 442 + 2t$, $M = -442 - 3t$, $t \in \mathbb{Z}$. Para que H e M sejam positivos, t deve satisfazer $-221 < t < -(442/3) \approx -147,33$. Por exemplo, se $t = -148$ então $(H, M) = (146, 2)$. Como entraram homens e mulheres, devemos ter $H \neq 0$, e $M \neq 0$. Assim, o maior valor possível para M é obtido ao considerarmos $t = -220$, que origina a solução $(H, M) = (2, 218)$. Portanto, o maior número de mulheres que pode ter entrado é $M = 218$.

Como 6 não divide 1450, a equação $18H + 12M = 1450$ não tem soluções inteiras, isto é, não existem quantidades de homens e mulheres que possibilitem arrecadar 1450 reais.

4.7 Relato de Experiência do Autor

Cursei Licenciatura em Matemática pela Universidade Federal do Ceará e sou professor efetivo na Rede Estadual de Ensino do Ceará desde 2014. Certa vez, ao ministrar uma aula, um aluno me questionou: "Professor, por que o senhor não faz uma aula diferente?" Esse questionamento me fez querer melhorar minhas aulas, então busquei uma especialização. Fiz Especialização *lato sensu* em Ensino de Matemática pela Universidade Estadual do Ceará.

Diferentemente do que ocorreu na graduação, na especialização, o uso de jogos e tecnologia em sala de aula, foi bastante discutido em algumas disciplinas e no quanto é importante para o desenvolvimento do aluno.

Ao aplicar jogos em salas de aula, com frequência, alguns alunos se comportam

como se este momento não fizesse parte da aula, como se não fosse importante. O professor deve portanto conscientizá-los sobre a sua participação na atividade, a importância do jogo e seus objetivos para a aprendizagem do conteúdo. O jogo deve possuir algumas características para que o aluno não se confunda, ache difícil ou se desinteresse como, por exemplo, ter poucas regras e não deve ser muito demorado.

A Secretaria de Educação do Estado do Ceará promove formações no decorrer do ano para os professores de Matemática das escolas públicas do Estado a fim de se obter uma melhora no aprendizado dos alunos e consequentemente nos resultados. A professora responsável pelas formações nos incentiva a utilizar jogos em sala de aula e a cada encontro leva mais de um jogo para que possamos conhecê-los e utilizá-los em sala de aula.

Um desses jogos é o dominó de frações, em que 28 peças são divididas entre os participantes. Escolhe-se alguém para iniciar colocando uma de suas peças sobre a mesa, em seguida o participante ao lado procura em suas peças alguma que seja equivalente a alguma extremidade da peça na mesa, caso tenha, ele a coloca de modo a ficarem juntas as frações equivalentes, caso não tenha, o jogador ao lado continua. O jogo prossegue até que alguém não tenha mais peças, esse será o vencedor.

Baseado no dominó descrito acima, uma possibilidade para abordagem do Ensino de Aritmética Modular no Ensino Básico é através do uso do jogo de dominó para que o aprendizado ocorra de forma mais lúdica e em grupo. Abaixo apresento doze peças que poderiam ser divididas em grupos com 2, 3 ou 4 alunos.

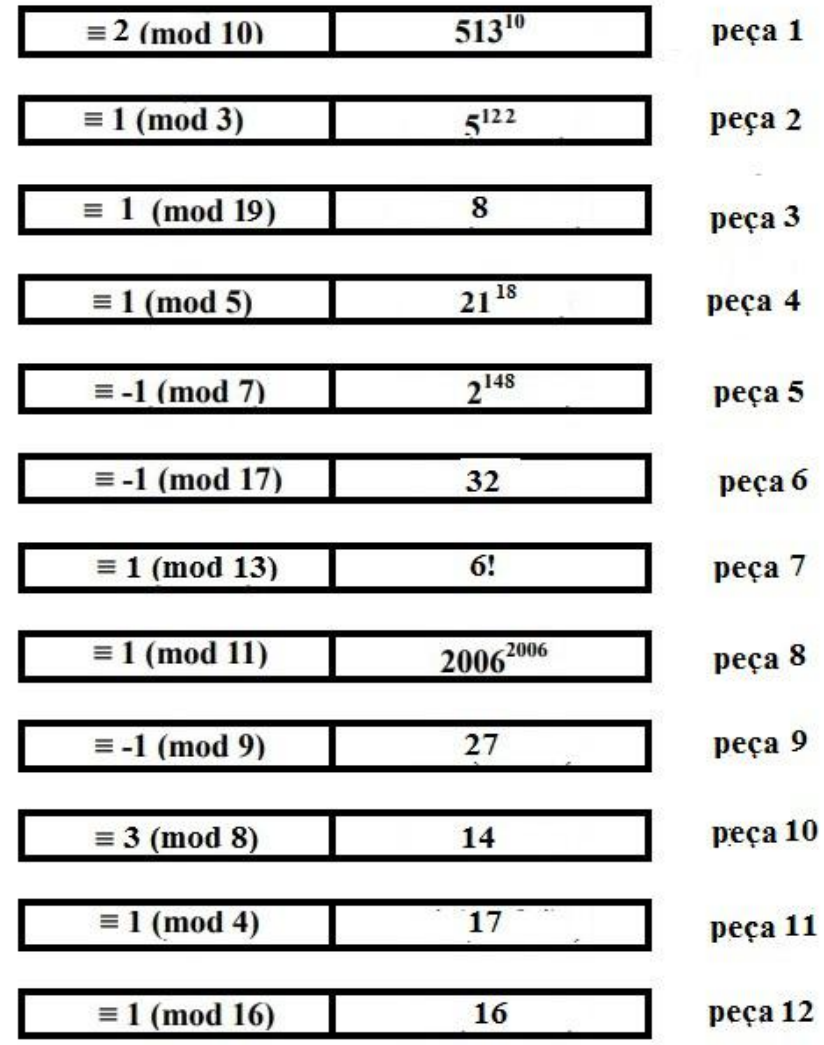
As etapas do jogo são as seguintes:

1. Dividir as peças do jogo igualmente;
2. Escolher um aluno para iniciar o jogo;
3. O aluno escolhido coloca uma de suas peças sobre a mesa;
4. O aluno ao lado (sentido horário) procura em suas peças se possui uma que seja pergunta ou resposta de alguma extremidade da peça na mesa, caso tenha, coloca-a de modo que pergunta e resposta fiquem juntas;
5. Caso o aluno não tenha peça que atenda à etapa anterior, passa a vez para o próximo (sentido horário);
6. O jogo continua até que alguém não tenha mais nenhuma peça, esse será o vencedor.

O objetivo do jogo é perceber se o conteúdo foi realmente aprendido. Serve para verificação de aprendizado dos conteúdos abordados como o Pequeno Teorema de Fermat e o Teorema de Wilson.

Pode acontecer de não haver vencedor se alguém tiver colocado alguma peça de forma errada na mesa ou estiver segurando o jogo, isto é, tenha a peça na mão e não a coloque, isso pode indicar que a pessoa não entendeu determinado resultado indicando a necessidade de uma revisão. Esse jogo deve ser utilizado apenas no final da explicação do conteúdo.

Figura 4: Jogo de dominó para aprendizado de aritmética modular.



Fonte: Autor.

Vejamos as combinações de algumas peças: O lado direito da peça 1 combina com o lado esquerdo da peça 8, ou seja, $513^{10} \equiv 1$ $(mod\ 11)$, pelo Pequeno Teorema de Fermat. O lado direito da peça 7 combina com o lado esquerdo da peça 5, uma vez que $6! \equiv -1$ $(mod\ 7)$, pelo Teorema de Wilson. O lado direito da peça 8 combina o lado esquerdo da peça 4 uma vez que, 2006^{2006} termina em 6, pelo fato de que qualquer potência de um número terminado em 6 também termina em 6, e um número terminado em 6 dividido por 5 sempre deixa resto 1. O lado esquerdo da peça 5 combina com o lado direito da peça 2, pois $2^2 \equiv 1$ $(mod\ 3)$. Utilizando a Proposição 2.4, temos $2^{148} \equiv 1$ $(mod\ 3)$. As outras peças são resolvidas através da definição de congruência ou pelos mesmos motivos anteriores.

Quando utilizo jogos em sala de aula, percebo que o interesse dos alunos é maior, que querem participar e aprender como se joga, há uma boa interação e um bom resultado.

5 CONSIDERAÇÕES FINAIS

Como exposto nesse trabalho, percebemos que Aritmética Modular não é estudada no Ensino Básico embora muitos autores defendam que isso aconteça por trazer benefícios aos estudantes como: melhora no raciocínio lógico, no cálculo mental, e colaboração para o amadurecimento matemático do aluno. Alguns autores defendem o estudo de tal conteúdo no Ensino Fundamental após terem sido estudados números primos, MMC e MDC, que são os pré-requisitos necessários para desenvolver a base da Aritmética Modular. Por exemplo, Ferreira (2018), propõe o ensino de congruências modulares a partir do 6º ano do Ensino Fundamental. Outros autores defendem que ocorra no Ensino Médio.

Acreditamos que seria interessante trabalhar a parte mais básica no Ensino Fundamental como a definição de congruência e suas propriedades operatórias acompanhadas de uma série de exemplos envolvendo números elevados, aparentemente difíceis de resolver, mas que podem ser solucionados com relativa facilidade usando a noção de congruência.

Para o Ensino Médio, sugerimos que sejam abordados os Teoremas de Fermat, de Wilson e de Zeller. Nada impede porém que esses tópicos sejam trabalhados no Ensino Fundamental. O Teorema de Zeller, por exemplo, pode ser ensinado para alunos do Ensino Fundamental e médio, veja Lage (2018).

Em ambos os casos, o jogo de dominó proposto em nosso trabalho pode ser adaptado conforme as características da turma e do assunto estudado.

Pommer (2008) propõe, por exemplo, que o estudo de equações diofantinas lineares ocorra no Ensino Médio o que disponibilizaria aos alunos uma maneira elegante e sistemática de obter soluções inteiras diferentemente das estratégias abordadas em muitos livros que são por meio de tentativa e erro ou da atribuição de valor a uma variável com a determinação do valor correspondente da outra variável. Não é a intenção desmerecer a técnica de tentativa e erro. Pelo contrário, tal método ajuda a desenvolver o raciocínio e a cada tentativa frustrada de resolução, devem ser observadas as falhas para que não sejam cometidas numa próxima tentativa. O objetivo é que além desse método, sejam ensinadas as técnicas de aritmética modular.

Os sites que sugerimos podem servir como auxílio no ensino da disciplina ou na verificação do aprendizado dos alunos. As questões de olimpíadas podem servir como desafio para os alunos. As aulas em vídeo podem auxiliar os alunos no aprendizado tendo a vantagem deles poderem assistir a elas quantas vezes forem necessárias. É fundamental também apresentar aplicações para dar mais sentido aos alunos do motivo de aquilo estar sendo estudado. Os livros didáticos dos alunos podem ser usados para verificar a veracidade do método de determinação do ISBN. Como muitos documentos atuais têm dígitos verificadores, será fácil encontrar outros casos de aplicações de aritmética modular. Entretanto, faz-se necessário explicar aos alunos o método usado para determinar o dígito

verificador da situação em questão.

Esperamos que, ao final da leitura desse trabalho, tenha ficado claro que ideias simples de aritmética modular podem ser ensinadas após assuntos que já são vistos no Ensino Básico. Os esforços adicionais seriam ínfimos e os ganhos compensatórios.

REFERÊNCIAS

[1] Aldeia Numaboa, **Ferramentas matemáticas**. Disponível em: http://www.numaboa.com.br/escolinha/ferramentas-matematicas. Acesso em 23/06/2018.

[2] ALENCAR FILHO, E. **Teoria Elementar dos Números**. São Paulo: Editora Nobel, 1981.

[3] ANDRINI, A.; VASCONCELLOS, M. **Praticando matemática** 6. 3.ed. São Paulo: Editora Brasil, 2015.

[4] BELLO, Moreia Gómez. **La Aritmética Modular y álgunas de sus aplicaciones.** 2011. 113f. Dissertação de Mestrado (Faculdade de Ciências) - Universidade Nacional de Colombia, Bogotá.

[5] BIANCHINI, E. **Matemática**. 8. ed. São Paulo: Editora Moderna, 2015.

[6] BRASIL, **Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais (PCN+).** Ciências da Natureza e Matemática e suas tecnologias. Brasília: MEC, 2006.

[7] BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais:** matemática/Secretaria de Educação Fundamental. Brasília : MEC/SEF, 1997.

[8] EUCLIDES. **Fórum PiR2.** Disponível em: https://pir2.forumeiros.com/t15286-dia-da-semana-como-calcular. Acesso em: 01/07/2018.

[9] FERREIRA, Rosiane Barros.**Congruência Modular no Ensino Básico.** 2018. 49f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Federal do Maranhão, Maranhão.

[10] FERREIRA, Francisco de Assis. **A prova dos noves, divisibilidade e congruência** 2017. 53f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Federal do Cariri, Ceará.

[11] FREITAS, Sávio Gomes. et al. **A prova dos nove: História e aplicabilidade na formação inicial e no comércio.** 2016. Educação Matemática Na Contemporaneidade: desafios e possibilidades, SBEM, XII ENEM.

[12] FREITAS, Ataniel Rogério Gonçalves. **Uma abordagem do ensino de con-**

gruência na educação básica. 2015. 77f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Federal de Sergipe, Sergipe.

[13] HEFEZ, Abramo. **Elementos de Aritmética**, 2^a edição, SBM, 2005.

[14] LAGE, Francisca Daniella Andreu Simões Moraes. **Um estudo de aritmética modular para a educação básica**. 2018. 61 f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Federal de Ouro Preto, Paraná.

[15] MARONESE, Diego Aparecido. **Tópicos de aritmética modular na educação básica:** Uma proposta de atividades. 2016. 66 f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Estadual de Londrina, Paraná.

[16] MATTOS, S. R.; PUGGIAN, C.; LOZANO, A. R. G. **Aritmética modular e suas possibilidades na formação continuada de professores de Matemática.** XIII CIAEM-IACME, Recife 2011.

[17] MOREIRA, Filipe Rodrigues de S. **Congruências Lineares** 2006. 8f.

[18] OLIMPÍADA BRASILEIRA DE MATEMÁTICA. 34^a **Olimpíada Brasileira de Matemática** Disponível em: https:www.obm.org.br/content/uploads/2017/01/eureka38.pdf. Acesso em: 02/09/2018.

[19] OLIMPÍADA CEARENSE DE MATEMÁTICA, **XXXIV Olimpíada Cearense de Matemática**-NÍVEL 3. Disponível em: http:www.mat.ufc.br/ocm/arquivos/Nivel_3_2014.pdf. Acesso em 01/07/2018.

[20] PINHEIRO, Rodolfo Cavalcante. **Aritmética Modular:** uma Aplicação no Ensino Fundamental. 2018. 81f. Dissertação de Mestrado (Programa de Mestrado Profissional em Matemática) - Universidade Federal de Goiás, Goiás.

[21] PINTO, M. A. D.; OLIVEIRA, E. M.; SILVA, M. R. S. P.; Costa, M. **Uma proposta de ensino de aritmética modular para educação básica.** In: VII Congresso Internacional de Ensino da Matemática. 9., 2017. ULBRA, Canoas, RS.

[22] POMMER, Wagner M., **Equações Diofantinas Lineares:** Um Desafio Motivador para Alunos do Ensino Médio. 2008. 153f. Dissertação de Mestrado Acadêmico em Educação Matemática-Pontifícia Universidade Católica de São Paulo, São Paulo.

[23] PORTAL OBMEP DO SABER. **Aritmética dos Restos.** Disponível em: https:portaldosaber.obmep.org.br/index.php/modulo/ver?modulo=63&tipo=4. Acesso em: 01/07/2018.

[24] POTI. **Aritmética Modular.** Disponível em: http://poti.impa.br/index.php/modulo/ver?modulo=4. Acesso em: 01/07/2018.

[25] ROLDÁN, Antonio. **Congruência.** Disponível em: http://hojamat.es/sindecimales/congruencias/inicongruencias.html. Acesso em: 21/09/2018.

[26] SÁ, Ilydio Pereira de. **Aritmética modular e algumas de suas aplicações.** Disponível em: http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf. Acesso em: 01/07/2018.

[27] SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números.** 3. ed. Rio de Janeiro: IMPA, 2006.

[28] SANTOS, Cássio. **Curso de Latex.** Disponível em: https://www.youtube.com/channel/$UCurZp_oi2Bhjb2hdzVhRrWw$. Acesso em 05/06/2018.

[29] SANT'ANNA, I. K. de. **A aritmética modular como ferramenta para as séries finais do ensino fundamental.** Dissertação de mestrado. Disponível em: https://impa.br/wp-content/uploads/2016/12/iury_kersnowsky.pdf. Acesso em: 01/07/2018.

[30] SOUZA, Leticia Vasconcellos de. **Congruência modular nas séries iniciais do ensino fundamental.** Trabalho de conclusão de curso (Dissertação) - Mestrado Profissional em Matemática. Universidade Federal de Juiz de Fora. Juiz de Fora, Minas Gerais. 2015.

[31] VIANA, João José Luiz. **Elementos de Arithmetica.** 11. ed. Rio de Janeiro: Livraria Francisco Alves, 1906.