UNIVERSIDADE ESTADUAL DE LONDRINA

LUCIDIO DE JESUS JUNIOR

TEORIA DOS NÚMEROS:
UM ESTUDO COM RESOLUÇÃO DE PROBLEMAS NA EDUCAÇÃO BÁSICA

LONDRINA
2013

LUCIDIO DE JESUS JUNIOR

TEORIA DOS NÚMEROS:
UM ESTUDO COM RESOLUÇÃO DE PROBLEMAS NA EDUCAÇÃO BÁSICA

Dissertação de mestrado apresentada ao Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual de Londrina como requisito parcial à obtenção do título de mestre em Matemática.

Orientador: Prof. Dr. Túlio Oliveira de Carvalho

Londrina
2013

Catalogação elaborada pela Divisão de Processos Técnicos da Biblioteca Central da Universidade Estadual de Londrina

Dados Internacionais de Catalogação-na-Publicação (CIP)

J58t Jesus Junior, Lucidio de.
Teoria dos números : um estudo com resolução de problemas na educação básica / Lucidio de Jesus Junior. – Londrina, 2013.
60 f. : il.

Orientador: Túlio Oliveira de Carvalho.
Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática, 2013.
Inclui bibliografia.

1. Matemática – Estudo e ensino – Teses. 2. Números – Divisibilidade – Teses. 3. Teoria dos números – Formação de conceitos – Teses. 4. Congruências e restos – Teses. I. Carvalho, Túlio Oliveira de. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática. III. Sociedade Brasileira de Matemática. IV. Título.

CDU 51:37.02

LUCIDIO DE JESUS JUNIOR

TEORIA DOS NÚMEROS:
UM ESTUDO COM RESOLUÇÃO DE PROBLEMAS NA EDUCAÇÃO BÁSICA

Dissertação de mestrado apresentada ao Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual de Londrina como requisito parcial à obtenção do título de mestre em Matemática.

BANCA EXAMINADORA

_____
Prof. Dr. Túlio Oliveira de Carvalho - Orientador
Universidade Estadual de Londrina

_____
Prof. Dra. Angela Marta P. das Dores Savioli
Universidade Estadual de Londrina

_____
Prof. Dr. André Luís Machado Martinez
Universidade Tecnológica Federal do Paraná

Londrina, 05 de agosto de 2013.

DEDICO ESTE TRABALHO AOS PROFESSORES DE MATEMÁTICA QUE ATUAM NA EDUCAÇÃO BÁSICA E QUE BUSCAM EM CURSOS DE PÓS-GRADUAÇÃO SE ESPECIALIZAR PARA ASSIM MELHOREM O PROCESSO DE ENSINO APRENDIZAGEM DE MATEMÁTICA.

AGRADECIMENTOS

Agradeço a Deus por toda a saúde e superação das dificuldades durante o curso, também pelos bons momentos presenteados para toda a turma.

Agradeço ao Professor Doutor e orientador Túlio Oliveira de Carvalho, pelo apoio, amizade e encorajamento contínuos na realização deste trabalho. E também a todos os professores que contribuíram para esta realizam na minha vida.

A minha esposa Camila e ao meu filho Emanuel por todo incentivo, cooperação, companheirismo e demais auxílios prestados durante a realização do curso. Além do apoio prestado pelos meus pais, irmã e sogros nesta trajetória.

Aos colegas de curso.

Á Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, pelo apoio financeiro prestado, durante a realização deste mestrado.

A Secretaria de Estado da Educação do Paraná – SEED/PR, pela licença parcial cedida para realização deste curso.

Enfim a todas as pessoas que de forma direta ou indireta contribuíram para a minha especialização.

”A Matemática apresenta invenções tão sutis que poderão servir não só para satisfazer os curiosos como, também para auxiliar as artes e poupar trabalho aos homens.”

(Descartes)

Jesus Jr., Lucídio de. *Teoria dos Números: um estudo com resolução de problemas na Educação Básica***.** 2013. 60 f. Dissertação – Mestrado Profissional em Matemática – Universidade Estadual de Londrina, Londrina 2013.

RESUMO

Este trabalho tem como objetivo rever e mostrar ao professor de Matemática que atua na Educação Básica, como conceitos relacionados à Teoria dos Números podem ser poderosas ferramentas na resolução de algumas situações problemas que envolvem divisibilidade. Como guia da discussão, são propostas quatro situações problemas, para em seguida discutir-se alguns tópicos fundamentais da Aritmética, de congruência, de congruência linear, e o Teorema Chinês dos Restos. Ao final, utilizam-se estes conceitos para solucionar as situações problemas.

Palavras-chave: Divisibilidade. Resolução de problemas. Congruência. Congruência Linear. Teorema Chinês dos Restos.

Jesus Jr., Lucídio de. *Number Theory: a study of problem solving in Basic Education*. 2013. 60 f. Dissertation – Professional Masters in Mathematics – State University in Londrina, Londrina, 2013.

ABSTRACT

This paper has the objective to review and show to the mathematics teacher, who teaches in Basic Education, how the concepts related to Theory of Numbers can be powerful tools to solve some problems situations involving divisibility. As a guide discussion, four problems situations are suggested, after to discuss some essencial topics of Arithmetic, congruence, linear congruence and The Chinese Remainder Theorem. Finally, are used these concepts to solve the problems situations.

Key words: Divisibility. Solving problems. Congruence. Linear congruence. The Chinese Remainder Theorem.

LISTA DE ILUSTRAÇÕES

ABREVIATURAS E SIGLAS

OBMEP – Olimpíada Brasileira de Matemática das Escolas Públicas

OBM – Olimpíada Brasileira de Matemática

ITA – Instituto Tecnológico da Aeronáutica

IME – Instituto Militar de Engenharia

IMPA – Instituto Nacional de Matemática Pura e Aplicada

PCN – Parâmetros Curriculares Nacionais

DCE/PR – Diretrizes Curriculares da Educação Básica do Estado do Paraná

SEED/PR – Secretaria de Estado da Educação do Paraná

SUMÁRIO

1. INTRODUÇÃO

Desde que a Olimpíada Brasileira de Matemática das Escolas Públicas – OBMEP passou a fazer parte do cotidiano escolar, algumas questões propostas nestas provas desafiam o conhecimento matemático tanto dos alunos como dos professores. A OBMEP é realizada pelo IMPA – Instituto Nacional de Matemática Pura e Aplicada – e tem como objetivo estimular o estudo da matemática e revelar talentos na área, com questões que envolvem geometria, aritmética, lógica matemática e álgebra.

Mas não apenas na OBMEP como também em concursos vestibulares como o ITA/IME ou em livros paradidáticos de Matemática, são propostas situações problemas que desafiam seus leitores, questões estas que podem ser resolvidas utilizando alguns conceitos estudados na Teoria dos Números. Em princípio estes problemas propostos parecem ser de difícil solução. Contudo, o professor de Matemática pode não se dar conta, mas em algum momento durante a sua formação, os conceitos da aritmética dos restos ou congruências, congruências lineares, Teorema Chinês dos Restos e também conceitos fundamentais da Teoria dos Números, como: divisibilidade, mínimo múltiplo comum, máximo divisor comum e números primos facilitam a resolução dessas situações problemas.

A Teoria dos Números é a área na qual se estudam as propriedades e as relações entre os números. O estudo destes conceitos é tratado com maior rigor em disciplinas como Álgebra ou Introdução a Álgebra, propostas na graduação de Matemática ou Ciências da Computação, por exemplo. Sendo a aritmética modular uma das ferramentas mais importantes desta área.

Embora os conceitos de divisibilidade, mínimo múltiplo comum, máximo divisor comum e números primos sejam pouco trabalhados na Educação Básica, acredita-se que problemas relacionados à Teoria dos Números tenham um potencial motivador no processo de ensino aprendizagem, pois são de fácil contextualização e possibilitam a elaboração de atividades didáticas capazes de desafiar os alunos, consolidam o aprendizado do conceito de divisibilidade além de promoverem o desenvolvimento do pensamento conceitual algébrico.

Trabalhar com a aritmética e a álgebra simultaneamente é essencial para a formação do educando. De acordo com os Parâmetros Curriculares Nacionais de Matemática do Ensino Fundamental (BRASIL, 1998):

> [...] *Embora nas séries iniciais já se possa desenvolver uma pré-álgebra, é especialmente nas séries finais do ensino fundamental que os trabalhos algébricos serão ampliados; trabalhando com situações-problema, o aluno reconhecerá diferentes funções da álgebra (como modelizar, resolver problemas aritmeticamente insolúveis, demonstrar), representando problemas por meio de equações (identificando parâmetros, variáveis e relações e tomando contato com fórmulas, equações, variáveis e incógnitas) e conhecendo a "sintaxe" (regras para resolução) de uma equação.*

Propor situações problemas desafiadoras desde o Ensino Fundamental, é essencial para auxiliar o educando no processo de abstração que se faz necessário no estudo de álgebra, ou seja, é onde o aluno pode expressar o seu raciocínio por meio de símbolos (letras – incógnitas / variáveis e números - constantes), e assim utilizar o seu conhecimento matemático para solucionar problemas.

Esse processo de abstrair os dados e aplicar o seu conhecimento em Matemática para resolver uma situação problema, estende-se ao Ensino Médio. De acordo com os Parâmetros Curriculares Nacionais de Matemática do Ensino Médio (BRASIL, 2002):

> [...] *O primeiro tema ou eixo estruturador, Álgebra, na vivência cotidiana se apresenta com enorme importância enquanto linguagem, como na variedade de gráficos presentes diariamente nos noticiários e jornais, e também enquanto instrumento de cálculos de natureza financeira e prática, em geral. No ensino médio, esse tema trata de números e variáveis em conjuntos infinitos e quase sempre contínuos, no sentido de serem completos.*

E ainda,

> [...] *Os procedimentos básicos desse tema se referem a calcular, resolver, identificar variáveis, traçar e interpretar gráficos e resolver equações de acordo com as propriedades das operações no conjunto dos números reais e as operações válidas para o cálculo algébrico. Esse tema possui fortemente o caráter de linguagem com seus códigos (números e letras) e regras (as propriedades das operações), formando os termos desta linguagem que são as expressões que, por sua vez, compõem as igualdades e desigualdades.*

O processo de abstração na Educação Básica é fundamental para o cotidiano escolar do educando. E uma das funções do professor é inserir os conceitos matemáticos que envolvem aritmética, álgebra e geometria de forma que torne o estudo de Matemática atrativo ao aluno.

De acordo com as Diretrizes Curriculares Estaduais de Matemática do estado do Paraná (PARANÁ, 2008):

> [...] *O conceito de álgebra é muito abrangente e possui uma linguagem permeada por convenções diversas de modo que o conhecimento algébrico não pode ser concebido pela simples manipulação dos conteúdos abordados isoladamente. Defende-se uma abordagem pedagógica que os articule, na qual os conceitos se complementem e tragam significado aos conteúdos abordados. Na Educação Básica, é preciso estabelecer uma relação intrínseca entre pensamento e linguagem, ou seja, a linguagem algébrica entendida como expressão do pensamento matemático.*

Sendo assim, este trabalho tem como objetivo rever e mostrar ao professor de Matemática, que atua na Educação Básica, como conceitos relacionados à Teoria dos Números podem ser poderosas ferramentas na resolução de algumas situações problemas que envolvem divisibilidade. Do ponto de vista deste trabalho, estas atividades podem ser adaptadas e aplicadas durante o processo de ensino aprendizagem de Matemática na Educação Básica.

No início do trabalho são propostos alguns problemas elementares que devem cativar o interesse de alunos e professores. Em seguida serão revisados alguns conceitos fundamentais da aritmética modular, a saber: divisibilidade, máximo divisor comum, mínimo múltiplo comum e números primos. Então daremos ênfase ao estudo da aritmética dos restos ou congruência, congruência linear e do Teorema Chinês dos Restos. Na sequência, mostraremos como utilizar estes conceitos na resolução dos problemas propostos.

2. PROBLEMATIZAÇÃO

No processo de ensino aprendizagem da Matemática, resolver problemas faz parte do cotidiano dos professores de Matemática da Educação Básica. Para determinar uma estratégia de solução para os diversos problemas propostos em livros didáticos, paradidáticos, revistas, concursos, e até em situações do cotidiano, o profissional que atua na área de Matemática busca ferramentas disponíveis em sua bagagem acadêmica, notadamente propriedades e teoremas. Porém, com o passar dos anos, o professor que atua na Educação Básica tende a utilizar apenas o material proposto pelas instituições de ensino – o livro didático ou apostilas, com resultados prontos e situações problemas de resolução direta. Dificilmente são encontrados nestes materiais alguns teoremas matemáticos seguidos de sua demonstração.

Um dos desafios do Ensino da Matemática é a abordagem de conteúdos para resolver um problema. A metodologia da resolução de problemas dá ao professor a oportunidade de aplicar os conhecimentos matemáticos adquiridos em novas situações, de modo a resolver a questão proposta.

De acordo com (Smole & Diniz, 2001):

> [...] *Cabe ao professor assegurar um espaço de discussão no qual os alunos pensem sobre os problemas que irão resolver, elaborem uma estratégia, apresentem suas hipóteses e façam o registro da solução encontrada ou de recursos que utilizaram para chegarem ao resultado. Isso favorece a formação do pensamento matemático, livre do apego às regras. O aluno pode lançar mão de recursos como a oralidade, o desenho e outros, até se sentir à vontade para utilizar sinais matemáticos.*

E, de acordo com (Polya, 2006), as etapas da resolução de um problema são:

> [...] Compreender o problema; destacar informações, dados importantes do problema, para a sua resolução; elaborar um plano de resolução; executar o plano; conferir resultados; estabelecer nova estratégia, se necessário, até chegar a uma solução aceitável.

Além disso, cumpre ressaltar que dada uma situação problema, esta pode ter, ou não, uma ou mais formas de resolução.

Para enfatizar nosso estudo, vamos considerar as quatro situações problemas a seguir:

Problema 1

No dia 7 de setembro no Brasil, comemora-se o dia da Independência do País. Em algumas cidades são realizados grandes desfiles, onde participam entidades e instituições públicas, privadas, filantrópicas, entre outros grupos participativos em prol da sociedade. Em certa cidade, o comandante do 5º batalhão da polícia militar ficou responsável em organizar os soldados da sua corporação e também do corpo de bombeiros, que são dois dos grupos participantes do desfile. Para isso, pensou em organizá-los em m filas com igual quantidade de pessoas. O comandante então percebeu que, se cada fila fosse composta por 9 soldados, então sobrariam 3, e ao organizar cada fila com 10 soldados, restariam 5. No entanto, ao organizar as filas com de 11 soldados, as m filas ficariam com a mesma quantidade de soldados. Dessa forma, qual é a quantidade soldados que irão desfilar pelo 5º batalhão e pelo corpo de bombeiros no dia da Independência do Brasil, sabendo que o número de soldados é o menor número natural que satisfaz as condições acima?

Problema 2

Camila gostaria de saber o dia da semana em que nasceu e também utilizar o mesmo processo para descobrir o dia do nascimento dos seus amigos. Sabendo que Camila nasceu em 12 de outubro de 1983, ajude-a a efetuar os cálculos necessários para saber o dia da semana do seu nascimento. Em seguida estabeleça um método prático para descobrir o dia da semana em que seus amigos nasceram sabendo que o primeiro dia do mês de janeiro de 1900 foi uma segunda-feira.

Problema 3

Um professor no 2º ano de graduação de Matemática, após revisar com os alunos o estudo de logaritmos e suas propriedades, solicitou que calculassem os seguintes logaritmos.

$$\log_5 2 \qquad \log_7 6 \qquad \log_3 8$$

E, após realizar os cálculos, eles deveriam descrever sobre os resultados obtidos. E ainda, caso notassem alguma regularidade nos resultados obtidos, destacar e conjecturar sobre tal regularidade.

Jonas após realizar os cálculos, observou e conjecturou que os resultados gerados por esses logaritmos, são números irracionais. Mostre que a conjectura citada por Jonas é verdadeira.

Problema 4

Emanuel notou que alguns dos seus amigos recebiam dos seus pais uma quantia mensal em dinheiro, a chamada “mesada”, para que eles gastassem com o que eles desejassem, porém se o dinheiro acabasse antes do dia de receber a mesada, ele não teria o direito de receber nenhuma quantia antecipadamente. Ao conversar com os seus pais sobre receber a tal mesada, os pais ficaram surpresos, conversaram e resolveram aceitar a proposta levantada pelo filho. Na euforia, Emanuel perguntou: Pai, mãe, quanto irei receber?

Então o pai de Emanuel falou: Some o quadrado de cada número natural até 100, pegue o resultado e divida por quatro. Agora, multiplique o resto gerado nessa divisão por 50. Dessa forma saberá antecipadamente o valor da sua mesada. O menino logo correu para o seu quarto e começou a efetuar os cálculos.

Ajude Emanuel a determinar o valor da sua mesada.

Para desenvolver as situações problemas propostas acima, antes vamos rever alguns conceitos que são trabalhados na Educação Básica, acrescentando os estudos de aritmética dos restos ou congruência, congruência linear, seguidos do Teorema Chinês dos Restos.

As definições apresentadas a seguir são acompanhadas de alguns teoremas fundamentais e suas devidas demonstrações, além de lemas e corolários. O processo de demonstração pelo Princípio de Indução Finita (PIF)[1] será utilizado para resolver algumas atividades propostas.

[1] Consulte o livro *Elementos de Aritmética* do autor HEFEZ, A.

3. TÓPICOS DE ARITMÉTICA

Em princípio, vamos considerar os resultados do estudo de divisibilidade dos números inteiros, como segue.

Seja $\mathbb{Z}$ o conjunto dos números inteiros formado pelo conjunto dos números naturais $\mathbb{N}=\{1,2,3,4,...\}$ munido do zero e dos números negativos, ou seja, $\mathbb{Z}=\{...,-3,-2,-1,0,1,2,3,...\}$. E ainda, que tanto as operações de multiplicação ou de adição entre dois ou mais números inteiros, também é um número inteiro. Porém, nem sempre a divisão entre dois números inteiros gera um número inteiro. Considere a definição a seguir:

DIVISIBILIDADE

Sejam a e b inteiros. Diz-se que um número inteiro a divide um número inteiro b, se e somente se, existe um inteiro q tal que $b=a\cdot q$. Neste caso diz-se também que a é divisor de b e que b é múltiplo de a, ou ainda que b é divisível por a. Notação: Indica-se por $a|b$ o fato de a dividir b.

Exemplo 1

Temos que $6|72$, pois $72=6\cdot 12$. Por outro lado, 7 não divide 20, pois não existe um número inteiro k tal que 20 seja igual a $7k$.

De acordo com a definição de divisibilidade, são gerados os resultados abaixo, denotados na proposição 1.

Proposição 1. Sejam a, b e c números inteiros. Então:

Se $a|b$ e $b|c$ então $a|c$.

Se $a|b$ e $a|c$ então $a|(b+c)$ e $a|(c-b)$.

Se a e b são positivos e $a|b$ então $0<a\leq b$.

Se $a|b$ e $b|a$ então $a=b$ ou $a=-b$.

E ainda, como foi visto na definição de divisibilidade nem sempre a divisão entre dois números inteiros resulta em um número inteiro. Para generalizar este fato, Euclides desenvolveu o denominado *Algoritmo da Divisão de Euclides* ou *Divisão Euclidiana*.

ALGORITMO DA DIVISÃO DE EUCLIDES

Teorema. Dados dois inteiros a e b, sendo b positivo, existem únicos inteiros q e r, tais que:

$$a = bq + r, 0 \le r < b.$$

onde q é o quociente e r é o resto da divisão de a (divisor) por b (dividendo).

Demonstração da Existência e da Unicidade do quociente q e do resto r:

Seja S o conjunto de todos os inteiros não negativos que são da forma $a - bx,\ \mathrm{x} \in \mathbb{Z}$, ou seja:

$$S = \{a - b\mathrm{x}; \mathrm{x} \in \mathbb{Z}, a - bx \ge 0\}$$

O conjunto S é não vazio, pois $b > 0$ implica em $b \ge 1$, e, portanto para $x = -|a|$ temos:

$$a - bx = a + b|a| \ge a + |a| \ge 0.$$

Sendo assim, pelo principio da boa ordenação, existe um elemento mínimo r de S tal que:

$$r \ge 0 \text{ e } r = a - bq \text{ ou a} = bq + r, \text{ com q} \in \mathbb{Z}.$$

Além disso, temos $r < b$, pois, se fosse $r \ge b$, teríamos:

$$0 \le r - b = a - bq - b = a - b(q+1) < r.$$

Isto é, r não seria o elemento mínimo de S.

Agora, para mostrar a unicidade, suponha que existam dois outros inteiros r_1 e q_1 tais que:

$$a = bq_1 + r_1 \text{ e } 0 \le r_1 < b$$

Então:

$$bq_1 + r_1 = bq + r \Rightarrow r_1 - r = b(q - q_1) \Rightarrow b|r_1 - r.$$

Por outro lado, temos:

$$-b < -r \le 0 \text{ e } 0 \le r_1 < b \ \Rightarrow -b < r_1 - r < b, \text{ isto é: } |r_1 - r| < b.$$

Assim, $b|r_1 - r$ e $\mathrm{b} > |r_1 - r|$ e, portanto $r_1 - r = 0$ e como $b \ne 0$, também temos $q - q_1 = 0$. Logo, $r_1 = r$ e $\mathrm{q}_1 = q$. ■

Exemplo 2

Mostre que o resto da divisão de 10^n por 9 é sempre 1, com $n \in \mathbb{N}$.

Solução

Mostraremos por Indução Finita. Para $n = 1$ temos que:

$$10^1 = 9 \cdot 1 + 1,$$

portanto para $n = 1$ a proposição é verdadeira.

Suponha agora que o resultado seja válido para um n qualquer, ou seja:

$$10^n = 9 \cdot q + 1.$$

Considere a igualdade:

$$10^{n+1} = (9+1) \cdot 10^n = 9 \cdot 10^n + 10^n = 9 \cdot 10^n + 9q + 1 = 9 \cdot (10^n + q) + 1 = 9q' + 1.$$

Provando que o resultado vale para $n+1$, e consequentemente vale para todo $n \in \mathbb{N}$, pelo PIF. ■

Note que para mostrar o resultado proposto no exemplo 2, a partir do algoritmo de Euclides foi utilizado o PIF, mostrando que o resultado é válido para todo $n \in \mathbb{N}$.

Outro importante resultado do estudo de divisibilidade é o lema a seguir:

LEMA DOS RESTOS. A soma e o produto de quaisquer dois números naturais deixa o mesmo resto que a soma e o produto dos seus restos, na divisão por um inteiro positivo a.

Demonstração:

Parte I - do produto.

Sejam $x, y \in \mathbb{N}$. Ao dividir ambos por a, temos que:

$$x = aq_1 + r_1 \text{ e } y = aq_2 + r_2, 0 \le r_1, r_2 < a,\ q_1, q_2, r_1, r_2 \in \mathbb{Z}.$$

Ao efetuarmos a multiplicação de x e y, segue que:

$$xy = (aq_1 + r_1) \cdot (aq_2 + r_2) \Rightarrow xy = a \cdot (aq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2 \Rightarrow$$
$$\Rightarrow xy = aq + r_1r_2 \ (*)$$

Note que o produto dos restos r_1r_2 pode ser maior do que a. Então fazendo a divisão euclidiana de r_1r_2 por a, temos:

$$r_1r_2 = ak + r,\ \ k, r \in \mathbb{Z} \text{ e } 0 \le r < a \ (**).$$

Substituindo r_1r_2 na equação $(*)$ pelo resultado obtido em $(**)$, segue que:

$$xy = aq + ak + r \Rightarrow xy = a(q + k) + r \Rightarrow$$
$$\Rightarrow xy = am + r, m \in \mathbb{Z}, 0 \leq r < a.$$

Portanto, o resto deixado pelo produto dos restos da divisão de x e y por a, é igual ao resto deixado pela divisão do produto de xy por a.

Parte II – da soma.

Utilizando o mesmo raciocínio acima, ao efetuarmos a soma de x e y, temos:

$$x + y = (aq_1 + r_1) + (aq_2 + r_2) \Rightarrow x + y = a \cdot (q_1 + q_2) + (r_1 + r_2) \Rightarrow$$
$$\Rightarrow x + y = aq + (r_1 + r_2), (*)$$

Como $r_1 + r_2$ pode ser maior do que a, então fazemos a divisão euclidiana de $r_1 + r_2$ por a:

$$(r_1 + r_2) = ak + r, k, r \in \mathbb{Z} \text{ e } 0 \leq r < a, (**).$$

Substituindo $r_1 + r_2$ na equação $(*)$ pelo resultado obtido em $(**)$, segue que:

$$x + y = aq + ak + r \Rightarrow x + y = a(q + k) + r \Rightarrow$$
$$\Rightarrow x + y = am + r, m \in \mathbb{Z}, 0 \leq r < a.$$

Portanto, o resto deixado pela soma dos restos da divisão de x e y por a, é igual ao resto deixado pela divisão da soma $x + y$ por a. ■

Para mostrar como esse resultado é útil na resolução de problemas, considere a situação proposta no exemplo a seguir.

Exemplo 3

Prove que em qualquer triângulo retângulo com lados inteiros, pelo menos um deles é múltiplo de 3.

Solução

Temos que os possíveis restos na divisão euclidiana de um número natural n qualquer por 3, são: 0, 1 ou 2. Elevando n ao quadrado, os possíveis restos da divisão de n^2 por 3, pelo lema dos restos, são: 0 ou 1.

Logo, se n^2 não é múltiplo de 3 então o resto da divisão de n^2 por 3 é igual a 1. E caso seja múltiplo, então o resto é igual a 0.

Por outro lado, sejam a e b os catetos de um triângulo retângulo e c a sua hipotenusa. Suponha que nem a, nem b e nem c sejam múltiplos de 3. Logo a soma $a^2 + b^2$ deixa resto 2 na divisão por 3, enquanto que c^2 deixa resto 1. O que contradiz o Teorema de Pitágoras, pois $a^2 + b^2 = c^2$.

Portanto, em qualquer triângulo retângulo com lados inteiros, pelo menos um deles é múltiplo de 3. ■

Note que para resolver a situação problema proposta no exemplo 3, o lema dos restos foi uma ferramenta eficiente.

Para dar continuidade ao nosso estudo, revisaremos o estudo do máximo divisor comum ou simplesmente do m.d.c. entre dois ou mais números naturais.

MÁXIMO DIVISOR COMUM (m.d.c.)

Definição. Sejam $a, b \in \mathbb{N}$. Um número $d \in \mathbb{N}$ se diz máximo divisor comum de a e b, se:

- ✓ $d \mid a$ e $d \mid b$
- ✓ Se c é um número natural tal que $c \mid a$ e $c \mid b$ então $c \mid d$.

Proposição 2. Dados $a, b \in \mathbb{N}$, o máximo divisor comum de a e b é único.

Demonstração:

De fato, se d e d' satisfazem a definição, então $d` \mid d$ (pois $d` \mid a$ e $d` \mid b$) e $d \mid d`$ (pois $d \mid a$ e $d \mid b$ e d' é por hipótese o máximo divisor comum de a e b). Implicando que $d = d`$. ■

Denotamos o máximo divisor comum de a e b, como:

$$mdc(a,b).$$

De acordo com a definição de m.d.c., temos que $mdc(a,b) = mdc(b,a)$.

Para verificar a existência do máximo divisor comum, primeiramente precisamos dos resultados gerados pelas proposições a seguir.

Proposição 3. Se $a \mid b$ então $mdc(a,b) = a$.

Demonstração:

De fato, $a \mid a$ e $a \mid b$ (hipótese). E se $c \mid a$ e $c \mid b$, segue que $c \mid a$. ■

Proposição 4. Se a e b são números inteiros e $a = bq + r$ onde q e r são inteiros, então:

$$mdc(a,b) = mdc(b,r).$$

Demonstração:

Da relação, $a = bq + r$ pode-se concluir que todo divisor de b e r é um divisor de a. Esta mesma relação, escrita na forma $r = a - bq$, nos diz que todo divisor de a e b é divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante que o $mdc(a,b) = mdc(b,r)$.

Para mostrar a existência de um máximo divisor comum, será aplicado sucessivamente, a partir de a e b, o algoritmo da divisão, como segue:

$$a = bq_1 + r_1, (r_1 < b)$$
$$b = r_1q_2 + r_2, (r_2 < r_1)$$
$$r_1 = r_2q_3 + r_3, (r_3 < r_2), ...$$

Dessa forma, se acontecer de r_1 ser nulo, então a proposição 3 nos garante que $b = mdc(a,b)$, e o processo finaliza na primeira etapa. Mas, de qualquer maneira, na sequência $b > r_1 > r_2 > r_3 > ...$ para algum índice n deverá ocorrer que $r_{n+1} = 0$. De fato, se todos os r_i forem não nulos, então $\{b, r_1, r_2, r_3, ...\}$ não teria mínimo, o que é impossível. Assim, para algum n:

$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1}.$$

Como consequência das proposições 3 e 4, obtemos então o seguinte:

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = ... = mdc(b, r_1) = mdc(a,b)$$

Portanto $r_n = mdc(a,b)$. ■

O processo de efetuar as divisões sucessivas para determinar o máximo divisor comum entre dois ou mais números é denominado como o *Algoritmo de Euclides*.

Outro importante resultado que é tratado na Educação Básica é a definição a seguir:

Definição. Dois números naturais a e b se dizem primos entre si se $mdc(a,b) = 1$. Neste caso diz se também que a é primo com b e vice-versa.

Proposição 5. Dois números consecutivos a e $a+1$ são sempre primos entre si.

Demonstração:

De fato, temos que $1 \mid a$ e $1 \mid a+1$. Agora, se $c \mid a$ e $c \mid a+1$, então $c \mid \big((a+1)-a\big)$, ou seja, $c \mid 1$. ■

Proposição 6. Se $d = mdc(a,b)$, *então* $mdc(sa, sb) = sd$, para todo $s \in \mathbb{N}$.

Demonstração:

Multipliquemos por s cada uma das igualdades obtidas pelo algoritmo da divisão no processo das divisões sucessivas que leva a d, a partir de a e b:

$$\begin{aligned} sa &= sbq_1 + sr_1 \\ sb &= sr_1q_2 + sr_2 \\ &... \\ sr_{n-2} &= sr_{n-1}q_n + sr_n \\ sr_{n-1} &= sr_nq_{n+1}. \end{aligned}$$

E, de acordo com as proposições 3 e 4, temos que:

$$sd = sr_n = mdc\left(sr_{n-1}, sr_n\right) = ... = mdc\left(sb, sr_1\right) = mdc(sa, sb)$$

Portanto,

$$mdc(sa, sb) = sd. \ ■$$

Corolário 1. Se $a,\ b \in \mathbb{N}$ e $mdc(a,b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, ou seja, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.

Demonstração:

Temos que

$$d = mdc(a,b) = mdc\left(d\,\frac{a}{d}, d\,\frac{b}{d}\right) = d \cdot mdc\left(\frac{a}{d}, \frac{b}{d}\right), d \neq 0.$$

Então

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \ ■$$

Corolário 2. Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.

Demonstração:

Da hipótese $mdc(a,b) = 1$, decorre que $mdc(ac, bc) = c$. Como $a \mid bc$, por hipótese, e é claro que $a \mid ac$, então $a \mid mdc(ac, bc)$.

Portanto $a \mid c$. ■

Para exemplificar o processo de determinar o m.d.c. entre dois ou mais números naturais, considere os exemplos 4 e 5, a seguir.

Exemplo 4

Calcule o $mdc(1126,522)$ pelo processo das divisões sucessivas e escreva as igualdades relacionadas.

Solução

Efetuando as divisões sucessivas, temos que:

$$1126 = 522\times 2 + 82$$
$$522 = 82\times 6 + 30$$
$$82 = 30\times 2 + 22$$
$$30 = 22\times 1 + 8$$
$$22 = 8\times 2 + 6$$
$$8 = 6\times 1 + 2$$
$$6 = 2\times 3 + 0$$

Logo,

$$mdc(1126,522) = mdc(522,82) = mdc(82,30) = mdc(30,22) =$$
$$= mdc(22,8) = mdc(8,6) = mdc(6,2) = 2$$

Exemplo 5

Calcule o $mdc\left(\underbrace{111...111}_{100\ vezes}, \underbrace{111...111}_{60\ vezes}\right)$.

Solução

Primeiro escrevemos os números na base decimal, ou seja:

$$\underbrace{111...111}_{100\ vezes} = 10^{99} + 10^{98} + 10^{97} + ... + 1$$

$$\underbrace{111...111}_{60\ vezes} = 10^{59} + 10^{58} + 10^{57} + ... + 1$$

Aplicamos o Algoritmo de Euclides para obter as igualdades:

$$\underbrace{111...111}_{100\ vezes} = \left(10^{59} + 10^{58} + 10^{57} + ... + 1\right)10^{40} + 10^{39} + 10^{38} + ... + 1,$$
$$10^{59} + 10^{58} + 10^{57} + ... + 1 = \left(10^{39} + 10^{38} + 10^{37} + ... + 1\right)10^{20} + 10^{19} + 10^{18} + ... + 1,$$
$$10^{39} + 10^{38} + 10^{37} + ... + 1 = \left(10^{19} + 10^{18} + 10^{17} + ... + 1\right)10^{20} + 10^{19} + 10^{18} + ... + 1.$$

Portanto:

$$mdc\left(\underbrace{111...111}_{100\ vezes},\underbrace{111...111}_{60\ vezes}\right)=10^{19}+10^{18}+10^{17}+...+1=\underbrace{111...111}_{20\ vezes}.$$

Note que no exemplo 4, a aplicação do algoritmo de Euclides foi utilizada de forma direta para obter o $mdc(1126,522)$. Já no exemplo 5, deve-se fazer uma manipulação numérica ao aplicar o algoritmo de Euclides.

Assim como é importante o estudo do máximo divisor comum entre dois ou mais números naturais na Educação Básica, temos também o estudo do menor múltiplo comum entre dois ou mais números naturais. Estes dois conceitos são utilizados na resolução de muitas situações problemas de Matemática, além de serem fundamentais na resolução de problemas que envolvem o estudo de congruência e congruência linear, que iremos ver adiante.

Pois bem, a definição do mínimo múltiplo comum entre dois ou mais números naturais, ou simplesmente m.m.c., é dada a seguir:

MÍNIMO MÚLTIPLO COMUM (m.m.c.)

Definição. O mínimo múltiplo comum de dois naturais a e b é o menor inteiro positivo que é múltiplo simultaneamente de a e de b, isto é, $mmc(a,b)$ é o menor s tal que existem r e t tais que $s=ra$, e $s=tb$. Se $a=0$ ou $b=0$ então $mmc(a,b)$ é zero por definição. E ainda:

$$mmc(a,b)=mmc(b,a)=m.$$

Para os demais casos, a garantia de existência é dada pela proposição a seguir.

Proposição 7. *Para quaisquer* $a, b\in\mathbb{N}$*, se* $d=mdc(a,b)$, então $m=\dfrac{ab}{d}$ é o mínimo múltiplo comum de a *e* b.

Demonstração:

Note que, como $d\mid(ab)$ então $m=\dfrac{ab}{d}$, $m\in\mathbb{N}$.

Como, evidentemente,

$$a\cdot\left(\frac{b}{d}\right)=\frac{ab}{d}=m,$$

Então $a \mid m$. Analogamente, $b \mid m$.

Seja m' um múltiplo de a e de b, e suponhamos $m` = ar$ e $m` = bs$, então $ar = bs$ e, portanto,

$$\frac{a}{d} r = \frac{b}{d} s.$$

Daí segue que $\frac{a}{d}$ divide $\frac{b}{d} s$ e, como $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ então $\frac{a}{d} \Big| s$. Assim,

$$s = \frac{a}{d} t, t \in \mathbb{N}.$$

E como, $m` = bs$, obtemos:

$$m` = b\frac{a}{d} t = \frac{ab}{d} t = mt,$$

ou seja,

$$m \mid m`. \ \blacksquare$$

Corolário 3. Se a e b são primos entre si então $mmc(a,b) = ab$. *De fato, como* $d = mdc(a,b) = 1$, então:

$$mmc(a,b) = m = \frac{ab}{1} = ab \ .$$

Assim como no estudo do máximo divisor comum, se $mmc(a,b) = m$, então:

$$mmc(sa, sb) = sm, \ \ s \in \mathbb{N} \ .$$

Demonstração:

Quando $a = 0$ ou $b = 0$, então $m = 0$ e $sa = 0$ ou $sb = 0$, daí $mmc(sa, sb) = ms = 0.$ Se $s = 0$ então $mmc(0a, 0b) = mmc(0,0) = 0$.

Agora, dados a e b não nulos, temos que:

$$mmc(sa, sb) = \frac{sa \cdot sb}{mdc(sa, sb)} = \frac{s^2 (a \cdot b)}{s \cdot mdc(a,b)} = s\frac{ab}{d} = s \cdot mmc(a,b). \ \blacksquare$$

A extensão do conceito de mínimo múltiplo comum em $\mathbb{N}$ para três ou mais números se faz naturalmente.

Para exemplificar o processo de obtenção do m.m.c. entre dois ou mais números naturais, considere os exemplos 6 e 7, a seguir.

Exemplo 6

Determine os números naturais a e b, tais que o $mdc(a,b)=12$ e $mmc(a,b)=240$.

Solução

Pela proposição 7 temos que:

$$mmc(a,b)\cdot mdc(a,b)=ab \Rightarrow 240\cdot 12=ab.$$

Note que $240\cdot 12=20\cdot 12\cdot 12$, segue:

$$240\cdot 12=ab \Rightarrow 20=\frac{a}{12}\cdot\frac{b}{12}.$$

E, como $mdc\left(\frac{a}{12},\frac{b}{12}\right)=1$, então $\frac{a}{12}=1$ e $\frac{b}{12}=20$ ou $\frac{a}{12}=4$ e $\frac{b}{12}=5$.

Portanto, as possíveis soluções são: 12 e 240 ou 48 e 60.

Exemplo 7

Dois amigos passeiam de bicicleta, na mesma direção, em torno de uma pista circular. Para dar uma volta completa um deles demora 15 minutos e o outro demora 18 minutos. Eles partem juntos e combinam interromper o passeio quando os dois se encontrarem pela primeira vez no ponto de partida. Quantas voltas deu cada um?

Uma Solução

Neste caso, devemos determinar uma quantidade comum de voltas entre os dois amigos, de tal maneira que seja a menor possível, após o inicio do passeio. Para isso, sejam a e b o número de voltas de cada um dos amigos. Note que o tempo total de corrida é o menor valor positivo de P que satisfaz as igualdades:

$$P=15a=18b \Rightarrow$$

$$\Rightarrow P=mmc(15,18)=\frac{15\cdot 18}{mdc(15,18)}\Rightarrow.$$

$$\Rightarrow P=\frac{15\cdot 18}{3}\Rightarrow P=90$$

Portanto, o número de voltas a é igual a 6, enquanto que o número de voltas b é igual a 5.

Outro conceito que é tratado na Educação Básica, e é um dos conceitos fundamentais em Teoria dos Números é o estudo dos *números primos*.

Ao longo da história da Matemática, os números primos foram protagonistas de célebres problemas que motivaram o desenvolvimento de teorias e técnicas pelas

mentes mais férteis, como Fermat, Euler e Gauss. Até hoje muitos desses problemas, simples de enunciar, que envolvem números primos são desafios intelectuais para toda a humanidade. O matemático grego Euclides foi o primeiro a provar que há uma sequencia infinita de números primos, por volta de 300 a. C.

NÚMEROS PRIMOS

Definição. Diz-se que um inteiro positivo p > 1 é um número primo ou apenas um primo se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se composto.

O inteiro positivo 1 não é nem primo e nem composto, e por conseguinte se a é um inteiro positivo qualquer, então a é primo, ou a é composto ou $a = 1$.

A partir desta definição, verifica-se que o número 2 é o único número par que é primo.

LEMA DE EUCLIDES. Se p é primo e $p \mid ab$ então $p \mid a$ ou $p \mid b$.

Demonstração:

Sejam $a \neq 0$ e $b \neq 0$. Admitamos que p não divide a e provemos que $mdc(a, p) = 1$. De fato, se $c \mid a$ e $c \mid p$ então $c = 1$ ou $c = p$ (pois p é primo); como, porém, p não divide a, então $c = 1$. E pelo corolário 2, temos que $p \mid b$. ■

Como consequência da definição de números primos, temos um dos principais teoremas do estudo da Teoria dos Números, a saber.

TEOREMA FUNDAMENTAL DA ARITMÉTICA (T.F.A.). Todo número inteiro n maior do que 1 pode ser representado de maneira única como um produto de fatores primos.

Demonstração:

Se n é primo não há nada a ser demonstrado. Suponhamos agora n composto. Seja $p_1 \left(p_1 > 1 \right)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois caso contrário existiria $p, 1 < p < p_1$ com $p \mid n$, contradizendo a escolha de p_1. Logo, $n = n_1 p_1,\ n_1 \in \mathbb{Z}$. Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento

anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$. Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros positivos maiores do que 1 este processo deve terminar. Como os primos na sequência $p_1, p_2, ..., p_k$, não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}.$$

Para mostrarmos a unicidade usamos indução finita em n.

Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é:

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j.

Como p_1 divide o produto $q_1 q_2 ... q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $\frac{n}{p_1} = p_2 p_3 ... p_s = q_2 q_3 ... q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_r$ são iguais. ■

O CRIVO DE ERATÓSTENES

Eratóstenes de Cirene (280 – 192 a. C.) foi um sábio de atividades várias, que além de matemático foi astrônomo, geógrafo e filósofo. Provavelmente é mais conhecido pelo seu fato de ter sido o responsável por calcular a circunferência da Terra.

O chamado crivo de Eratóstenes é um procedimento que ajuda a determinar quais são os números naturais primos em um intervalo qualquer de 1 a n, partindo de um quadro contendo todos esses números e consequentemente eliminado todos os números que não são primos.

Proposição 8. Se n > 1 é um número composto, então há um número primo p tal que:

$$p \mid n \text{ e } p^2 \leq n \ \left(\Leftrightarrow p \leq \sqrt{n}\right).$$

Demonstração:

Por hipótese, n pode ser decomposto da seguinte maneira:

$$n = ab(2 \leq a \leq b < n).$$

Logo, $n = ab \geq a^2$.Seja p um divisor primo de a. Então $p^2 \mid a^2$ e, portanto, $p^2 \leq a^2$. Donde $p^2 \leq n$, o que pode ser traduzido por $p \leq \sqrt{n}$. ■

Exemplo 8

Determine se o número 271 é primo ou composto.

Solução

Temos que:

$$256 < 271 < 289 \Rightarrow \sqrt{256} < \sqrt{271} < \sqrt{289} \Rightarrow 16 < \sqrt{271} < 17 .$$

Os números primos menores que 16, são: 2, 3, 5, 7, 11 e 13. Mas nenhum destes números é divisor de 271. Portanto 271 é um número primo.

Vamos determinar todos os números primos compreendidos entre 1 e 50.

Inicialmente verificamos que:

$$49 < 50 < 121 \Rightarrow \sqrt{49} < \sqrt{50} < \sqrt{121} \Rightarrow 7 < \sqrt{50} < 11 .$$

Então basta trabalhamos com os primos 2, 3, 5 e 7. Pelo método de Eratóstenes, basta eliminar todos os múltiplos de 2, 3, 5 e 7 menores do que 50. O resultado segue no quadro a seguir:

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

Neste caso, os números que aparecem em vermelho são os números compostos. Observe que nos primeiros 50 números naturais, existem apenas 15 números primos.

É fácil encontrar números primos pequenos, porém encontrar números primos maiores torna-se cada vez mais difícil.

Após rever os conceitos de divisibilidade, do m.d.c., do m.m.c. e dos números primos, seguidos de seus principais resultados e demonstrações, daremos inicio aos estudos da aritmética dos restos (congruências), congruência linear e do Teorema Chinês dos Restos. Estes conceitos são tratados com exclusividade na graduação, mas nada impede o professor de Matemática de inseri-los na Educação Básica, por meio de situações problemas ou como proposta de desafios aos seus alunos.

4. A ARITMÉTICA DOS RESTOS (CONGRUÊNCIAS)

O conceito da aritmética dos restos está relacionado com o estudo de bases numéricas. Como vimos no estudo da divisão euclidiana, ao efetuarmos a divisão de um número inteiro não negativo a por um número inteiro positivo b, isto gera um quociente q e um resto r. Note que ao fixarmos o número b, os possíveis valores do resto r, são:

$$0,1,2,3,...,b-1.$$

Por exemplo, ao efetuarmos a divisão euclidiana de 5 por 2 ou de 7 por 2, as divisões irão ter quocientes diferentes, porém o resto gerado nestas divisões é igual a 1.

Por outro lado, o sistema universalmente utilizado para representar os números naturais é o sistema decimal posicional, onde, todo número natural n é escrito como um polinômio:

$$n = a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + ... + a_r 10^r$$

onde, r ≥ 0 e os $a_i \in \{0,1,2,...,9\} (i = 1,2,3,...,r)$ estão univocamente determinados. E sua escrita é dada por:

$$a_r ... a_3 a_2 a_1 a_0$$

Como mostra o exemplo a seguir:

$$712 = 2 + 1 \cdot 10^1 + 7 \cdot 10^2 .$$

Mas, podemos pensar que é uma opção se trabalhar com a base 10 em nosso sistema de numeração. Existem outros sistemas de numeração em uso, além do sistema decimal. Por exemplo, a base 2 ou sistema binário como é chamado, é utilizado na computação. Além do que, pode-se trabalhar com qualquer base em um sistema de numeração posicional, como mostra o teorema a seguir:

Seja b um número natural maior do que 1 e seja $M = \{0,1,2,...,b-1\}$. Então todo número n pode ser representado univocamente da seguinte maneira:

$$n = a_0 + a_1 b^1 + a_2 b^2 + a_3 b^3 + ... + a_r b^r ,$$

onde,

$$r \geq 0 , \ a_i \in M (i = 1,2,3,...,r) \text{ e } a_r \neq 0.$$

Por exemplo, o número 52 (escrito na base 10) pode ser escrito em qualquer base que desejamos, ou seja, se b for igual a 5 então a sua escrita só pode ser realizada com os algarismos 0, 1, 2, 3 ou 4 (que são os possíveis restos da divisão de um número inteiro positivo por 5). Neste caso, efetuamos sucessivamente a divisão euclidiana de 52 por 5 até obtermos quociente zero. Observe:

$$52 = 10 \times 5 + 2$$
$$10 = 2 \times 5 + 0$$
$$2 = 0 \times 5 + 2$$

Observe que os restos das divisões sucessivas são 2, 0 e 2. Então o número 52 quando escrito na base 5, é igual a $52 = 2 + 0 \times 5 + 2 \times 5^2$ e representado por $(202)_5$.

Observe como o estudo da aritmética dos restos está relacionado com o estudo das bases numéricas, pois em ambos os casos, levamos em consideração o resto gerado na divisão. O professor pode inserir estes conceitos ao trabalhar a divisibilidade no Ensino Fundamental.

A aritmética dos restos também é denominada como congruência.

O estudo de congruência, bem como a notação por meio da qual se torna um dos instrumentos mais fortes da Teoria dos Números, foi introduzido por Karl Friedrich Gauss (1777 – 1855), em sua Disquisitiones Arithmeticae de 1801.

Antes de iniciarmos o estudo de congruência, considere a situação problema:

Dado que $7^4 = 2401$, determine os algarismos da dezena e da unidade do número 7^{99999}.

É claro que resolver a potência não é o melhor caminho. Então para resolver não só problemas desta forma, mas também varias outras situações, utilizamos o estudo de congruências para auxiliar a resolução. Do estudo da divisão euclidiana temos que dados $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$, existe e são únicos $q, \mathrm{r} \in \mathbb{Z}$, tal que:

$$a = bq + r, 0 \leq r < b. \text{ (i)}$$

Digamos que:

$$c = bq` + r, 0 \leq r < b. \text{ (ii)}$$

De (i) e (ii), segue que:

$$a - r = bq \text{ e } c - r = bq`.$$

O fato de $a-r$ e $c-r$ serem múltiplos de b cria uma relação entre a e c que pode ser explorada. O ponto é definir um conjunto de números cujo resto da divisão por b é r.

Quando a divisão de a por b produz o resto r, podemos simbolizar essa divisão euclidiana $a = bq + r$ por:

$$\begin{cases} a \equiv r \ (\text{mod b}), \text{ ou} \\ a \equiv r \ (\text{b}), \text{ ou} \\ a \overset{b}{\equiv} r. \end{cases}$$

O símbolo $\overset{b}{\equiv}$ é conhecido como congruência módulo b. Assim quando um inteiro a ou c produz o mesmo resto r quando divididos por b, dizemos que a e c pertencem a uma mesma classe de equivalência[2] módulo b.

CONGRUÊNCIAS

Sejam a, b e c números inteiros, $b > 0$. Dizemos que a é congruente a c módulo b, se $b \mid a - c$.

Por exemplo, os números 23 e 15 pertencem à mesma classe de equivalência módulo 8, pois:

$$8 \mid 23 - 15.$$

Ou seja, 23 e 15 são congruentes quando b = 8. Denotamos este fato por:

$$23 \overset{8}{\equiv} 15$$

Onde 23 e 15 pertencem à classe de equivalência 7 módulo 8.

A definição acima estabelece uma relação sobre $\mathbb{Z}$, chamada de congruência, para a qual valem as propriedades a seguir:

i) Para todo $b > 0$, a relação de congruência é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência. Para qualquer $a, b, c \in \mathbb{Z}, b > 0$, temos:

a) $a \in \mathbb{Z} \Rightarrow a \overset{b}{\equiv} a;$

b) $a \overset{b}{\equiv} c \Rightarrow c \overset{b}{\equiv} a;$

[2] Congruência é uma relação de equivalência.

c) $a \overset{b}{\equiv} c$ e $c \overset{b}{\equiv} d \Rightarrow a \overset{b}{\equiv} d$;

Demonstração do item (c):

Por hipótese $a \overset{b}{\equiv} c$ e $c \overset{b}{\equiv} d$, então:

$$b \mid a-c \text{ e } b \mid c-d \Rightarrow b \mid (a-c)+(c-d) \Rightarrow b \mid a-d \Rightarrow a \overset{b}{\equiv} d. \blacksquare$$

ii) Para quaisquer $a, c \in \mathbb{Z}: a \overset{b}{\equiv} c$ se, e somente se, a e c fornecem o mesmo resto na divisão euclidiana por b.

Demonstração:

($\Rightarrow$) Por hipótese $a = c + bk, k \in \mathbb{Z}.$ Se a divisão euclidiana de c por b se expressa por $c = bq + r, 0 \leq r < b,$ então:

$$a = c + bk \Rightarrow a = bq + r + bk \Rightarrow a = b\underbrace{(q+k)}_{q'} + r\,.$$

Como $0 \leq r < b$, então r é o resto na divisão euclidiana de a por b.

($\Leftarrow$) Se

$$a = bk_1 + r \text{ e } c = bk_2 + r, 0 \leq r < b,$$

Então,

$$a - c = bk_1 + r - (bk_2 + r) \Rightarrow a - c = b\underbrace{(k_1 - k_2)}_{k_3}.$$

Portanto,

$$b \mid a - c. \blacksquare$$

iii) Se $a \overset{b}{\equiv} c$, então $a \pm x \overset{b}{\equiv} c \pm x$ e $ax \overset{b}{\equiv} cx, \forall x \in \mathbb{Z}.$

Demonstração (produto de a e c por x).

Por hipótese

$$b \mid a - c \Rightarrow a - c = bk, k \in \mathbb{Z}.$$

Logo,

$$ax - cx = b(kx) \Rightarrow ax \overset{b}{\equiv} cx. \blacksquare$$

iv) Se $a \overset{b}{\equiv} c$ e $x \overset{b}{\equiv} y$, então $a \pm x \overset{b}{\equiv} c \pm y$ e $ax \overset{b}{\equiv} cy$.

Demonstração (produto de ax e cy).

Das hipóteses e pela propriedade (iii), temos que:

$$ax \overset{b}{\equiv} cx \text{ e } xc \overset{b}{\equiv} yc.$$

Logo, pela transitividade:

$$ax \overset{b}{\equiv} cy. \quad \blacksquare$$

Em particular, em decorrência da propriedade (iv), temos:

v) Se $a \overset{b}{\equiv} c$ então $ka \overset{b}{\equiv} kc$ e $a^k \overset{b}{\equiv} c^k, \forall k \in \mathbb{Z} : k \geq 1$.

Dessa forma, para verificar se dois números são congruentes módulo b, não é necessário efetuar a divisão euclidiana de ambos por b para depois comparar os seus restos.

Por exemplo, ao efetuar a divisão euclidiana de um número inteiro por 3, temos que os possíveis restos r, são: 0, 1 e 2.

Sendo assim, podemos induzir que os inteiros pertencentes ao conjunto $A = \{..., -4, -1, 1, 4, 7, ...\}$, estão na categoria dos que produzem resto 1, quando divididos por 3, enquanto que os inteiros que pertencem ao conjunto $B = \{..., -6, -3, 0, 3, 6, ...\}$ estão na categoria dos que produzem resto 0, e ainda, os inteiros que pertencem ao conjunto $C = \{..., -5, -2, 2, 5, ...\}$ estão na categoria dos que produzem resto 2, quando divididos por 3. Estes conjuntos são chamados de "classes de equivalência módulo 3", pois neles estão inteiros que produzem o mesmo resto na divisão por 3. As classes de equivalências podem ser denotadas entre colchetes ou com uma barra sobre o valor de r. Por exemplo, a classe de equivalência de inteiros que produz resto 0, pode ser denotada como:

$$\overline{0} \text{ ou } [0].$$

A definição a seguir generaliza este fato.

SISTEMA COMPLETO DE RESÍDUOS

Dado um conjunto A de b inteiros, $b > 0$, temos que A é um sistema completo de resíduos módulo b se dois quaisquer desses números, diferentes entre si, não são congruentes módulo b.

Por exemplo, o conjunto $A=\{0,1,2,3,4,...,b-1\}$ é um sistema completo de resíduos módulo b. De fato, se i e j são inteiros tais que $0 \le i < j < b$, então $0 < j-i < b$ e, portanto j não é congruente a i módulo b. Esse conjunto é chamado de sistema completo de resíduos mínimos positivos.

Proposição 9. Se $\{r_1, r_2, r_3, ..., r_m\}$ é um sistema completo de resíduos módulo b, então todo inteiro positivo a é congruente a um e somente um dos r_i.

Demonstração:

Pelo algoritmo da divisão temos que:

$$a = bq + r, 0 \le r < b \Leftrightarrow a \overset{b}{\equiv} r.$$

onde, $r \in \{0,1,2,3,4,...,b-1\}$. Por outro lado, a divisão de $r_1, r_2, r_3, ..., r_m$ por b fornecerá b restos, distintos dois a dois, e daí, para um certo r_j, obter-se-á:

$$r_j = bq_j + r \text{ ou } r_j \overset{b}{\equiv} r.$$

Como $a \overset{b}{\equiv} r$, então $a \overset{b}{\equiv} r_j$. E se $a \overset{b}{\equiv} r_k$ então $r_j \overset{b}{\equiv} r_k$ o que implica que $r_j = r_k$ pela definição de sistema completo de resíduos.

Agora temos as ferramentas necessárias para resolver o problema proposto inicialmente, vejamos:

Dado que $7^4 = 2401$, determine os algarismos da dezena e da unidade do número 7^{99999}.

Solução

Temos que

$$99999 = 4 \times 24999 + 3 \text{ e } 7^4 = 2401 \overset{100}{\equiv} 1.$$

Segue,

$$7^{99999} = 7^{4 \times 24999 + 3} = 7^{4 \times 24999} \cdot 7^3 = \left(7^4\right)^{24999} \cdot 7^3.$$

Note que 7^4 deixa resto 1 quando dividido por 100, então:

$$\left(7^4\right)^{24999} \cdot 7^3 \overset{100}{\equiv} (1)^{24999} \cdot 7^3 \overset{100}{\equiv} 7^3.$$

Como 7^3 é igual a 343, temos que:

$$343 \overset{100}{\equiv} 43.$$

Portanto os algarismos da unidade e da dezena do número 7^{99999} são 3 e 4, reciprocamente.

O estudo de congruências é fundamental tanto para a resolução de problemas como o apresentado acima, como em muitas aplicações do cotidiano, como a geração dos números de um código de barras, geração dos números de um CPF ou RG. Outra importante aplicação de congruências é no ramo da criptografia, que consiste em manter informações sigilosas e pessoais em segurança, como é o caso das senhas bancárias e de um e-mail, por exemplo.

CRIPTOGRAFIA

A palavra criptografia provém do grego e significa, em outras palavras, "esconder a escrita". A criptografia estuda os métodos para codificar (esconder) uma mensagem de modo que só a pessoa destinada a ler a mensagem e que possua a chave secreta, consiga decifrá-la.

A ocultação da escrita tem longa data e durante todo esse tempo diferentes mecanismos foram e são utilizados até os dias de hoje. Um exemplo de utilização é transmissão de dados via internet. Mas voltando um pouco no tempo, em 1563, Blaise de Vigenere criou uma cifra baseando-se no método desenvolvido por Júlio César em criptografar uma mensagem, denominada como *Cifra de César*[3].

Inicialmente ele associou cada letra do alfabeto a um número de 0 a 25, e fornecia uma chave cujas letras representavam os deslocamentos da cifra de César:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

De acordo com as informações acima, vamos decifrar o código "xaimeltxks" sabendo que a palavra chave é "lapis".

Em princípio, escrevemos a palavra chave repetindo-a sob cada letra até o final da mensagem a ser decodificada, como mostra o quadro a seguir:

x	a	i	m	e	l	t	x	k	s
l	a	p	i	s	l	a	p	i	s

Seja z_i a letra a ser descoberta a partir de uma letra y_i que está cifrada, então:

[3] Na cifra de César, cada letra a ser codificada é substituída por outra, que se apresenta no alfabeto abaixo dela um número n de vezes. Por exemplo, se $n = 2$ então a palavra "*pouco*" codificada é escrita como "*nmsam*".

$$z_i \overset{26}{\equiv} y_i - \delta_i + 26,$$

onde δ_i é o deslocamento.

Vamos agora descodificar a mensagem. A primeira letra criptografada é “x” que corresponde ao número 23. O deslocamento da letra z_1 foi feito pela letra “l”, que corresponde ao número 11. Calculando z_1, segue:

$$z_1 \overset{26}{\equiv} y_1 - \delta_1 + 26 \Rightarrow z_1 \overset{26}{\equiv} 23 - 11 + 26 \Rightarrow z_1 \overset{26}{\equiv} 38 \Rightarrow z_1 \overset{26}{\equiv} 12 \Rightarrow z_1 = \text{`}m\text{`}.$$

Então a primeira letra da mensagem original corresponde a letra “m”. Procedendo desta forma até o fim da mensagem criptografada, temos:

$$z_2 \overset{26}{\equiv} 0 - 0 + 26 \Rightarrow z_2 \overset{26}{\equiv} 26 \Rightarrow z_2 \overset{26}{\equiv} 0 \Rightarrow z_2 = \text{`}a\text{`}$$
$$z_3 \overset{26}{\equiv} 8 - 15 + 26 \Rightarrow z_3 \overset{26}{\equiv} 19 \Rightarrow z_3 = \text{`}t\text{`}$$
$$z_4 \overset{26}{\equiv} 12 - 8 + 26 \Rightarrow z_4 \overset{26}{\equiv} 30 \Rightarrow z_4 \overset{26}{\equiv} 4 \Rightarrow z_4 = \text{`}e\text{`}$$
$$z_5 \overset{26}{\equiv} 4 - 18 + 26 \Rightarrow z_5 \overset{26}{\equiv} 12 \Rightarrow z_5 = \text{`}m\text{`}$$
$$z_6 \overset{26}{\equiv} 11 - 11 + 26 \Rightarrow z_6 \overset{26}{\equiv} 26 \Rightarrow z_6 \overset{26}{\equiv} 0 \Rightarrow z_6 = \text{`}a\text{`}$$
$$z_7 \overset{26}{\equiv} 19 - 0 + 26 \Rightarrow z_7 \overset{26}{\equiv} 45 \Rightarrow z_7 \overset{26}{\equiv} 19 \Rightarrow z_7 = \text{`}t\text{`}$$
$$z_8 \overset{26}{\equiv} 23 - 15 + 26 \Rightarrow z_8 \overset{26}{\equiv} 34 \Rightarrow z_8 \overset{26}{\equiv} 8 \Rightarrow z_8 = \text{`}i\text{`}$$
$$z_9 \overset{26}{\equiv} 10 - 8 + 26 \Rightarrow z_9 \overset{26}{\equiv} 28 \Rightarrow z_9 \overset{26}{\equiv} 2 \Rightarrow z_9 = \text{`}c\text{`}$$
$$z_{10} \overset{26}{\equiv} 18 - 18 + 26 \Rightarrow z_{10} \overset{26}{\equiv} 26 \Rightarrow z_{10} \overset{26}{\equiv} 0 \Rightarrow z_{10} = \text{`}a\text{`}$$

De acordo com as operações de congruência acima, concluímos que o código decifrado é “Matemática”.

Para fazer o processo inverso, ou seja, esconder uma mensagem pelo sistema criado por Vigenere basta fazer $z_i \overset{26}{\equiv} y_i + \delta_i$, onde y_i é a letra original e z_i será a letra cifrada.

Existem outras formas de codificar informações, muitas das quais não fazem o uso de congruências, outras utilizam esquemas mais elaborados, como curvas elípticas[4], por exemplo.

[4] A criptografia com Curvas Elípticas foi proposta por Victor Miller (1986) e Neal Koblitz (1987).

CÓDIGO DE BARRAS EAN-13

Outra aplicação do estudo de congruências no nosso cotidiano é a geração do dígito verificador do código de barras EAN-13, que é o mais usado no mundo todo. Constituído de 13 algarismos, sendo que o último é o dígito de controle. Para determinar o dígito de controle, é utilizada a congruência módulo 10 e os fatores que compõem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita. Sendo S a soma das multiplicações, basta determinar o valor x tal que $x \overset{10}{\equiv} S$. Para exemplificar, seja a situação problema:

João estava anotando os códigos de barras dos produtos do seu bazar para inseri-los no sistema eletrônico que acabou de comprar para melhor acompanhar o estoque, porém um lote do produto A apresentou falha na impressão do 13º dígito. Dessa forma, qual é o 13º dígito que João deve inserir no sistema?

Figura 1 - Código de barras do produto A

Solução

Seja x o dígito verificador. Pelo processo descrito acima, basta fazer:

$$1\cdot 5+3\cdot 9+1\cdot 0+3\cdot 1+1\cdot 2+3\cdot 3+1\cdot 4+3\cdot 1+1\cdot 2+3\cdot 3+1\cdot 4+3\cdot 5+x \overset{10}{\equiv} 0$$

Segue que,

$$83+x \overset{10}{\equiv} 0 \Rightarrow 83+x=10k \Rightarrow x=10k-83 \Rightarrow x=7.$$

Portanto João deve inserir o número 7, pois é o menor inteiro não-negativo no conjunto solução.

Outro importante resultado que utiliza a notação de congruência e que auxilia na resolução de muitos problemas é o teorema a seguir.

PEQUENO TEOREMA DE FERMAT. Se p é um número primo e $a \in N$, então:

$$a^p \overset{p}{\equiv} a.$$

Além disso, se p não divide a, então:

$$a^{p-1} \overset{p}{\equiv} 1.$$

Este teorema é utilizado para a codificação e decodificação de mensagens, além de facilitar a resolução de problemas, como mostra o exemplo a seguir.

Exemplo 9

Determine o resto da divisão da soma $S = 1^{16} + 2^{16} + 3^{16} + ... + 85^{16}$ por 17.

Solução

Pelo Pequeno Teorema de Fermat, temos que:

$a^{16} \overset{17}{\equiv} 1$, se 17 não divide a, e, $a^{16} \overset{17}{\equiv} 0$, se 17 divide a.

Como $85 = 17 \times 5$, então existem 5 múltiplos de 17 no intervalo de 1 a 85. Logo, teremos 80 números não múltiplos de 17 e que elevados a 16 são côngruos a 1. Segue que:

$$S = 1^{16} + 2^{16} + 3^{16} + ... + 85^{16} \Rightarrow S \overset{17}{\equiv} \underbrace{1+1+1+...+1}_{80} + \underbrace{0+...+0}_{5} \Rightarrow S \overset{17}{\equiv} 80.$$

Logo o resto da divisão da soma S por 17 é igual a 12, pois $80 = 17 \times 4 + 12$.

5. CONGRUÊNCIAS LINEARES

Por outro lado, para resolver problemas onde a situação não é apenas numérica, e sim algébrica, recorremos ao estudo de *congruência linear.*

CONGRUÊNCIA LINEAR

Uma congruência algébrica do tipo $ax \overset{m}{\equiv} b$, onde a, b e m são números inteiros, $a \neq 0$, e x é uma variável em $\mathbb{Z}$, recebe o nome de congruência linear ou congruência do primeiro grau.

Seja k uma solução de $ax \overset{m}{\equiv} b$, ou seja, k é um inteiro tal que $ak \overset{m}{\equiv} b$. Aplicando o algoritmo da divisão para k e m,

$$k = mq + x_0, 0 \leq x_0 < m.$$

Assim, $ak = amq + ax_0$, e como $m \overset{m}{\equiv} 0$ e, portanto, $amq \overset{m}{\equiv} 0$, então $ax_0 \overset{m}{\equiv} ak$. Segue que:

$$ax_0 \overset{m}{\equiv} b,$$

o que mostra que x_0 também é solução da congruência considerada.

Trabalhamos com a classe de equivalência dos $x \in \mathbb{Z}$ tais que $x \overset{m}{\equiv} x_0$.

Proposição 10. Uma congruência linear $ax \overset{m}{\equiv} b$, com $a \neq 0$, admite soluções em $\mathbb{Z}$ se, e somente se, b é divisível por $d = mdc(a, m)$. E, neste caso, se x_0 é uma solução particular, então o conjunto de todas as soluções tem d elementos, a saber:

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d}.$$

Demonstração:

Seja x_0 uma solução de $ax \overset{m}{\equiv} b$. Então $ax_0 + my_0 = b,$ para algum $y_0 \in \mathbb{Z}$. Logo, (x_0, y_0) é uma solução da equação diofantina $ax - my = b$. Da mesma forma, se (x_0, y_0) é solução de $ax - my = b$, então x_0 é solução de $ax \overset{m}{\equiv} b$. Como a condição de

existência de soluções para $ax - my = b$, é que b seja divisível por $d = mdc(a,m)$, o mesmo vale para $ax \overset{m}{\equiv} b$.

Lembremos ainda que, se (x_0, y_0) é solução de $ax - my = b$, então:

$$x = x_0 + \frac{m}{d}t, \text{ e } y = y_0 + \frac{a}{d}t, \ (t \in \mathbb{Z}),$$

fornecem todas as soluções. Logo, a solução genérica de $ax \overset{m}{\equiv} b$ é dada por:

$$x = x_0 + \frac{m}{d}t, (t \in \mathbb{Z}).$$

Aplicando o algoritmo da divisão para t e d, $t = dq + r, 0 \le r < d$. Assim,

$$x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r) = x_0 + \frac{m}{d}r + mq \overset{m}{\equiv} x_0 + \frac{m}{d}r,$$

ou seja, x está entre as soluções apontadas no enunciado.

Por outro lado, supondo:

$$x_0 + \frac{m}{d}t_1 \overset{m}{\equiv} x_0 + \frac{m}{d}t_2, 0 \le t_1 < t_2 < d.$$

Então,

$$\frac{m}{d}t_1 \overset{m}{\equiv} \frac{m}{d}t_2$$

E como $mdc\left(\frac{m}{d}, m\right) = \frac{m}{d}$, então $t_1 \overset{d}{\equiv} t_2$, o que é impossível.

Sendo assim, as soluções do enunciado, não sendo congruentes mutuamente módulo m, são todas as soluções de $ax \overset{m}{\equiv} b$. ■

Exemplo 10

Determine o conjunto solução da congruência $6x \overset{21}{\equiv} 15$.

Solução

Note que 6 é uma solução particular da congruência $6x \overset{21}{\equiv} 15$. Como o $mdc(6,21) = 3$, então o conjunto de todas as soluções da congruência, é dado por:

$$\left\{6, 6 + \frac{21}{3}, 6 + 2 \cdot \frac{21}{3}\right\} = \{6, 13, 20\}.$$

De acordo com a proposição 10, temos que dado $ax \overset{m}{\equiv} b$ se tem $mdc(a,m)=1$, então essa congruência linear só admite uma solução. Como é o caso de $3x \overset{5}{\equiv} 1$, cujo conjunto solução é $\{2\}$.

6. O TEOREMA CHINÊS DOS RESTOS

No primeiro século da nossa era, o matemático e astrônomo chinês Sun-Tsu, propôs o seguinte problema:

Qual é o menor número que deixa resto 2, 3 e 2 quando dividido, respectivamente, por, 3, 5 e 7?

Para resolver o problema proposto por Sun-Tsu, devemos determinar um número x que satisfaz as três congruências lineares a seguir:

$$x \overset{3}{\equiv} 2,\ x \overset{5}{\equiv} 3 \text{ e } x \overset{7}{\equiv} 2.$$

Ou seja, devemos resolver um sistema de congruências lineares.

TEOREMA CHINÊS DOS RESTOS. Sejam m_1, m_2, ..., m_r números inteiros maiores que zero e tais que $mdc(m_i, m_j) = 1$, sempre que $i \neq j$. Façamos $m = m_1 \cdot m_2 \cdot ... \cdot m_r$ e sejam b_1, b_2, ..., b_r, respectivamente, soluções das congruências lineares.

$$\frac{m}{m_j} y \overset{m_j}{\equiv} 1, (j = 1, 2, ..., r).$$

Então o sistema:

$$\begin{cases} x \overset{m_1}{\equiv} a_1 \\ x \overset{m_2}{\equiv} a_2 \\ \vdots \\ x \overset{m_r}{\equiv} a_r \end{cases}$$

é possível (admite soluções) para quaisquer $a_1, a_2, ..., a_r \in \mathbb{Z}$ e sua solução geral é dada por

$$x \overset{m}{\equiv} a_1 b_1 \frac{m}{m_1} + ... + a_r b_r \frac{m}{m_r}.$$

Demonstração:

Como $mdc(m_j, m_i) = 1$ para $i \neq j$, então:

$$mdc\left(m_j, \frac{m}{m_j}\right) = 1.$$

Isso implica que existem soluções para cada congruência linear $\frac{m}{m_j} y \overset{m_j}{\equiv} 1$, as quais indicamos por $b_j \left(j = 1, 2, ..., r \right)$. Assim,

$$\frac{m}{m_j} b_j \overset{m_j}{\equiv} 1,$$

E, portanto,

$$\frac{m}{m_j} a_j b_j \overset{m_j}{\equiv} a_j, \; j = 1, 2, ..., r.$$

Por outro lado, se $i \neq j$:

$$\frac{m}{m_i} \overset{m_j}{\equiv} 0 .$$

E então

$$a_i b_i \frac{m}{m_i} \overset{m_j}{\equiv} 0.$$

Logo,

$$a_1 b_1 \frac{m}{m_1} + ... + a_j b_j \frac{m}{m_j} + ... + a_r b_r \frac{m}{m_r} \overset{m_j}{\equiv} a_j \text{, para todo } \; j, \; 1 \leq j \leq r.$$

Portanto $x_0 = \sum_{i=1}^{r} a_i b_i \frac{m}{m_i}$ é uma solução particular do sistema.

Então $x \overset{m}{\equiv} x_0$ é a solução geral posto que, como $mdc\left(m_i, m_j \right) = 1$, sempre que $i \neq j$, então:

$$mmc\left(m_1, m_2, ..., m_r \right) = m_1 \cdot m_2 \cdot ... \cdot m_r = m \text{ . } \blacksquare$$

Agora, resolvendo o problema proposto por Sun-Tsu, temos:

$$\begin{cases} x \overset{3}{\equiv} 2 \\ x \overset{5}{\equiv} 3 \\ x \overset{7}{\equiv} 2 \end{cases}$$

Pelo Teorema Chinês dos Restos, temos que:

$$x \overset{N}{\equiv} n_1 y_1 r_1 + n_2 y_2 r_2 + n_3 y_3 r_3$$

Onde:

$$n_1 = m.m.c.(m_2, m_3) \Rightarrow n_1 = m.m.c.(5,7) \Rightarrow n_1 = 35$$
$$n_2 = m.m.c.(m_1, m_3) \Rightarrow n_2 = m.m.c.(3,7) \Rightarrow n_2 = 21$$
$$n_3 = m.m.c.(m_1, m_2) \Rightarrow n_3 = m.m.c.(3,5) \Rightarrow n_3 = 15$$
$$N = m.m.c.(m_1, m_2, m_3) \Rightarrow N = m.m.c.(3,5,7) = 105$$
$$r_1 = 2$$
$$r_2 = 3$$
$$r_3 = 2$$

E,

$$n_1 y_1 \overset{3}{\equiv} 1 \Rightarrow 35 y_1 \overset{3}{\equiv} 1 \Rightarrow y_1 = 2$$
$$n_2 y_2 \overset{5}{\equiv} 1 \Rightarrow 21 y_2 \overset{5}{\equiv} 1 \Rightarrow y_1 = 1$$
$$n_3 y_3 \overset{7}{\equiv} 1 \Rightarrow 15 y_3 \overset{7}{\equiv} 1 \Rightarrow y_3 = 1$$

Logo:

$$x \overset{105}{\equiv} 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2$$
$$x \overset{105}{\equiv} 233 \Rightarrow x \overset{105}{\equiv} 23$$

Portanto, pelo Teorema Chinês dos Restos, o número x é igual a 23.

Este teorema é fundamental para resolver situações problemas onde é possível a adequação para um sistema de congruências lineares. E muitas atividades que antes pareciam insolúveis, agora com o estudo de congruências e congruências lineares, seguido do Teorema Chinês dos Restos, tornam-se triviais.

7. SOLUÇÕES DOS PROBLEMAS

Após estudar e rever alguns tópicos da Teoria dos Números, vamos resolver os problemas de 1 a 4 utilizando os conceitos e propriedades vistos anteriormente.

Problema 1

No dia 7 de setembro no Brasil, comemora-se o dia da Independência do País. Em algumas cidades são realizados grandes desfiles, onde participam entidades e instituições públicas, privadas, filantrópicas, entre outros grupos participativos em prol da sociedade. Em certa cidade, o comandante do 5º batalhão da polícia militar ficou responsável em organizar os soldados da sua corporação e também do corpo de bombeiros, que são dois dos grupos participantes do desfile. Para isso, pensou em organizá-los em m filas com igual quantidade de pessoas. O comandante então percebeu que, se cada fila fosse composta por 9 soldados, então sobrariam 3, e ao organizar cada fila com 10 soldados, restariam 5. No entanto, ao organizar as filas com de 11 soldados, as m filas ficariam com a mesma quantidade de soldados. Dessa forma, qual é a quantidade soldados que irão desfilar pelo 5º batalhão e pelo corpo de bombeiros no dia da Independência do Brasil, sabendo que o número de soldados é o menor número natural que satisfaz as condições acima?

Uma solução

Devemos encontrar um número X, tal que a divisão deste número por 9, 10 e 11, deixa restos 3, 5 e 0, simultaneamente. Ou seja, qual é o número X que satisfaz as congruências lineares:

$$X \overset{9}{\equiv} 3, X \overset{10}{\equiv} 5 \text{ e } X \overset{11}{\equiv} 0.$$

Para isso, basta resolver o sistema de congruências:

$$\begin{cases} X \overset{9}{\equiv} 3 \\ X \overset{10}{\equiv} 5 \\ X \overset{11}{\equiv} 0 \end{cases}$$

Pelo Teorema Chinês do Resto, temos que:

$$X \overset{N}{\equiv} n_1 y_1 r_1 + n_2 y_2 r_2 + n_3 y_3 r_3$$

Onde:

$$n_1 = m.m.c.(m_2, m_3) \Rightarrow n_1 = m.m.c.(10,11) \Rightarrow n_1 = 110$$
$$n_2 = m.m.c.(m_1, m_3) \Rightarrow n_2 = m.m.c.(9,11) \Rightarrow n_2 = 99$$
$$n_3 = m.m.c.(m_1, m_2) \Rightarrow n_3 = m.m.c.(9,10) \Rightarrow n_3 = 90$$
$$N = m.m.c.(m_1, m_2, m_3) \Rightarrow N = m.m.c.(9,10,11) = 990$$
$$r_1 = 3$$
$$r_2 = 5$$
$$r_3 = 0$$

E,

$$n_1 y_1 \overset{9}{\equiv} 1 \Rightarrow 110 y_1 \overset{9}{\equiv} 1 \Rightarrow 2 y_1 \overset{9}{\equiv} 1 \Rightarrow y_1 = 5$$
$$n_2 y_2 \overset{10}{\equiv} 1 \Rightarrow 99 y_2 \overset{10}{\equiv} 1 \Rightarrow 9 y_2 \overset{10}{\equiv} 1 \Rightarrow y_2 = 9$$

Observe que não é necessário o cálculo de y_3, pois r_3 é igual a 0. Logo:

$$X \overset{990}{\equiv} 110 \cdot 5 \cdot 3 + 99 \cdot 9 \cdot 5$$
$$X \overset{990}{\equiv} 6105$$
$$X \overset{990}{\equiv} 165$$

Portanto, pelo Teorema Chinês dos Restos a quantidade de soldados que vão desfilar pelo 5º batalhão da polícia e pelo corpo de bombeiros é igual a 165, ou seja, o comandante organizará 15 filas com 11 soldados cada.

Comentário: Esse problema pode ser proposto na Educação Básica como um desafio aos educandos, onde o aluno tem que descobrir qual é o menor número que dividido por 9, 10 e 11, deixam os respectivos restos 3, 5 e 0.

Problema 2

Camila gostaria de saber o dia da semana em que nasceu e também utilizar o mesmo processo para descobrir o dia do nascimento dos seus amigos. Sabendo que Camila nasceu em 12 de outubro de 1983, ajude-a a efetuar os cálculos necessários para saber o dia da semana do seu nascimento. Em seguida estabeleça um método prático para descobrir o dia da semana em que seus amigos nasceram sabendo que o primeiro dia do mês de janeiro de 1900 foi uma segunda-feira.

Uma solução

Como uma semana tem 7 dias, então vamos associar cada dia da semana a um dos restos da divisão de um inteiro positivo por 7, conforme o quadro 1 a seguir:

segunda	terça	quarta	quinta	sexta	sábado	domingo
0	1	2	3	4	5	6

Atribuímos o valor zero (0) a segunda-feira, de acordo com os dados fornecidos pelo problema.

E ainda, os meses de janeiro, março, maio, julho, agosto, outubro e dezembro possuem 31 dias, enquanto que os meses de abril, junho, setembro e novembro possuem 30 dias. E o mês de fevereiro em ano bissexto ele possui 29 dias, enquanto que em anos não bissextos, ele possui 28.

Se todos os meses possuíssem 28 dias, não era necessário realizar cálculo algum, pois o dia 1 de janeiro de qualquer ano seria sempre uma segunda feira. Mas não é o caso, pois de mês em mês o dia da semana desloca-se conforme o resto da divisão por 7. Iremos atribuir o valor deslocado com o passar dos meses durante um ano, como mostra o quadro 2, a seguir.

Para isso vamos considerar os anos que não são bissextos.

Mês	Deslocamento (mod 7)	Dias no mês	Dias no mês (mod 7)
Janeiro	0	31	3
Fevereiro	3	28	0
Março	3	31	3
Abril	6	30	2
Maio	1	31	3
Junho	4	30	2
Julho	6	31	3
Agosto	2	31	3
Setembro	5	30	2
Outubro	0	31	3
Novembro	3	30	2
Dezembro	5	31	3

O mês de janeiro recebe zero (0) pelo fato de ser o mês de referência. Já para o mês de julho, por exemplo, atribuímos o valor 6 pelo fato de junho ter acumulado 4 dias e mais 2 por ter 30 dias. Como Camila nasceu em outubro, o deslocamento é igual a zero (0).

E finalmente, cada ano desloca-se em uma unidade, pois 365 é congruente a 1 módulo 7.

Pois bem, de 1900 a 1983, o deslocamento foi de 83 unidades. E durante 83 anos tivemos 20 anos bissextos. Como ela nasceu em outubro então o deslocamento entre os meses é igual a 0. E ainda, nasceu no 12º dia do mês, em relação ao dia 1º, são 11 deslocamentos. Somando os deslocamentos, temos:

$$83+20+0+11=114$$

E 114 é congruente a 2 módulo 7. Conforme o quadro 1, o resto 2 refere-se a uma quarta feira.

Criando um método prático, de acordo com os cálculos efetuados anteriormente, basta seguirmos alguns passos:

Passo 1 – Faça a subtração entre o ano de nascimento e o ano 1900. Represente essa subtração por x_1.

Passo 2 – Agora faça a divisão de x_1 por 4, e determine a quantidade x_2 inteira de anos bissextos.

Passo 3 – Verifique o número do deslocamento x_3 referente ao mês de nascimento, no quadro 2.

Passo 4 – Calcule a diferença entre o dia do nascimento e o dia 1º. Represente essa subtração por x_4.

Após realizar os quatro passos acima, some x_1, x_2, x_3 e x_4. Em seguida faça a divisão da soma por 7. Por fim verifique no quadro 1 qual é o dia associado ao resto da divisão. Dessa forma Camila pode determinar o dia da semana que um de seus amigos nasceu a partir da data de nascimento.

Problema 3

Um professor no 2º ano de graduação de Matemática, após revisar com os alunos o estudo de logaritmos e suas propriedades, solicitou que calculassem os seguintes logaritmos.

$$\log_5 2 \qquad \log_7 6 \qquad \log_3 8$$

E, após realizar os cálculos, eles deveriam descrever sobre os resultados obtidos. E ainda, caso notassem alguma regularidade nos resultados obtidos, destacar e conjecturar sobre tal regularidade.

Jonas após realizar os cálculos, observou e conjecturou que os resultados gerados por esses logaritmos, são números irracionais. Mostre que a conjectura citada por Jonas é verdadeira.

Uma solução

Inicialmente, com o auxílio de uma calculadora científica, vamos resolver os logaritmos propostos pelo professor.

a) $\log_5 2 = 0.43067655807339305067010656876397...$

b) $\log_7 6 = 0.92078222116160179031872724517 62...$

c) $\log_3 8 = 1.89278926071437231129858134302 83...$

Em todos os casos, possivelmente os resultados gerados na calculadora para esses logaritmos são número irracionais. Note ainda que os números atribuídos ao logaritmando e a base, em cada caso, são primos entre si, ou seja, o máximo divisor comum entre eles é igual a 1.

Dessa forma, consideremos os números naturais: a, b, m e n, tal que o $mdc(a,b)=1$, $mdc(m,n)=1$ e $\log_b a = \frac{m}{n}$, ou seja, $\log_b a$ é um número racional.

Segue,

$$\log_b a = \frac{m}{n} \Leftrightarrow b^{\frac{m}{n}} = a\,.$$

Elevando ambos os lados da igualdade $b^{\frac{m}{n}} = a$ a n, segue:

$$b^m = a^n \quad (*)$$

Pelo Teorema Fundamental da Aritmética, os números a e b, podem ser escritos como produto de números primos, ou seja:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_i, \ e$$
$$b = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_j.$$

E ainda, dado $k \in \{1, 2, ..., i\}$ temos que $p_k < p_{k+1}$. Da mesma forma, dado $k \in \{1, 2, ..., j\}$ temos que $q_k < q_{k+1}$.

Segue em (*) que:

$$b^m = a^n \Rightarrow q_1^m \cdot q_2^m \cdot q_3^m \cdot \ldots \cdot q_j^m = p_1^n \cdot p_2^n \cdot p_3^n \cdot \ldots \cdot p_i^n$$

Então pelo Teorema Fundamental da Aritmética, não só i é igual a j, como p_k é igual a q_k para todo k e $m = n$. O que é uma contradição, pois a e b são primos entre si.

Portanto dados a e b, inteiros positivos maiores do que um (1) e primos entre si, então o logaritmo de base b e logaritmando a é um número irracional.

Mostrando assim, que a conjectura observada por Jonas é verdadeira.

Problema 4

Emanuel notou que alguns dos seus amigos recebiam dos seus pais uma quantia mensal em dinheiro, a chamada “mesada”. Para que eles gastassem com o que eles desejassem, porém se o dinheiro acabasse antes do dia de receber a mesada, ele não teria o direito de receber nenhuma quantia antecipadamente. Ao conversar com os seus pais sobre receber a tal mesada, os pais ficaram surpresos, conversaram e resolveram aceitar a proposta levantada pelo filho. Na euforia, Emanuel perguntou: Pai, mãe, quanto irei receber?

Então o pai de Emanuel falou: Some o quadrado de cada número natural até 100, pegue o resultado e divida por quatro. Agora, multiplique o resto gerado nessa divisão por 50. Dessa forma saberá antecipadamente o valor da sua mesada. O menino logo correu para o seu quarto e começou a efetuar os cálculos.

Ajude Emanuel a determinar o valor da sua mesada.

Uma solução

Inicialmente, pensamos em elevar cada um dos 100 primeiros números naturais ao quadrado e efetuar a soma, e na sequência proceder como o pai de Emanuel solicitou. Mas, e se não fossem os 100, e sim o quadrado dos 1000 primeiros números naturais, ou até mesmo dos 10000 primeiros. É o que nos leva a raciocinar em criar uma estratégia de resolução, que exija o mínimo de cálculos possível.

Para isso, seja S a soma do quadrado dos 100 primeiros números naturais. Sabemos que os possíveis restos da divisão de um número natural n por 4, são: 0, 1, 2 e 3, ou seja:

$$n \overset{4}{\equiv} 0,\ n \overset{4}{\equiv} 1,\ n \overset{4}{\equiv} 2 \text{ ou } n \overset{4}{\equiv} 3.$$

Elevando ao quadrado cada um dos restos, segue que:

$$\begin{cases} n^2 \overset{4}{\equiv} 0^2 \Rightarrow n^2 \overset{4}{\equiv} 0 \\ n^2 \overset{4}{\equiv} 1^2 \Rightarrow n^2 \overset{4}{\equiv} 1 \\ n^2 \overset{4}{\equiv} 2^2 \Rightarrow n^2 \overset{4}{\equiv} 4 \Rightarrow n^2 \overset{4}{\equiv} 0 \\ n^2 \overset{4}{\equiv} 3^2 \Rightarrow n^2 \overset{4}{\equiv} 9 \Rightarrow n^2 \overset{4}{\equiv} 1. \end{cases}$$

Ou seja, os possíveis restos da divisão do quadrado de um número natural n por 4, são: 0 ou 1.

Pois bem, de 1 a 100, temos 50 números que elevados ao quadrado e divididos por 4 geram resto 0 (pares), e, 50 números que elevados ao quadrado e divididos por 4 geram resto 1 (ímpares), na divisão.

Desta forma:

$$S \overset{4}{\equiv} 1^2 + 2^2 + 3^2 + ... + 98^2 + 99^2 + 100^2 \Rightarrow$$

$$S \overset{4}{\equiv} 1 + 0 + 1 + ... + 0 + 1 + 0 \Rightarrow$$

$$S \overset{4}{\equiv} 50 \Rightarrow S \overset{4}{\equiv} 2$$

Portanto o resto da divisão da soma S por 4 é igual a 2.

Como Emanuel vai receber 50 vezes esse valor, então ele receberá R$ 100,00, de mesada.

OUTRAS PROPOSTAS INTERESSANTES

1. (OBMEP – 2012) Júlio escreveu todos os números de 1 a 1000. Depois ele apagou o número 3 e, em ordem crescente, prosseguiu apagando os números que eram soma de dois números não apagados. Quantos números restaram quando Júlio terminou a tarefa?

a) 333 **b) 335** **c) 337** **d) 340** **e) 345**

2. Calcule o resto da divisão de $N = 1^{2007} + 2^{2007} + 3^{2007} + ... + 2006^{2007} + 2007^{2007}$ por 5.

3. (DOMINGUES, 2009) Um bando de 17 piratas, ao tentar dividir entre si, igualmente, as moedas de ouro de uma arca, verifica que 3 moedas sobrariam. Na discussão que se seguiu, um dos piratas foi morto; na nova tentativa de divisão, já com um pirata a menos, desta feita 10 moedas sobrariam. Novo quiproquó e mais um pirata é morto. Mas agora, por fim, é possível dividir igualmente a fortuna entre eles. Qual é o menor número de moedas que a arca poderia conter?

Respostas:

1) Item B.

2) 4.

3) O menor número de moedas é 3930.

8. CONCLUSÃO

Os estudos de divisibilidade, do máximo divisor comum e do mínimo múltiplo comum como também dos números primos iniciam-se na Educação Básica e são vistos com maior rigor no Ensino Superior, em cursos de graduação relacionados à área das ciências exatas, como é o caso do curso de Matemática. A proposta aqui formulada é que estes conteúdos sejam mais explorados tanto no Ensino Fundamental como no Ensino Médio. O Algoritmo da Divisão de Euclides e o Teorema Fundamental da Aritmética são inseridos de forma implícita nesta fase de aprendizagem dos educandos, mas não são mencionados com a devida nomenclatura e importância. O Lema dos Restos não aparece nos Parâmetros Curriculares Nacionais de Matemática e nem nas Diretrizes Curriculares Estaduais de Matemática do estado do Paraná como proposta de ensino no currículo da Educação Básica, mas nada impede o professor de Matemática de trabalhar este lema nessa fase de aprendizagem. Como foi visto no exemplo 3, atividade que envolve o estudo do Teorema de Pitágoras e divisibilidade, o Lema dos Restos foi fundamental para a solução do problema.

Os estudos de congruência, congruência linear e do Teorema Chinês dos Restos são realizados no Ensino Superior. Os conceitos de congruência e congruência linear, e suas propriedades são fundamentais para resolver atividades mais elaboradas que envolvem divisibilidade. Por fim, o Teorema Chinês dos Restos é essencial para solucionar um sistema de congruências lineares. Há variadas aplicações em situações problemas do cotidiano em que estes conceitos são utilizados.

As situações problemas propostas inicialmente foram resolvidas por meio dos tópicos da Teoria dos Números desenvolvidos neste trabalho. No problema 1 foi aplicado o Teorema Chinês dos Restos para determinar o total de soldados a participar do desfile. Nos problemas 2 e 4, o conceito de congruência e algumas de suas propriedades foram essenciais para resolver essas atividades. E por fim, no problema 3 foi utilizado o estudo de máximo divisor comum seguido do Teorema fundamental da Aritmética para resolução.

O tema abordado constitui uma fonte "pródiga" em problemas que os alunos aceitarão bem, especialmente aqueles que se sintam movidos pela Matemática.

Dessa forma, situações problemas que envolvem a Teoria dos Números, incluindo as que foram desenvolvidas neste trabalho, serão adequadas (se for o caso) e propostas aos alunos da Educação Básica, por meio de atividades complementares ou desafios. As diversas facetas dos resultados deverão ser publicadas, por meio de artigos, contribuindo assim com o processo de ensino aprendizagem de aritmética e álgebra na Educação Básica.

Por outro lado, o professor de Matemática que atua na Educação Básica não pode deixar de utilizar estes conceitos em seu cotidiano. A participação em congressos, e eventos de divulgação da Matemática é importante. O trabalho mais focado, de leitura de revistas com problemas, como a Revista do Professor de Matemática – RPM é imprescindível. É possível contribuir enviando as possíveis soluções para as situações problemas propostas nesta revista. Situações problemas diversificadas que envolvem não apenas o tema desenvolvido neste trabalho são propostas nos bancos de questões da OBMEP e da OBM (Olimpíada Brasileira de Matemática). Estes materiais são boas referências para permanente exercício do trabalho docente.

REFERÊNCIAS

BRASIL. Ministério da Educação. Secretaria da Educação Média e Tecnológica. *Parâmetros Curriculares Nacionais + (PCN+) - Ciências da Natureza, Matemática e suas Tecnologias*. Brasília: MEC, 2002.

BRASIL. Ministério da Educação. Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais: Matemática.* (3º e 4º ciclos do ensino fundamental). Brasília: MEC, 1998.

DOMINGUES, H. H. *Fundamentos de Aritmética*. Florianópolis: Editora da UFSC, 2009.

HEFEZ, A. *Elementos de Aritmética***.** 2ª edição. Rio de Janeiro: SBM, 2011.

OBMEP. *Olimpíada Brasileira de Matemática das Escolas Públicas*. Disponível em: <http://www.obmep.org.br>. Acesso em 04 de março de 2013.

OLIVEIRA, K. I. M.; FERNÁNDEZ, A. J. C. *Iniciação a Matemática: um curso com problemas e soluções*. Rio de Janeiro: SMN, 2010.

PARANÁ. Secretaria de Estado da Educação. Departamento da Educação Básica. *Diretrizes Curriculares para Educação Básica: Matemática*. Curitiba: SEED-PR, 2008.

POLYA, G. *A Arte de Resolver Problemas*. Rio de Janeiro: Editora Interciência, 2006.

ROONEY, A. *A História da Matemática – Desde a criação das pirâmides até a exploração do infinito*. São Paulo: Editora M. Books do Brasil, 2012.

SANTOS, J. P. O. *Introdução à Teoria dos Números*. Rio de Janeiro: SBM, 1998.

SHOKRANIAN, S.; SOARES, M.; GODINHO, H. *Teoria dos Números*. 2ª edição. Brasília: Editora UNB, 1999.

SMOLE, K.S.; DINIZ, M. I. *Ler, Escrever e Resolver Problemas*. Porto Alegre: Editora Artmed, 2001.