Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

PROFMAT (Mestrado Profissional em Matemática em Rede Nacional)

Leticia Vasconcellos de Souza

Congruência modular nas séries finais do ensino fundamental

Juiz de Fora

2015

Leticia Vasconcellos de Souza

Congruência modular nas séries finais do ensino fundamental

Dissertação apresentada ao PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) da Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Luiz Fernando de Oliveira Faria

Juiz de Fora

2015

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Souza, Leticia Vasconcellos de.
Congruência modular nas séries finais do ensino fundamental / Leticia Vasconcellos de Souza. – 2015.
39 f. : il.

Orientador: Luiz Fernando de Oliveira Faria
Dissertação (PROFMAT) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. PROFMAT (Mestrado Profissional em Matemática em Rede Nacional), 2015.

1. Congruência Modular. 2. Ensino fundamental. 3. Números primos. 4. Mínimo múltiplo comum (mmc). 5. Máximo divisor comum (mdc). 6. Divisão euclidiana. I. Faria, Luiz Fernando de Oliveira, orient. II. Título.

Leticia Vasconcellos de Souza

Congruência modular nas séries finais do ensino fundamental

Dissertação apresentada ao PROFMAT (Mestrado Profissional em Matemática em Rede Nacional) da Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em: 14 de agosto de 2015.

BANCA EXAMINADORA

Prof. Dr. Luiz Fernando de Oliveira Faria - Orientador
Universidade Federal de Juiz de Fora

Professor Dr. Eduard Toon
Universidade Federal de Juiz de Fora

Professor Dr. Anderson Luis Albuquerque de Araujo
Universidade Federal de Viçosa

Dedico este trabalho aos meus pais, Eliane Ingrede Vasconcellos de Souza e Ventura Alves de Souza Neto, e ao meu esposo Renato de Freitas Generozo.

AGRADECIMENTOS

Agradeço primeiramente a Deus por todas as bênçãos a mim concedidas.

Ao meu esposo, Renato de Freitas Generozo, que a todo momento esteve ao meu lado me apoiando e incentivando a prosseguir.

Aos meus pais, Eliane e Ventura, pelo amor, incentivo e apoio incondicional.

Ao meu orientador, Prof. Dr. Luiz Fernando de Oliveira Faria, pela disponibilidade e apoio.

Aos companheiros de viagem, Renato Cruz e Ricardo Almeida e aos demais colegas de curso, que fazem parte dessa trajetória.

“A Matemática é a rainha das ciências, e a Aritmética é a rainha da Matemática”
Carl Friedrich Gauss

RESUMO

Este trabalho é voltado para professores que atuam nas séries finais do Ensino Fundamental. Tem como objetivo mostrar que é possível introduzir o estudo de Congruência Modular nesse segmento de ensino, buscando facilitar a resolução de diversas situações-problema. A motivação para escolha desse tema é que há a possibilidade de tornar mais simples a resolução de muitos exercícios trabalhados nessa etapa de ensino e que são inclusive cobrados em provas de admissão à escolas militares e em olimpíadas de Matemática para esse nível de escolaridade. Inicialmente é feita uma breve síntese do conjunto dos Números Inteiros, com suas operações básicas, relembrando também o conceito de números primos, onde é apresentado o crivo de Eratóstenes; o *mmc* (mínimo múltiplo comum) e o *mdc* (máximo divisor comum), juntamente com o Algoritmo de Euclides. Apresenta-se alguns exemplos de situações-problema e exercícios resolvidos envolvendo restos deixados por uma divisão para então, em seguida, ser dada a definição de congruência modular. Finalmente, são apresentadas sugestões de exercícios para serem trabalhados em sala de aula, com uma breve resolução.

Palavras-chave: Congruência Modular. Ensino Fundamental. Números primos. Mínimo múltiplo comum (*mmc*). Máximo divisor comum (*mdc*). Divisão euclidiana.

ABSTRACT

The aims of this work is teachers working in the final grades of elementary school. It aspires to show that it is possible to introduce the study of Modular congruence this educational segment, seeking to facilitate the resolution of numerous problem situations. The motivation for choosing this theme is that there is the possibility to make it simpler to solve many problems worked at this stage of education and are even requested for admittance exams to military schools and mathematical Olympiads for that level of education. We begin with a brief summary about integer numbers, their basic operations, also recalling the concept of prime numbers, where the sieve of Eratosthenes is presented; the *lcm* (least common multiple) and the *gcd* (greatest common divisor), along with the Euclidean algorithm. We present some examples of problem situations and solved exercises involving debris left by a division and then, we give the definition of modular congruence . Finally , we present suggestions for exercises to be worked in the classroom, with a short resolution.

Key-words: Modular congruence . Elementary School. Prime numbers. Least Common Multiple (*lcm*). Greatest common divisor (*gcm*). Euclidean division.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Em provas como a Olimpíada Brasileira de Matemática das Escolas públicas, OBMEP, e de admissão à escolas militares, para as séries finais do Ensino Fundamental, cada vez mais é percebido a presença de questões que poderiam ser desenvolvidas utilizando-se o conceito de congruência modular. E, apesar de esse conteúdo ser aplicado a alunos do ensino fundamental através do Programa de Iniciação Científica-jr. da OBMEP, propomos que seja introduzido também na grade curricular de Matemática das séries finais do Ensino Fundamental Regular.

No capítulo denominado O Conjunto dos Números Inteiros, apresentamos um breve resumo dos conteúdos sobre os quais os alunos já devem ter conhecimento para que então seja introduzido o conceito de Congruência Modular. Começamos com as operações básicas de Adição, Subtração, Multiplicação e Divisão, abordando suas principais propriedades, Em seguida exploramos os conceitos de Divisibilidade e Números Primos, utilizando o Crivo de Eratóstenes, através de exemplos, como um método interessante para encontrar números primos relativamente pequenos. Faremos uma breve abordagem do Mínimo Múltiplo Comum (mmc) e do Máximo Divisor comum (mdc) mostrando o cálculo de cada um deles através de exemplos, apresentando o Algoritmo de Euclides para o cálculo do mdc.

Em seguida, no capítulo denominado Congruência Modular, traremos exemplos de questões que podem ser resolvidas aplicando o conceito de congruência modular e, em seguida, apresentaremos sua definição e algumas de suas propriedades, bem como uma pequena lista de exercícios resolvidos. Espera-se com esse trabalho trazer uma nova visão sobre diversas situações, baseados nessa teoria.

2 O CONJUNTO DOS NÚMEROS INTEIROS

O conjunto dos Números Inteiros, $Z = \{..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}$, é ensinado nas séries finais do Ensino Fundamental e é formado pelo conjunto dos Números Naturais, $N = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ...\}$, e seus respectivos opostos ou simétricos (números inteiros negativos correspondentes aos naturais, que quando colocados na reta numérica estão à mesma distância da origem, ou seja, de zero). A letra Z, usada pra representar o conjunto, vem do alemão *Zahlen*, que significa número.

A construção do conjunto dos números naturais baseia-se na ideia do sucessor, que consiste em adicionar 1 unidade a um número para se obter o próximo número da sequência. Já a construção dos inteiros é feita através de uma relação de equivalência no conjunto dos naturais, e pode ser encontrada no livro "A Construção dos Números,"de Jamil Ferreira, para maiores detalhes ver [1].

Exemplo 1

- O sucessor do 0 (zero) é um, pois $0 + 1 = 1$.
- O sucessor do 5 é 6, pois $5 + 1 = 6$.
- O sucessor do -10 é -9 pois $-10 + 1 = -9$.
- O sucessor do 99 é o 100, pois $99 + 1 = 100$.

O conjunto dos números inteiros está munido das seguintes operações: adição $(+)$, subtração $(-)$, multiplicação $(\cdot)$ e divisão $(\div)$.

2.1 ADIÇÃO DE NÚMEROS INTEIROS

É a operação que reúne em um só número as quantidades representadas por dois ou mais números. Seus termos são chamados de parcelas e o resultado de uma adição recebe o nome de soma.

Devemos estar atentos pois na adição de números inteiros, se ambos possuírem o mesmo sinal, somaremos os números e conservaremos o sinal, mas se os números possuírem sinais diferentes (um positivo e outro negativo), o resultado terá o sinal do número que estiver mais distante do zero. Lembrando que quando o sinal de um número não está escrito significa que ele é positivo.

2.1.1 **Propriedades da Adição**

2.1.1.1 *Fechamento*

A soma de números inteiros resulta sempre em um número inteiro.

Exemplo 2

- $5 + 8 = 13$
- $-2 + 3 + 7 = 8$
- $-4 + (-8) = -12$

2.1.1.2 *Elemento Neutro*

Ao somarmos zero a qualquer número inteiro, a soma será o próprio número.

Exemplo 3

- $6 + 0 = 6$
- $-9 + 0 = -9$
- $0 + 50 = 50$

2.1.1.3 *Comutativa*

A ordem das parcelas não altera a soma.

Exemplo 4

- $5 + 8 = 8 + 5 = 13$
- $-4 + (-8) = -8 + (-4) = -12$

2.1.1.4 *Associativa*

A ordem em que somamos as parcelas não alteram o resultado.

Aqui usamos parenteses ( ) para representar quais parcelas estão sendo adicionadas primeiro.

Exemplo 5

- $(4 + 3) + 9 = 4 + (3 + 9) \Rightarrow 7 + 9 = 4 + 12 \Rightarrow 16 = 16$
- $(-5 + 7) + 2 = -5 + (7 + 2) \Rightarrow 2 + 2 = -5 + 9 \Rightarrow 4 = 4$

2.2 SUBTRAÇÃO DE NÚMEROS INTEIROS

A subtração tem por finalidade calcular a diferença entre dois números inteiros, ou seja, quanto um número excede ou quantas unidades é menor que o outro.

Exemplo 6

- $+12 - (+9) = 3$, pois 12 excede 9 em 3 unidades.
- $+23 - (-4) = 27$, pois 23 excede -4 em 27 unidades.
- $-8 - (+3) = -11$, pois -8 é 11 unidades menor que 3.
- $-2 - (-7) = 5$, pois -2 excede -7 em 5 unidades.

Em uma subtração, o primeiro número chama-se minuendo, o segundo número subtraendo e o resultado é chamado de diferença.

Exemplo 7

- $250 - 145 = 105$, onde 250 é o minuendo, 145 é o subtraendo e 105 é a diferença entre 250 e 145.

2.2.1 Propriedades da Subtração

As propriedades do *Fechamento* e *Elemento Neutro* da adição são mantidas na subtração, porém as propriedades *Comutativa* e *Associativa* não serão mantidas. Observe:

2.2.1.1 *Fechamento*

A subtração de dois números inteiros resulta sempre em um número inteiro.

Exemplo 8

- $15 - 8 = 7$
- $21 - (-3) = 24$
- $(-9) - (-2) = -7$

2.2.1.2 *Elemento Neutro*

Ao subtrairmos zero de qualquer número inteiro, a diferença será o próprio número.

Exemplo 9

- $6 - 0 = 6$
- $-9 - 0 = -9$
- $0 - 0 = 0$

2.2.1.3 *Comutativa*

Essa propriedade não é válida para a subtração, pois a ordem dos termos altera a diferença.

Exemplo 10

- $5 - 8 = -3$ e $8 - 5 = 3$
- $4 - (-8) = 12$ e $-8 - 4 = -12$

2.2.1.4 *Associativa*

Essa propriedade não é válida para a subtração, pois a ordem em que subtraímos os termos altera o resultado.

Exemplo 11

- $(4 - 3) - 9 \neq 4 - (3 - 9) \Rightarrow -1 - 9 \neq 4 - (-6) \Rightarrow -10 \neq 10$
- $(-5 - 7) - (-2) \neq -5 - (7 - (-2)) \Rightarrow -12 - (-2) \neq -5 - 9 \Rightarrow -10 \neq -14$

2.3 MULTIPLICAÇÃO DE NÚMEROS INTEIROS

A multiplicação é uma operação binária, ou seja, realizada com dois números de cada vez, e é uma forma simples de se adicionar uma quantidade finita de números inteiros iguais. O resultado de uma multiplicação é chamado produto e seus termos recebem o nome de fatores.

Na multiplicação de números inteiros, se os sinais dos fatores forem iguais (os dois positivos ou os dois negativos), o produto será positivo, mas se os sinais forem diferentes (um positivo e outro negativo) o produto será negativo.

Exemplo 12

- $7 \cdot 5 = 35$
- $-3 \cdot (-8) = 24$
- $6 \cdot (-2) = -12$
- $-9 \cdot 4 = -36$

2.3.1 Propriedades da Multiplicação

2.3.1.1 *Fechamento*

O produto entre dois números inteiros será sempre um número inteiro.

Exemplo 13

- $4 \cdot 5 = 20$
- $-2 \cdot 7 = -14$
- $-6 \cdot (-8) = 48$

2.3.1.2 *Elemento Neutro*

Ao multiplicarmos qualquer número inteiro por 1, o produto será o próprio número.

Exemplo 14

- $6 \cdot 1 = 6$
- $-9 \cdot 1 = -9$
- $1 \cdot 50 = 50$

2.3.1.3 *Comutativa*

A ordem dos fatores não altera o produto.

Exemplo 15

- $5 \cdot 8 = 8 \cdot 5 = 40$
- $-4 \cdot (-8) = -8 \cdot (-4) = 32$
- $7 \cdot (-2) = -2 \cdot 7 = -14$

2.3.1.4 *Associativa*

A ordem em que multiplicamos os fatores não alteram o produto.

Exemplo 16

- $(4 \cdot 3) \cdot 5 = 4 \cdot (3 \cdot 5) \Rightarrow 12 \cdot 5 = 4 \cdot 15 \Rightarrow 60 = 60$
- $(-5 \cdot 7) \cdot 2 = -5 \cdot (7 \cdot 2) \Rightarrow -35 \cdot 2 = -5 \cdot 14 \Rightarrow -70 = -70$

2.3.1.5 *Distributiva*

A multiplicação de um número inteiro por uma adição (ou subtração) apresenta o mesmo resultado que soma (ou diferença) da multiplicação desse número inteiro por cada fator da adição (ou subtração).

Exemplo 17

- $3 \cdot (4 + 9) = 3 \cdot 4 + 3 \cdot 9 \Rightarrow 3 \cdot 13 = 12 + 27 \Rightarrow 39 = 39$
- $-2 \cdot (7 - 12) = -2 \cdot 7 - (-2) \cdot 12 \Rightarrow -2 \cdot (-5) = -14 - (-24) \Rightarrow 10 = 10$

2.3.1.6 *Cancelamento*

A multiplicação de qualquer número inteiro por zero terá produto igual a zero.

Exemplo 18

- $9 \cdot 0 = 0$
- $(-4) \cdot 0 = 0$
- $0 \cdot 325 = 0$

2.4 DIVISÃO DE NÚMEROS INTEIROS

Sua finalidade é repartir um número inteiro em partes iguais. O número a ser dividido recebe o nome de dividendo, o número que representa em quantas partes iguais vamos dividir é chamado de divisor (e deve ser diferente de zero) e o resultado da divisão é chamado de quociente. Mas nem sempre é possível realizar a divisão de um inteiro por outro, por isso o matemático Euclides, conhecido como pai da geometria, nascido na Síria em aproximadamente 330 a.C., em sua obra "Elementos", representou esse tipo de divisão, que é conhecida como "divisão euclidiana", da seguinte forma:

Proposição 1 *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos inteiros q e r tais que $b = a \cdot q + r$, com $0 \leq r <\mid a \mid$.*

Onde b é o dividendo, a é o divisor, q é o quociente e r é chamado de resto da divisão. $\mid a \mid$ representa a distância de a até a origem (zero).

Exemplo 19

- $50 \div 8 \Rightarrow 50 = 8 \cdot 6 + 2$
- $-120 \div 12 \Rightarrow 12 \cdot (-10) + 0$

Quando $r = 0$, dizemos que a divisão de inteiros é exata e representa um número inteiro. Quando $r \neq 0$, dizemos que a divisão é não exata, portanto não representa um número inteiro. Nos exemplos acima temos que $-120 \div 12$ representa um número inteiro ($r = 0$), enquanto $50 \div 8$ não representa um número inteiro ($r = 2$).

Na divisão de números inteiros, se os sinais do divisor e do dividendo forem iguais, o quociente será positivo, se os sinais do divisor e do dividendo forem diferentes (um positivo e outro negativo) o quociente será negativo.

As únicas propriedades da multiplicação válidas também para a divisão de números inteiros são *Elemento Neutro* e *Distributiva*, veja:

2.4.1 Propriedades da Divisão

2.4.1.1 *Fechamento*

Não é válida pois a divisão entre dois números inteiros nem sempre resulta em um número inteiro, ou seja, nem sempre o resto é zero.

Exemplo 20

- $10 \div 3$ não é inteiro, pois $10 = 3 \cdot 3 + 1$ com $r = 1$.
- $-25 \div 7$ não é inteiro, pois $-25 = 7 \cdot (-4) + 3$ com $r = 3$.

2.4.1.2 *Elemento Neutro*

Ao dividirmos qualquer número inteiro por 1, o quociente será o próprio número e o resto será igual a zero.

Exemplo 21

- $6 \div 1 = 6$, pois $6 = 1 \cdot 6 + 0$
- $-9 \div 1 = -9$, pois $-9 = 1 \cdot (-9) + 0$

2.4.1.3 *Comutativa*

Não é válida pois a ordem dos termos altera o resultado da divisão.

Exemplo 22

- $50 \div 5 \neq 5 \div 50$

2.4.1.4 *Associativa*

Não é válida, pois a ordem em que dividimos os termos altera o resultado.

Exemplo 23

- $(40 \div 4) \div 2 \neq 40 \div (4 \div 2) \Rightarrow 10 \div 2 \neq 40 \div 2 \Rightarrow 5 \neq 20$

2.4.1.5 *Distributiva*

É válida para as divisões exatas, ou seja, com resto zero, onde a divisão de uma adição (ou subtração) por um número inteiro apresenta o mesmo resultado que a soma (ou diferença) da divisão de cada fator da adição (ou subtração) por esse número inteiro.

Exemplo 24

- $(45 + 36) \div 9 = 45 \div 9 + 36 \div 9 \Rightarrow 81 \div 9 = 5 + 4 \Rightarrow 9 = 9$
- $(-54 - 33) \div 3 = -54 \div 3 - 33 \div 3 \Rightarrow -87 \div 3 = -18 - 11 \Rightarrow -29 = -29$

2.4.1.6 *Cancelamento*

Não é válida pois não existe divisão por zero.

O estudo dos restos deixados pela divisão de inteiros fornece importantes resultados e facilita a resolução de diversos problemas, como veremos mais adiante. Podemos também estabelecer uma relação de divisibilidade entre números inteiros.

2.5 DIVISIBILIDADE EM Z

Como a divisão de um número inteiro por outro com resto zero nem sempre é possível, esta possibilidade é expressa através da relação de *divisibilidade*.

Dados dois números inteiros a e b, diremos que $a \mid b$ (a divide b), se houver algum número inteiro q, onde $b = q \cdot a$. Neste caso, diremos também que a é um *divisor* ou um *fator* de b, ou ainda, que b é um *múltiplo* de a.

É preciso observar que $a \mid b$ não representa uma operação em Z, nem uma fração. Trata-se de uma sentença que diz ser verdade que a divide b (ou b é divisível por a).

Exemplo 25

- $3 \mid 21$, pois $21 = 7 \cdot 3$. Dizemos que 21 é divisível por 3.
- $-5 \mid 60$, pois $60 = 12 \cdot (-5)$. Dizemos então que 60 é divisível por -5.
- $8 \mid -96$, pois $-96 = -12 \cdot 8$. Dizemos então que -96 é divisível por 8.
- $2 \mid 0$, pois $0 = 0 \cdot 2$. Dizemos então que 0 é divisível por 2.

Observação 1 *Como qualquer número quando multiplicado por zero resulta em zero, dizemos que zero é divisível por todos os números inteiros.*

Alguns números inteiros positivos só são divisíveis por eles mesmos e por 1. Estes são chamados Números Primos.

2.6 NÚMEROS PRIMOS

Definição 1 *Um número inteiro, $p \neq 1$ é chamado número primo se os seus únicos divisores naturais são 1 e p.*

Ou seja, denominaremos números primos os naturais não nulos, diferentes de 1, que possuem apenas dois divisores naturais, o 1 e ele mesmo; sendo os demais naturais denominados *números compostos*.

Os números primos são muito importantes pois, dentre outros motivos, seus produtos representam todos os números naturais, diferentes de 1 e zero; ou seja, todos os números naturais, diferentes de 1 e zero, podem ser escritos de forma única como um produto de fatores primos.

Os números 2, 3, 5 e 7 são exemplos de números primos. Mas como encontrar números primos?

2.6.1 Crivo de Eratóstenes

Existem muitos métodos para encontrar números primos. Um método bastante antigo, e simples (quando consideramos números relativamente pequenos) para se obter números primos de modo sistemático é o chamado *Crivo de Eratóstenes*, devido ao matemático grego Eratóstenes.

Eratóstenes nasceu em Cirene, cidade grega ao norte da África, atual Líbia, em 276 a.C. e morreu na cidade de Alexandria, Egito, em 194 a.C.. Além de matemático, foi um importante geógrafo, astrônomo e filósofo, sendo seu feito científico mais importante a determinação do perímetro da Terra.

A palavra crivo significa peneira, e o método consiste em peneirar os números naturais, jogando fora os números que não são primos. Eratóstenes baseou-se na seguinte proposição, devida a ele próprio, para construir o crivo:

Proposição 2 *Se um número natural $n > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leq n$. Equivalentemente, é primo todo número n que não é múltiplo de nenhum primo p tal que $p^2 \leq n$.*

Ou seja, para determinar se n é primo, vamos calcular a raiz quadrada de n, e se n não for divisível por nenhum número primo menor ou igual à $\sqrt{n}$, então n é primo.

Exemplo 26

- Para $n = 30$, temos $\sqrt{30} \simeq 5,5$. Tomando os primos 2, 3 e 5, menores que $\sqrt{30}$, temos que 30 é múltiplo de todos eles, pois $2 \mid 30$, $3 \mid 30$ e $5 \mid 30$. Ou seja, 30 é composto.
- Para $n = 79$, temos $\sqrt{79} \simeq 8,9$. Tomando os primos 2, 3, 5 e 7, menores que $\sqrt{79}$, temos que 79 não é múltiplo de nenhum deles. Ou seja, 79 é primo.
- Para $n = 50$, temos $\sqrt{50} \simeq 7$. Tomando os primos 2, 3, 5 e 7, menores ou iguais a $\sqrt{50}$, temos que 50 é múltiplo de 2 e de 5, pois $2 \mid 50$ e $5 \mid 50$. Ou seja, 50 é composto.

Então, para obtermos os números primos até n, no crivo de Eratóstenes, devemos escrever os números de 2 até n em uma tabela e retirar os múltiplos dos números primos já conhecidos até obtermos o primeiro número primo cujo quadrado ultrapasse n.

Observe o exemplo para $n = 100$:

Primeiro escrevemos os números de 2 até 100 em uma tabela.

Figura 1 – Crivo de Eratóstenes

	02	03	04	05	06	07	08	09	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	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

O primeiro número a ser escrito é o 2, que é primo, pois não é múltiplo de nenhum número anterior. Riscaremos todos os demais múltiplos de 2 na tabela, pois não são primos.

Figura 2 – Crivo de Eratóstenes

	02	03	~~04~~	05	~~06~~	07	~~08~~	09	~~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~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

O próximo número não riscado na tabela é o 3 que é primo, pois não é múltiplo de nenhum número anterior na tabela. Riscaremos todos os demais múltiplos de 3 ainda não riscados na tabela, pois não são números primos.

Figura 3 – Crivo de Eratóstenes

	02	**03**	~~04~~	05	~~06~~	07	~~08~~	~~09~~	~~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~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

O primeiro número maior que 3 não riscado na tabela é o 5 que é primo. Riscaremos todos os demais múltiplos de 5 na tabela, que ainda não foram riscados, pois não são primos.

Figura 4 – Crivo de Eratóstenes

	02	**03**	~~04~~	**05**	~~06~~	07	~~08~~	~~09~~	~~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~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

O primeiro número maior que 5 não riscado na tabela é o 7 que é primo. Riscaremos todos os demais múltiplos de 7 na tabela, que ainda não foram riscados.

Figura 5 – Crivo de Eratóstenes

	02	**03**	~~04~~	**05**	~~06~~	**07**	~~08~~	~~09~~	~~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~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

O primeiro número maior que 7 não riscado na tabela é o 11, que é primo.

Observe que o procedimento terminou, pois atingimos o número 11, e como $11^2 > 100$, pela *Proposição 1*, já teriam sido riscados todos os números compostos menores ou iguais a 100.

Ao término desse procedimento, os números não riscados são todos os primos menores que 100.

Desta forma, os números destacados em negrito são todos primos.

Figura 6 – Crivo de Eratóstenes

	02	**03**	~~04~~	**05**	~~06~~	**07**	~~08~~	~~09~~	~~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~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~	~~70~~
71	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~

Dois conceitos importantes da Aritmética estudados no Ensino Fundamental são o *mmc* (mínimo múltiplo comum) e o *mdc* (máximo divisor comum), como veremos a seguir:

2.7 MÍNIMO MÚLTIPLO COMUM (*mmc*)

Como visto na Seção 2.5, um número inteiro é múltiplo de outro quando é divisível por esse outro número inteiro. O conjunto dos múltiplos de um inteiro qualquer é obtido multiplicando-se esse número por todos os elementos do conjunto dos números inteiros.

Exemplo 27

- $M(2) = \{..., -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, ...\}$
- $M(5) = \{..., -30, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, 30\}$
- $M(-5) = \{..., -30, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, 30\}$
- $M(8) = \{..., -48, -40, -32, -24, -16, -8, 0, 8, 16, 24, 32, 40, 48, ...\}$

Observação 2 *Podemos verificar que o elemento 0 (zero) é múltiplo de todo número inteiro, já que é divisível por todos eles.*

Observação 3 *Números opostos, como* 5 *e* -5*, possuem os mesmos múltiplos.*

Sejam a e b dois números inteiros. Chama-se mínimo múltiplo comum de a e b, representado por $mmc(a,b)$, o menor número natural, diferente de zero, que é múltiplo comum de a e b.

Exemplo 28

- Tomando $M(2) = \{..., -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, ...\}$ e $M(-5) = \{..., -30, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, 30\}$, então teremos o $mmc(2, -5) = 10$.
- Tomando $M(3) = \{..., -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, ...\}$ e $M(6) = \{..., -30, -24, -18, -12, -6, 0, 6, 12, 18, 24, 30, ...\}$, temos que $mmc(3, 6) = 6$.

Na educação básica, os alunos aprendem a cacular o *mmc* entre números naturais através da fatoração simultânea, processo em que decompõem-se simultaneamente os dois ou mais números em fatores primos, e depois multiplica-se esses fatores, obtendo o mínimo múltiplo comum entre eles, o que torna bem mais simples o processo.

Exemplo 29

- Calcule o $mmc(12, 30)$:

12 , 30	2
6 , 15	2
3 , 15	3
1 , 5	5
1 , 1	2 x 2 x 3 x 5 = 60

Figura 7 – $mmc(12, 30)$

Logo, o $mmc(12, 30) = 60$.

- Calcule o $mmc(15, 25, 40)$:

15 , 25 , 40	2
15 , 25 , 20	2
15 , 25 , 10	2
15 , 25 , 5	3
5 , 25 , 5	5
1 , 5 , 1	5
1 , 1 , 1	2 x 2 x 2 x 3 x 5 x 5 = 600

Figura 8 – $mmc(15, 25, 40)$

Logo, o $mmc(15, 25, 40) = 600$.

2.8 MÁXIMO DIVISOR COMUM (mdc)

Como visto na Seção 2.5, os divisores de um número a são os números inteiros que dividem a, ou seja, pelos quais a é divisível. Portanto, considerando o número natural a, indicaremos por *D(a)* o conjunto dos divisores de a. Por exemplo, $D(6) = \{-1, 1, -2, 2, -3, 3, -6, 6\}$. Para qualquer natural, tem-se que *D(a)* é finito.

Um divisor comum de a e b é o número que é ao mesmo tempo divisor de a e de b. Sendo a e b inteiros, chama-se *máximo divisor comum* de a e b, indicado por $mdc(a, b)$, o maior número natural que é divisor comum de a e de b. Então, para calcular o mdc entre números inteiros basta escrevermos seus divisores positivos.

Exemplo 30

- Tomando $D(12) = \{1, 2, 3, 4, 6, 12\}$ e $D(15) = \{1, 3, 5, 15\}$, temos $mdc(12, 15) = 3$.
- Tomando $D(8) = \{1, 2, 4, 8\}$ e $D(15) = \{1, 3, 5, 15\}$, temos $mdc(8, 15) = 1$.
- Tomando $D(-12) = \{1, 2, 3, 4, 6, 12\}$ e $D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$, temos $mdc(-12, 24) = 12$.

Observação 4 *Percebemos que o único divisor comum entre os números* 8 *e* 15 *é o* "1", *ou seja,* $mdc(8, 15) = 1$. *Sejam* a, $b \in N$. *Se* $mdc(a, b) = 1$, *diremos que* a *e* b *são primos entre si.*

Observação 5 *Os números* -12 *e* 24 *são tais que* 24 *é um múltiplo de* -12, *e que o* $mdc(-12, 24) = 12 = |-12|$. *De modo geral, sendo* a *e* b *dois números inteiros tais que* b *é um múltiplo de* a, *então o* $mdc(a, b) = |a|$.

Observação 6 *A multiplicação do mdc pelo mmc entre dois números* a *e* b *é igual à multiplicação de* a *por* b, *ou seja,* $mdc(a, b) \cdot mmc(a, b) = a \cdot b$.

Um método bastante simples para calcular o mdc entre dois números naturais é o Algoritmo de Euclides, como veremos a seguir.

2.8.1 Algoritmo de Euclides

O Algoritmo de Euclides é um método bastante eficiente para encontrar o mdc entre dois naturais, pois para obter o mdc entre números muito grandes torna-se complicado escrever o conjunto de todos os divisores dos números em questão.

Proposição 3 *Se a e b são números naturais e $b = a \cdot q + r$, onde q e r são naturais, $mdc(a, b) = mdc(a, r)$.*

Ou seja, o *mdc* entre dois números naturais é igual ao *mdc* entre o resto da divisão do maior pelo menor número e o menor dos números.

Exemplo 31

- $mdc(10, 15)$

  Como $15 = \mathbf{10} \cdot 1 + \mathbf{5}$, $mdc(10, 15) = mdc(10, 5) = 5$.

- $mdc(12, 32)$

  Como $32 = \mathbf{12} \cdot 2 + \mathbf{8}$, $mdc(12, 32) = mdc(12, 8)$, aplicando novamente o algoritmo de Euclides, temos que:

  Como $12 = \mathbf{8} \cdot 1 + \mathbf{4}$, $mdc(12, 32) = mdc(12, 8) = mdc(8, 4) = 4$.

- $mdc(2125, 350)$

  Como $2125 = \mathbf{350} \cdot 6 + \mathbf{25}$, $mdc(2125, 350) = mdc(350, 25) = 25$.

Podemos usar um dispositivo prático para realizar as sucessivas divisões no algoritmo de Euclides, onde os números são colocados como mostra o exemplo a seguir.

Exemplo 32 *Veja como calcular o $mdc(12, 32)$ utilizando o dispositivo prático:*

- 1º Escrevemos os números 32 e 12 no dispositivo, primeiro o maior e depois o menor;

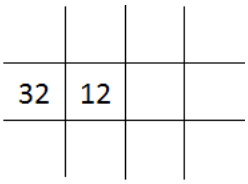

Figura 9 – $mdc(12, 32)$

- 2º Realizamos a divisão colocando o quociente sobre o menor número e o resto abaixo do maior, como $32 = \mathbf{12} \cdot 2 + \mathbf{8}$, temos:

	2		
32	12		
8			

Figura 10 – $mdc(12, 32)$

- 3º Para prosseguir com o algoritmo, escrevemos o resto na linha do meio, à frente do menor número;

	2		
32	12	8	
8			

Figura 11 – $mdc(12, 32)$

- 4º Realizando novamente a divisão, $12 = \mathbf{8} \cdot 1 + \mathbf{4}$, e escrevendo o quociente e o resto nos locais indicados, temos:

	2	1	
32	12	8	
8	4		

Figura 12 – $mdc(12, 32)$

- 5º Repetimos o processo até encontrar resto zero, que indica um número múltiplo do outro, e pela *Observação 2* obtemos o *mdc* procurado. Como $8 = \mathbf{4} \cdot 2 + \mathbf{0}$, chegamos ao fim do algoritmo:

	2	1	2
32	12	8	④
8	4	0	

Figura 13 – $mdc(12, 32)$

O número que estiver escrito na linha do meio quando chegarmos ao resto zero é o *mdc* que procuramos. De fato, pelo algoritmo de Euclides, temos $mdc(12, 32) =$

$mdc(12, 8) = mdc(8, 4) = 4$. Ou seja, $mdc(12, 32) = 4$.

Exemplo 33 *Utilizando o dispositivo prático, calcule:*

- $mdc(150, 60)$

	2	2	
150	60	30	
30	0		

Figura 14 – $mdc(150, 60)$

- $mdc(35, 63)$

	1	1	4
63	35	28	7
28	7	0	

Figura 15 – $mdc(35, 63)$

Quando chegam às séries finais do Ensino Fundamental, os alunos já tem conhecimento sobre os assuntos acima relacionados (exceto algumas vezes o algoritmo de Euclides), estando ainda os mesmos conceitos presentes no currículo escolar de Matemática para estas séries, tornando possível inserir um importante conceito sobre os restos deixados por uma divisão de números inteiros, que não é explorado no ensino básico, mas que torna simples a resolução de diversos problemas aritméticos, muitas vezes presentes no dia a dia dos alunos: a Congruência Modular.

3 CONGRUÊNCIA MODULAR

Diversas situações-problema presentes no dia a dia dos alunos do Ensino Fundamental podem ser resolvidos usando o conceito de congruência modular, que nada mais é do que trabalhar com os restos obtidos através da divisão de números inteiros.

Nesta abordagem, trabalharemos exemplos envolvendo apenas números naturais. Vejamos alguns:

Exemplo 34

1. (Questão retirada do concurso de admissão ao 6º ano do Ensino Fundamental 2012/2013 Colégio Militar do Rio de Janeiro, [2])
Estamos no mês de novembro de 2012. Daqui a 363 meses, estaremos no mês de
A) janeiro
B) fevereiro
C) março
D) abril
E) maio

Como o ano possui 12 meses, e iniciamos no mês de novembro, após decorridos 12 meses (1 ano) estaremos novamente no mês de novembro, e assim sucessivamente. Portanto, para resolver essa questão podemos descobrir quantos anos completos se passaram e contar os meses restantes a partir de novembro. Faremos isso dividindo 363 por 12 e observando o resto dessa divisão. Se o resto for zero estaremos em novembro, se o resto for 1 estaremos em dezembro (1 mes após novembro), se o resto for 2 estaremos em janeiro (2 meses após novembro), e assim sucessivamente, como mostra a tabela abaixo:

Mês	**Jan**	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**	**Jul**	**Ago**	**Set**	**Out**	**Nov**	**Dez**
Resto	2	3	4	5	6	7	8	9	10	11	0	1

Como $363 = 12 \cdot 30 + 3$, ou seja, $363 \div 12 = 30$, com resto 3, observando a tabela vemos que estaremos no mês de Fevereiro.
O que fizemos nessa questão foi analisar o resto da divisão de 363 meses por 12 (nº de meses em um ano).

2. (Questão retirada do banco de questões da OBMEP, [3])
A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua

teia, conforme mostra a figura 10. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

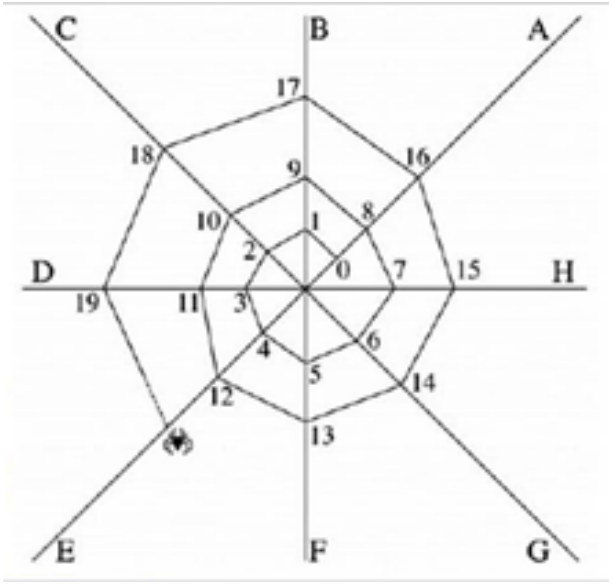

Figura 16 – OBMEP

Nessa questão, temos 8 fios de apoio para a aranha. Como ela inicia sua teia no fio A, ela voltará a esse mesmo fio após ter realizado 8 movimentos, novamente após 16 movimentos, ou seja, a cada 8 movimentos que ela realizar estará novamente no fio A. Isso significa que os movimentos múltiplos de 8 (aqueles que deixam resto zero quando divididos por 8) levarão a aranha novamente ao fio A. Ao dividirmos 118 por 8, temos $118 = 8 \cdot 14 + 6$, ou seja, $118 \div 8 = 14$, com resto 6. Isso significa que a aranha passou 14 vezes pelo fio A e, em seguida, realizou mais 6 movimentos, parando sobre o fio G. Logo, o número 118 estará apoiado sobre o fio G. Note que, neste exemplo, ao realizarmos a divisão de 118 por 8 e analisarmos o resto deixado por esta divisão, pudemos rapidamente chegar ao resultado.

Vamos a outro exemplo.

3. Sabendo que o dia 1º de janeiro de 2015 caiu numa quinta-feira, descubra em qual dia da semana cairá o feriado de 7 de setembro desse mesmo ano.

Nessa questão, primeiro vamos descobrir quantos dias há entre 1º de janeiro e 7 de setembro de 2015. Como não é um ano bissexto, temos:

Janeiro = 30 dias

Fevereiro = 28 dias

Março = 31 dias

Abril = 30 dias

Maio = 31 dias

Junho = 30 dias

Julho = 31 dias

Agosto = 31 dias

Setembro = 7 dias

Somando tudo, temos um total de $30 + 28 + 31 + 30 + 31 + 30 + 31 + 31 + 7 = 249$ dias.

Agora, como cada semana tem 7 dias, devemos dividir 249 por 7. O resultado dessa divisão mostrará quantas semanas tivemos no decorrer desses 249 dias, o número de vezes que voltamos a uma quinta-feira, e o resto dessa divisão, o que mais nos interessa, dirá quantos dias após uma quinta-feira 7 de setembro de 2015 se encontra.

Se o resto da divisão for zero, significa que paramos novamente em uma quinta-feira, se o resto for 1, significa que paramos 1 dia depois de quinta, ou seja, sexta, e assim por diante, como mostra a tabela.

Dia da semana	**Quinta**	**Sexta**	**Sábado**	**Domingo**	**Segunda**	**Terça**	**Quarta**
Resto	0	1	2	3	4	5	6

Como $249 = 7 \cdot 35 + 4$, ou seja, $249 \div 7 = 35$ com resto 4, o feriado de 7 de setembro, no ano de 2015, cairá em uma segunda-feira.

O que fizemos nessa questão foi analisar o resto da divisão de 249 dias por 7 (nº de dias em uma semana).

Ao trabalharmos com o resto de uma divisão estamos usando uma importante ferramenta da teoria dos números, a Aritmética Modular, que nos permite resolver problemas de forma simples, apenas analisando os restos de uma divisão.

Definição 2 *Quando dois números inteiros a e c, ao serem divididos pelo número natural b, deixam mesmo resto, dizemos que eles são congruentes módulo b, e escrevemos* $a \equiv c \mod b$ *(lê-se: a é congruente a c módulo b). Em outras palavras, dois números inteiros a e c são congruentes módulo b se a diferença* $(a - c)$ *é divisível por b, ou seja,* $b \mid (a - c)$.

No primeiro exemplo, podemos escrever $363 \equiv 3 \mod 12$, pois $12 \mid (363 - 3)$; no segundo exemplo, $118 \equiv 6 \mod 8$, pois $8 \mid (118 - 6)$. Já no terceiro exemplo, podemos escrever $249 \equiv 4 \mod 7$, pois $7 \mid (249 - 4)$.

A congruência modular é uma relação de equivalência, pois ela é *Reflexiva*, *Simétrica* e *Transitiva*. De fato, sendo a, b, c e $n \in Z$:

- *Reflexiva*: $a \equiv a \bmod n$, de fato, $n \mid (a - a) = 0$.

  Exemplo 35

  $2 \equiv 2 \bmod 3$
  $5 \equiv 5 \bmod 7$
  $0 \equiv 0 \bmod 4$

- *Simétrica*: $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$, de fato, se $n \mid (a - b)$, então $n \mid (b - a)$, pois $\mid a - b \mid = \mid b - a \mid$.

  Exemplo 36

  Como $5 \mid (12 - 2) = 10$, temos $12 \equiv 2 \bmod 5 \Rightarrow 2 \equiv 12 \bmod 5$, de fato, $5 \mid (2 - 12) = -10$.

- *Transitiva*: $a \equiv b \bmod n$ e $b \equiv c \bmod n \Rightarrow a \equiv$ c $\bmod n$, de fato se $n \mid (a - b)$ e $n \mid (b - c)$ então $n \mid [(a - b) + (b - c)] \Rightarrow n \mid [a - b + b - c] \Rightarrow n \mid (a - c)$.

  Exemplo 37

  Como $5 \mid (12 - 7) = 5$, e $5 \mid (7 - 2) = 5$, temos $12 \equiv 7 \bmod 5$ e $7 \equiv 2 \bmod 5 \Rightarrow 12 \equiv 2 \bmod 5$, de fato, $5 \mid (12 - 2) = 10$.

Propriedades:

1. Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a + c) \equiv (b + d) \bmod n$.
Exemplo: $10 \equiv 3 \bmod 7$ e $8 \equiv 1 \bmod 7$, então $(10 + 8) \equiv (3 + 1) \bmod 7 \Rightarrow 18 \equiv 4 \bmod 7$, de fato, $7 \mid (18 - 4) = 14$.

2. Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a - c) \equiv (b - d) \bmod n$.
Exemplo: $10 \equiv 3 \bmod 7$ e $8 \equiv 1 \bmod 7$, então $(10 - 8) \equiv (3 - 1) \bmod 7 \Rightarrow 2 \equiv 2 \bmod 7$, de fato, $7 \mid (2 - 2) = 0$.

3. Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a \cdot c) \equiv (b \cdot d) \bmod n$.
Exemplo: $10 \equiv 3 \bmod 7$ e $8 \equiv 1 \bmod 7$, então $(10 \cdot 8) \equiv (3 \cdot 1) \bmod 7 \Rightarrow 80 \equiv 3 \bmod 7$, de fato, $7 \mid (80 - 3) = 77$.

4. Sejam a, b, c e n números inteiros tais que $ac \equiv bc \bmod n$ e $mdc(c, n) = 1$. Então $a \equiv b \bmod n$.
Exemplo: $3 \mid (50 - 20) = 30$, logo $50 \equiv 20 \bmod 3 \Rightarrow 10 \cdot 5 \equiv 4 \cdot 5$ e $mdc(5, 3) = 1$, então $10 \equiv 4 \bmod 3$, de fato, $3 \mid (10 - 4) = 6$.

Uma demonstração das propriedades acima será feita no Apêndice A e pode ser também encontrada outra demonstração no livro "Elementos de Aritmética"de Abramo Hefez, [4].

3.1 EXERCÍCIOS RESOLVIDOS

1) Determine os restos (r) das divisões:

a) $54 \div 7$

Solução: Como, pela divisão euclidiana, $54 = 7 \cdot 7 + 5$, temos $r = 5$.

b) $123 \div 3$

Solução: Como, pela divisão euclidiana, $123 = 3 \cdot 41 + 0$, temos $r = 0$.

c) $67 \div 5$

Solução: Como, pela divisão euclidiana, $67 = 5 \cdot 13 + 2$, temos $r = 2$.

d) $256 \div 12$

Solução: Como, pela divisão euclidiana, $256 = 12 \cdot 21 + 4$, temos $r = 4$.

2) Verifique quais dos pares de números abaixo são congruentes módulo 6, ou seja, quais deixam o mesmo resto quando divididos por 6:

a) 35 e 53

Solução: Temos $35 = 6 \cdot 5 + 5$, com $r = 5$ e $53 = 6 \cdot 8 + 5$, com $r = 5$.
Como os restos são iguais esses números são congruentes módulo 6, $35 \equiv 53 \bmod 6$.

b) 49 e 82

Solução: Temos $49 = 6 \cdot 8 + 1$, com $r = 1$ e $82 = 6 \cdot 13 + 4$, com $r = 4$.
Como os restos são diferentes, $49 \not\equiv 82 \bmod 6$.

c) 96 e 124

Solução: Temos $96 = 6 \cdot 16 + 0$, com $r = 0$ e $124 = 6 \cdot 20 + 4$, com $r = 4$.
Como os restos são diferentes $96 \not\equiv 124 \bmod 6$.

d) 9 e 75

Solução: Temos $9 = 6 \cdot 1 + 3$, com $r = 3$ e $75 = 6 \cdot 12 + 3$, com r = 3.
Como os restos são iguais esses números são congruentes módulo 6, $9 \equiv 75 \bmod 6$.

3) Escreva as congruências abaixo, usando os restos das divisões:

a) 25 é congruente a quanto módulo 2?

Solução: Como $25 = 2 \cdot 12 + 1$, com $r = 1$, temos $25 \equiv 1 \bmod 2$.

b) 30 é congruente a quanto módulo 4?

Solução: Como $30 = 4 \cdot 7 + 2$, com $r = 2$, temos $30 \equiv 2 \bmod 4$.

c) 45 é congruente a quanto módulo 9?

Solução: Como $45 = 9 \cdot 5 + 0$, com $r = 0$, temos $45 \equiv 0 \bmod 9$.

d) 238 é congruente a quanto módulo 10?

Solução: Como $238 = 10 \cdot 23 + 8$, com $r = 8$, temos $238 \equiv 8 \bmod 10$.

4) Se hoje é uma sexta-feira, daqui a 100 dias vai ser que dia da semana?

Solução: Como a semana tem 7 dias, vamos dividir 100 por 7.

$100 = 7 \cdot 14 + 2$, com $r = 2$.

Como o resto da divisão é 2, $100 \equiv 2 \bmod 7$, será 14 semanas completas e dois dias após sexta-feira, ou seja, será um domingo.

5) Se estamos no mês de agosto e faltam 30 prestações para dona Maria quitar uma dívida, em que mês ela quitará sua dívida?

Solução: Como o ano tem 12 meses, vamos dividir 30 por 12.

$30 = 12 \cdot 2 + 6$, com $r = 6$.

Como o resto da divisão é 6, $30 \equiv 6 \bmod 12$, dona Maria quitará sua dívida dois anos completos e 6 meses após agosto, ou seja, quitará a dívida em fevereiro.

6) A expressão $(52678 + 24569^{\smile}39806)$, ao ser dividida por 5, deixa que resto?

Solução: Pelas propriedades 1. e 2. da seção 3, podemos dividir cada um dos números por 5 e operar com os restos das divisões, observe:

$52678 = 10535 \cdot 5 + 3$, com $r = 3$. Logo, $52678 \equiv 3 \bmod 5$.

$24569 = 4913 \cdot 5 + 4$, com $r = 4$. Logo, $24569 \equiv 4 \bmod 5$.

$39806 = 7961 \cdot 5 + 1$, com $r = 1$. Logo, $39806 \equiv 1 \bmod 5$.

Pelas propriedades citadas acima, $(52678 + 24569 - 39806) \equiv (3 + 4 - 1) \bmod 5 \Rightarrow (52678 + 24569 - 39806) \equiv 6 \bmod 5$. Como $6 = 1 \cdot 5 + 1$, com $r = 1$, temos $(52678 + 24569 - 39806) \equiv 1 \bmod 5$.

Ou seja, a expressão $(52678 + 24569 - 39806)$, ao ser dividida por 5, deixa resto 1.

7) A expressão $(52678 \cdot 24569 \cdot 39806)$, ao ser dividida por 5, deixa que resto? *Solução:*

Pelo exercício 6), sabemos que:

$52678 \equiv 3 \bmod 5$.

$24569 \equiv 4 \bmod 5$.

$39806 \equiv 1 \bmod 5$.

Pela propriedade 3. da seção 3, temos: $(52678 \cdot 24569 \cdot 39806) \equiv (3 \cdot 4 \cdot 1) \bmod$

$5 \Rightarrow (52678 \cdot 24569 \cdot 39806) \equiv 12 \bmod 5$. Como $12 = 2 \cdot 5 + 2$, com $r = 2$, temos $(52678 \cdot 24569 \cdot 39806) \equiv 2 \bmod 5$.
Ou seja, a expressão $(52678 \cdot 24569 \cdot 39806)$, ao ser dividida por 5, deixa resto 2.

4 CONSIDERAÇÕES FINAIS

Congruência modular é um conceito aritmético muito importante e de simples entendimento, que pode enriquecer o ensino de Matemática na Educação Básica, porém não é ensinado nem trabalhado nesse segmento de ensino. Com a introdução do conceito de congruência modular nas séries finais do Ensino Fundamental, os alunos terão uma ferramenta a mais para resolver determinadas situações-problema, presentes em exames de acesso à escolas militares no 6º ano do Ensino Fundamental e na OBMEP, de forma mais prática.

REFERÊNCIAS

[1] FERREIRA, Jamil. A Construção dos Números, 2a edição, SBM, 2011.

[2] RIO DE JANEIRO. CMRJ. Coletânea de Provas. 2013. Disponível em: <www.cmrj.ensino.eb.br>. Acesso em: 10 jun. 2015.

[3] IMPA/OBMEP, Banco de Questões. Nível 2. 2006. Rio de Janeiro: IMPA.

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

APÊNDICE A – Demonstrações

Aqui apresentamos uma demonstração para as propriedades da Congruência Modular:

- Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a + c) \equiv (b + d) \bmod n$.
  Demonstração: $n \mid (b - a)$, $n \mid (d - c) \Rightarrow n \mid ((b + d) - (a + c)) \Rightarrow (a + c) \equiv (b + d) \bmod n$.

- Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a - c) \equiv (b - d) \bmod n$.
  Demonstração: $n \mid (b - a)$, $n \mid (c - d) \Rightarrow n \mid ((b - d) - (a - c)) \Rightarrow (a - c) \equiv (b - d) \bmod n$.

- Sejam a, b, c, d e n números inteiros tais que $a \equiv b \bmod n$ e $c \equiv d \bmod n$. Então $(a \cdot c) \equiv (b \cdot d) \bmod n$.
  Demonstração: $bd - ac = b(d - c) + c(b - a)$, como $n \mid (d - c)$ e $n \mid (b - a)$, temos que $n \mid (bd - ac) \Rightarrow bd \equiv ac \bmod n$.

- Sejam a, b, c e n números inteiros tais que $ac \equiv bc \bmod n$ e $mdc(c, n) = 1$. Então $a \equiv b \bmod n$.
  Demonstração: $ac \equiv bc \bmod n \Rightarrow n \mid (bc - ac) \Rightarrow n \mid c(b - a) \Rightarrow n \mid c$ ou $n \mid (b - a)$. Como $mdc(c, n) = 1$, n não divide c , logo $n \mid (b - a) \Rightarrow a \equiv b \bmod n$.